

# Configuration Guide for Mobility Based Policy Control for Overlay Deployments

Ericsson Service-Aware Policy Controller

USER GUIDE

## **Copyright**

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

## **Trademark List**

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

## **Abstract**

This document is a guideline to configure the SAPC node for the most typical functions for mobility based policy control for overlay deployments.



# Contents

<b>1</b>	<b>Configuration and Provisioning Overview</b>	<b>1</b>
1.1	Other Conventions	2
<b>2</b>	<b>Configuration Prerequisites</b>	<b>5</b>
<b>3</b>	<b>Smp Diameter Data</b>	<b>7</b>
<b>4</b>	<b>Provision PDN-GW Selection</b>	<b>9</b>
4.1	Provision PDN-GW Profiles	9
4.2	Provision PDN-GW List Profiles	10
4.3	Provision PDN-GW Lists to Subscribers or Subscriber Groups	10
4.4	Provision Conditional PDN-GW List with Policies	11
<b>5</b>	<b>Provision SPID Selection</b>	<b>13</b>
5.1	Provision SPIDs to Subscribers or Subscriber Groups	13
5.2	Provision Conditional SPID Selection Policies	13
<b>6</b>	<b>Configure Smp Session Control</b>	<b>15</b>
<b>7</b>	<b>Appendix A. Policy Types</b>	<b>17</b>
<b>8</b>	<b>Appendix B. Tags Related to Mobility Based Policy Control</b>	<b>19</b>
	<b>Reference List</b>	<b>21</b>





# 1 Configuration and Provisioning Overview

Next figure, shows the main parts related to configuration and provisioning in the SAPC.

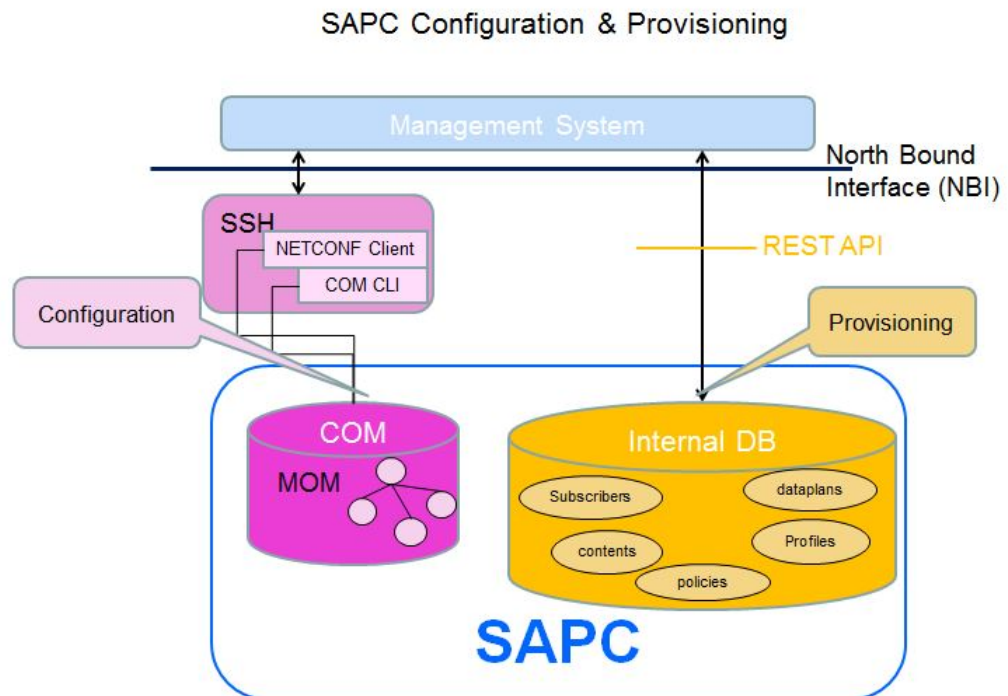


Figure 1 Configuration and Provisioning Overview

The purpose of this document is to provide guidelines and examples to configure Mobility Based Policy Control for Overlay Deployments and Smp interface related data in the SAPC node.

This document is not intended as an exhaustive guide to configure the SAPC for every possible scenario.

For general concepts about provisioning of policies, refer to [Configuration Guide for Subscription and Policies](#).

The complete parameter list and details of all configured options of the SAPC are included in separate documents. Refer to [Managed Object Model \(MOM\)](#) and [Provisioning REST API](#).

Examples on this document cover the case of data configured in the SAPC internal repository. In case an external repository is used, refer to [Database Access](#).



## 1.1 Other Conventions

This document refers to some configuration and provisioning data.

To clarify which detailed data is managed by COM or by the REST API, this document uses the following conventions:

- Configuration: whenever referring to Managed Object Class (MOC).

The detailed description for the object and attributes can be found in [Managed Object Model \(MOM\)](#).

Example: set `enableReauthsOnSubsChange` attribute in class `AppConfig`.

The tools or interfaces to manage these data in the SAPC are:

- a NETCONF interface, refer to [Ericsson NETCONF Interface](#).

The configuration examples show the NETCONF file contents, using the following syntax:

```
<edit-config>
...
<config>
  <ManagedElement xmlns="urn:com:ericsson:ecim:ComTop">
    <managedElementId>1</managedElementId>
    ...
  </ManagedElement>
</config>
</edit-config>
```

- b Or COM CLI, refer to [Ericsson Command-Line Interface](#).

- Provisioning: mainly subscribers, subscriber groups (dataplan), services (contents), profiles, and policy-related data. The SAPC provides a REST API for them, see [Provisioning REST API](#).

This document uses the following terminology for them: `<resource-name>` URI in the provisioning REST API.

Example: To provision subscriber groups, use the `dataplan` URI in the provisioning REST API.

And provisioning examples show HTTP operations on REST resources with the following syntax:

HTTP-Operation /resource-URI  
{json content} where /resource-URI is the relative URI from the SAPC provisioning base URI detailed in [Provisioning REST API](#).

Example:



```
PUT /dataplan/Gold
{ "dataplanName" : "Gold",
  "subscribedContents" : [{"contentName" : "HTTP_Streaming",
                           "redirect" : false}]
}
```

**Note:** To ease provisioning operations, the SAPC provides an HTTPS CLI client named resty, refer to [Provisioning Tools](#).







## 2 Configuration Prerequisites

Before configuring the SAPC in an operational network, assure that:

- CBA Components are installed.
- The SAPC product software is installed.
- To have a detailed understanding of the function.





## 3 Smp Diameter Data

No new configuration is needed for diameter in Smp.

**Note:** Origin-Host, Origin-Realm, IP address and diameter port values are set during the SAPC installation procedure. Diameter data related to capabilities exchange (application and vendor identifiers) are provided at installation time, so that no manual procedure is needed.





## 4 Provision PDN-GW Selection

This chapter shows how to provision the necessary data for the PDN-GW selection: PDN-GW profiles and PDN-GW list profiles, and how to assign PDN-GW list profiles conditionally or unconditionally.

### 4.1 Provision PDN-GW Profiles

To define a PDN-GW in profiles, use the corresponding pdn-gw URI in the Provisioning REST API for each PDN-GW.

The PDN-GW can be defined according to one of the following rules:

- The PDN-GW profile has FQDN definition, but it has no IP definition.
- The PDN-GW profile has no FQDN definition, but it has at least one IP (IPv4, IPv6 or both).
- The PDN-GW profile has both FQDN and IP definitions.

**Note:** All the PDN-GWs within a PDN-GW list must fit in just one of these entries.

See Example 1 for provisioning three PDN-GWs: pgw1 with FQDN only, pgw2 with IP addresses only, and pgw3 with both FQDN and IP.

```
PUT /profiles/pdn-gw/pgw1
{
  "name" : "pgw1",
  "fqdn" : "pgw1.ericsson.com"
}

PUT /profiles/pdn-gw/pgw2
{
  "name" : "pgw2",
  "ipv4" : "10.10.22.2",
  "ipv6" : "1238:9671:0E2A:2D64:AF00:0000:0000:01D1"
}

PUT /profiles/pdn-gw/pgw3
{
  "name" : "pgw3",
  "fqdn" : "pgw3.ericsson.com",
  "ipv6" : "1238:9671:0E2A:2D64:0000:0000:3300:1100"
}
```

#### Example 1 Provisioning of PDN-GWs



## 4.2 Provision PDN-GW List Profiles

A PDN-GW list is composed of one or more PDN-GWs. To define a PDN-GW list in profiles, use the `pdn-gw-list` URI in the Provisioning REST API listing the associated PDN-GWs in the `pdnGwList` attribute.

See Example 2 for provisioning PDN-GW list `pgwListEricsson`, in which `pgw1` and `pgw2` should obey the same rule for PDN-GW definition described in Section 4.1 on page 9.

```
PUT /profiles/pdn-gw-list/pgwListEricsson
{
  "name": "pgwListEricsson",
  "pdnGwList": ["pgw1", "pgw2"]
}
```

### Example 2 Provisioning of a PDN-GW List

## 4.3 Provision PDN-GW Lists to Subscribers or Subscriber Groups

A PDN-GW list profile can be assigned to a subscriber or subscriber group. Profiles assigned to a subscriber prevail over profiles assigned to a subscriber group if both are provisioned.

To assign a PDN-GW list to a subscriber or subscriber group, use the `pdnGwListName` field in the `staticQualification` attribute of the `subscribers` or `dataplane` URI in the Provisioning REST API.

**Note:** The SAPC uses the IMSI to access the subscriber profile, so the subscribers must be provisioned with IMSI.

See Example 3 for assigning `pgw1List` to a subscriber and assigning `pgwListEricsson` to a subscriber group.



```
PUT /subscribers/7160652952503786
{
  "staticQualification" :
  {
    "pdnGwListName" : "pgw1List"
  },
  "subscriberId" : "7160652952503786"
}

PUT /dataplan/Gold
{
  "staticQualification" :
  {
    "pdnGwListName" : "pgwListEricsson"
  },
  "dataplanName" : "Gold"
}
```

### Example 3 Provisioning of staticQualification

## 4.4 Provision Conditional PDN-GW List with Policies

To configure PDN-GW lists depending on conditions, create the needed policies using:

— For **Global policy locator**:

`/locators/resources/any/contexts/pdn-gw`

— For **Subscriber group locator**

`/dataplan/<dataplanName>/locators/resources/any/contexts/pdn-gw`

— For **Subscriber locator**

`/subscribers/<subscriberId>/locators/resources/any/contexts/pdn-gw`

— Within the `outputAttributes` object in the rule, set:

- `attrName` attribute to `pdn-gw-list`
- `attrValue` to the provisioned PDN-GW list name

Example 4 shows the configuration of a policy to return a PDN-GW list for a subscriber group.



```
PUT /rules/pdnGw_rule
{
  "condition" : "(AccessData.bearer.accessPoint == \"APN1\")",
  "outputAttributes" :
  [
    {
      "attrName" : "pdn-gw-list",
      "attrValue" : "\"pgwConditionalList\"",
      "result" : "permit"
    }
  ],
  "ruleName" : "pdnGw_rule"
}

PUT /policies/pdnGw_policy
{
  "policyName" : "pdnGw_policy",
  "ruleCombiningAlgorithm" : "permit-overrides",
  "rules" : [ "pdnGw_rule" ]
}

PUT /dataplan/Silver/locators/resources/any/contexts/pdn-gw
{
  "policies" : [ "pdnGw_policy" ]
}
```

#### Example 4 Provisioning of rule, policy and locator for a PDN-GW List dynamic selection





## 5 Provision SPID Selection

### 5.1 Provision SPIDs to Subscribers or Subscriber Groups

An SPID can be assigned unconditionally to a subscriber or subscriber group. Values assigned to a subscriber prevail over the ones assigned to a subscriber group if both are provisioned.

To assign an SPID to a subscriber or subscriber group, use the `spid` field in the `staticQualification` attribute of the `subscribers` or `dataplan` URI in the Provisioning REST API.

**Note:** The SAPC uses the IMSI to access the subscriber profile, so the subscribers must be provisioned with IMSI.

See Example 5 for provisioning SPIDs to a subscriber and a subscriber group.

```
PUT /subscribers/7160652952503786
```

```
{
  "staticQualification" :
  {
    "spid" : 200
  },
  "subscriberId" : "7160652952503786"
}
```

```
PUT /dataplan/Bronze
```

```
{
  "staticQualification" :
  {
    "spid" : 133
  },
  "dataplanName" : "Bronze"
}
```

#### Example 5 Provisioning of Unconditional SPIDs

### 5.2 Provision Conditional SPID Selection Policies

To configure SPID depending on conditions, create the needed policies using:

— For **Global policy locator**:

```
/locators/resources/any/contexts/spid
```

— For **Subscriber group locator**

```
/dataplan/<dataplanName>/locators/resources/any/contexts/spid
```

— For **Subscriber locator**



/subscribers/<subscriberId>/locators/resources/any/contexts/spid

— Within the outputAttributes object in the rule, set:

- attrName attribute to spid
- attrValue to the SPID value

Example 6 shows the configuration of a policy to return an SPID for a subscriber.

```
PUT /rules/r_spidSelectionAPN1
{
  "condition" : "(AccessData.bearer.accessPoint == \"APN1\")",
  "outputAttributes" :
  [
    {
      "attrName" : "spid",
      "attrValue" : "25",
      "result" : "permit"
    }
  ],
  "ruleName" : "r_spidSelectionAPN1"
}

PUT /rules/r_spidSelectionNotAPN1
{
  "condition" : "(AccessData.bearer.accessPoint != \"APN1\")",
  "outputAttributes" :
  [
    {
      "attrName" : "spid",
      "attrValue" : "45",
      "result" : "permit"
    }
  ],
  "ruleName" : "r_spidSelectionNotAPN1"
}

PUT /policies/p_spidSelection
{
  "policyName" : "p_spidSelection",
  "ruleCombiningAlgorithm" : "permit-overrides",
  "rules" : [ "r_spidSelectionAPN1", "r_spidSelectionNotAPN1" ]
}

PUT /subscribers/34699009900/locators/resources/any/contexts/spid
{
  "policies" : [ "p_spidSelection" ]
}
```

## Example 6 Provisioning of Conditional SPIDs



## 6 Configure Smp Session Control

To configure Smp session control depending on conditions, for notifying the SGSN-MME to continue the IP-CAN session but drop the Smp session, create the needed policies using:

- For **Global policy locator**  
/locators/resources/sx-session/contexts/access
- For **Subscriber group locator**  
/dataplanes/<dataplanName>/locators/resources/sx-session/contexts/access
- For **Subscriber locator**  
/subscribers/<subscriberId>/locators/resources/sx-session/contexts/access
- No need to use outputAttributes

Example 7 shows configuration of a policy to maintain or drop the Smp session.

```
PUT /rules/SxAccessControl_rule
{
  "ruleName" : "SxAccessControl_rule",
  "condition" : "not(Subscription.group[\"2g-group\"].isActive) && not(Subscription.group[\"3g-group\"].isActive)
}
PUT /policies/SxAccessControl_policy
{
  "policyName" : "SxAccessControl_policy",
  "ruleCombiningAlgorithm" : "permit-overrides",
  "rules" : ["SxAccessControl_rule"]
}
PUT /locators/resources/sx-session/contexts/access
{
  "policies": ["SxAccessControl_policy"]
}
```

### Example 7 Configuration of Smp Session Control

In this example, the Smp session is maintained if:

- The subscriber does not belong to 2g-group or 3g-group, or
- The subscriber belongs to 2g-group or 3g-group, or both groups, but neither 2g-group nor 3g-group is active.

Else, the Smp session is dropped and no further Smp controls are executed.





# 7 Appendix A. Policy Types

Next figure shows the different policy types applicable to mobility based policy control, which can be used in the SAPC.

Smp related Policies  
(Mobility based Policy Control)



Policy Type	Policy Locator			Output Attributes	Comments
	Context	Resource	Subject		
Smp Session control	access	sx-session	<subscriberId> <dataplanId>	-	Type I = Only policies, no qualification Smp Conditions: Access Data Subscriber
PDN GW Selection	pdn-gw	any	<subscriberId> <dataplanId> 	permit pdn-gw-list "<pdnGwList name value>"	Type II = Mixing policies and qualification Smp Conditions: Access Data Subscriber
SPID Selection	spid	any	<subscriberId> <dataplanId> 	permit spid <value>	Type II = Mixing policies and qualification Smp Conditions: Access Data Subscriber

Figure 2 Mobility based Policy Control (Smp) Policies





## 8 Appendix B. Tags Related to Mobility Based Policy Control

The following table shows the tags used for mobility based policy control:

Table 1 Incoming Message Tags

Tag	Return Type	Possible Values	Comments
AccessData.bearer.accessPoint	String	any	The Called Station ID. Address where the user is connected to. Network ID + Operator ID
AccessData.subscriber.imsi	String	any	Subscriber identifier in international IMSI format.
AccessData.subscriber.locationInfo.cellIdentity	Integer	0-65535 for GPRS, 0-268435455 for EPS	Cell identity where the user currently is registered.  For 3GPP-GPRS and 3GPP-EPS access types, the cell identity is obtained from the 3GPP-User-Location-Info AVP.  For non-LTE, the cell identity is obtained when geographic location type is Cell Global Identification (CGI).  For LTE scenarios, E-UTRAN Cell Identifier (ECI) is obtained when geographic location type is ECGI.
AccessData.subscriber.locationInfo.locationAreaCode	Integer	0-65535	Location area code where the user currently is registered, within the geographic location.  For 3GPP-GPRS and 3GPP-EPS, the location area code is obtained from 3GPP-User-Location-Info AVP, or if this AVP is not available, the location area code is obtained from RAI AVP.



Tag	Return Type	Possible Values	Comments
AccessData.subscriberLocationInfo.routingAreaCode	Integer	0-65535	<p>For non-LTE scenarios, the routing area code is the code of routing area where the user currently is registered, within the Routing Area Identification (RAI) geographical location type.</p> <p>The routing area code is obtained from 3GPP-User-Location-Info AVP, or if this AVP is not available, obtained from RAI AVP.</p> <p>For LTE scenarios, the Tracking Area Code (TAC) obtained is from 3GPP-User-Location-Info AVP, when geographic location type is TAI.</p>
AccessData.subscriberLocationInfo.serviceAreaCode	Integer	0-65535	<p>Service area code where the user is registered, within the Service Area Identification (SAI) geographical location type.</p> <p>For 3GPP-GPRS and 3GPP-EPS, it is obtained from 3GPP-User-Location-Info AVP.</p>
AccessData.subscriber.msisdn	String	any	Subscriber identifier in international E.164 format (MSISDN).
AccessData.userEquipmentInfo.model	Integer	any	IMEI-SV Type Allocation Code
AccessData.userEquipmentInfo.serialNr	Integer	any	IMEI-SV Serial Number
AccessData.userEquipmentInfo.version	Integer	any	IMEI-SV Software Version Number





## Reference List

### **Ericsson Documents**

- [1] Configuration Guide for Subscription and Policies
- [2] Database Access