

# System Administrator Guide

## Ericsson Service-Aware Policy Controller

### USER INSTRUCTIONS

**Copyright**

© Ericsson España 2018. 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

<b>1</b>	<b>System Administration Overview</b>	<b>1</b>
<b>2</b>	<b>Administration Interfaces and Tools</b>	<b>3</b>
2.1	Interfaces	3
2.1.1	REST API	3
2.1.2	NETCONF	3
2.1.3	SSH	4
2.1.4	SFTP	4
2.1.5	SNMP	4
2.2	Tools	4
2.2.1	Policy Studio	5
2.2.2	COM CLI	5
2.2.3	SSH	5
<b>3</b>	<b>Configuration and Provisioning Overview</b>	<b>7</b>
3.1	Configuration through COM	8
<b>4</b>	<b>Performance Measures Management</b>	<b>9</b>
<b>5</b>	<b>Fault Management</b>	<b>11</b>
<b>6</b>	<b>Logging Management</b>	<b>13</b>
<b>7</b>	<b>Security Management</b>	<b>15</b>
<b>8</b>	<b>Startup and Shutdown</b>	<b>17</b>
8.1	SAPC Restart	17
8.2	SAPC Stop	17
8.3	SAPC Start	17
8.4	Processor Restart	18
<b>9</b>	<b>Directory Structure</b>	<b>19</b>





# 1 System Administration Overview

This document is a guide used in the SAPC for the purposes of node administration and configuration providing information about what can be accessed or configured in the SAPC node and through which interfaces or tools this access or configuration is to be performed. This document is not intended to describe how to install and perform the initial configuration of the SAPC, neither the hardware replacement.

The SAPC provides several interfaces and tools for system administrators, for the following purposes:

- Configuration and provisioning
- Performance management
- Fault management
- Logging management

These different interfaces, tools, and procedures are described in the following sections.





## 2 Administration Interfaces and Tools

### 2.1 Interfaces

This section describes all the different operation and maintenance interfaces provided by the SAPC to the operator to access and configure the node. An overall view of these interfaces is shown in Figure 1 and they are depicted in the following chapters.

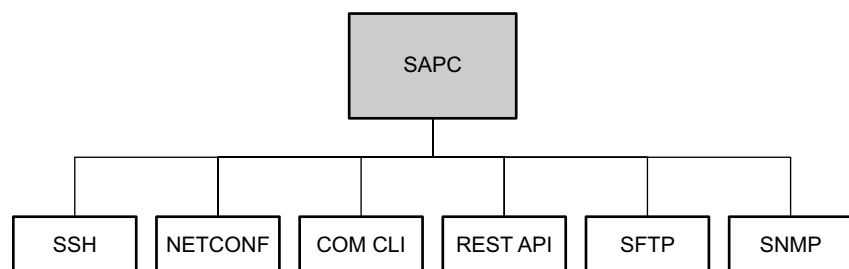


Figure 1 Operation and Maintenance of the SAPC Interfaces

The access to the interfaces depends on the roles defined in Section 7 on page 15.

#### 2.1.1 REST API

The SAPC provides the following REST APIs:

- Analytics REST API for getting analytics data from internal or external systems, refer to [Analytics REST API](#).
- Provisioning REST API for provisioning data, refer to [Provisioning REST API](#). Provisioning data persist in an internal database.

#### 2.1.2 NETCONF

The Network Configuration Protocol (NETCONF), built on top of SSH, is a machine-machine interface that provides mechanisms to create, modify, and delete the SAPC configuration data.

The NETCONF interface is provided by Common Operation and Maintenance (COM).

For more information about NETCONF, refer to [Ericsson NETCONF Interface](#).



### 2.1.3 SSH

Secure Shell (SSH) is a network protocol that allows data to be exchanged by using a secure channel between two network devices.

**Note:** Access by SSH to the SAPC is only recommended when it is indicated in this document or any other that this one is referring to.

### 2.1.4 SFTP

The Secure File Transfer Protocol, built on top of SSH, is supported to securely transfer or access files from the SAPC to external systems. For file management, see [Handling Files](#).

1. Connect to the SAPC by SFTP, to the <OAM VIP>, with user=sapcadmin and port=115.
2. To know the path to the needed file, follow the procedure explained in [List File Groups and File Information in Logical File System](#).

For example, for Performance Management files, see FileGroup=PerformanceManagementReportFiles.

The following file groups are created by the SAPC:

- uetracefiles
- PolicyControlPdcFiles
- PolicyControlRestGetCollections
- ConfigurationFiles
- TracesFiles

3. Then, follow the procedure explained in [Fetch File in Logical File System](#).

**Note:** The SAPC also provides SFTP access in port 22. Then the remote working directory is /home/<user\_sftp> or /home/system-oam/<user\_sftp> for COM users.

### 2.1.5 SNMP

Simple Network Management Protocol (SNMP) is based on the agent and manager communication protocol over the User Datagram Protocol (UDP). A standard protocol is used to interchange administrative information between Network Elements.

## 2.2 Tools

This section describes the tools to be used through the different interfaces for operation and maintenance purposes.





### 2.2.1 Policy Studio

Policy Studio can be used for operation and maintenance purposes. For further information refer to [Policy Studio](#).

### 2.2.2 COM CLI

COM CLI (also known as ECLI) is a terminal-based command line interface which allows the operator to monitor and manage (for example check active alarms, manage the SAPC configuration data) the Managed Element (ME). It enables interaction with the Management Information Base (MIB) through common, generic-purpose commands.

To access the COM CLI for administration node operations, the system administrator must use:

```
ssh sapcadmin@<OAM VIP> -p <COM_port> -t -s cli
```

where <OAM VIP> is the SAPC VIP OAM and <COM\_port> is the COM port, normally 830.

```
ssh sapcadmin@10.42.118.235 -p 830 -t -s cli
```

As an example of use of this tool is:

```
>show ManagedElement=1
ManagedElement=1
SystemFunctions=1
Transport=1
JavaCaf=1
PolicyControlFunction=1
```

For further information about this interface, refer to [Ericsson Command-Line Interface](#).

### 2.2.3 SSH

SSH access to the system must be used for operation and maintenance purposes specified along this document or in any other document that this refers to. The access to the SSH tool depends on the roles defined in Section 7 on page 15.

To access the system, execute the following command:

```
ssh sapcadmin@<OAM VIP>
```





### 3 Configuration and Provisioning Overview

The following sections introduce the main concepts related to configuring and provisioning data in the SAPC.

Guidelines for configuring the SAPC in each specific scenario (function) can be found in the SAPC Configuration Guides.

Figure 2 shows the main parts related to configuration and provisioning in the SAPC.

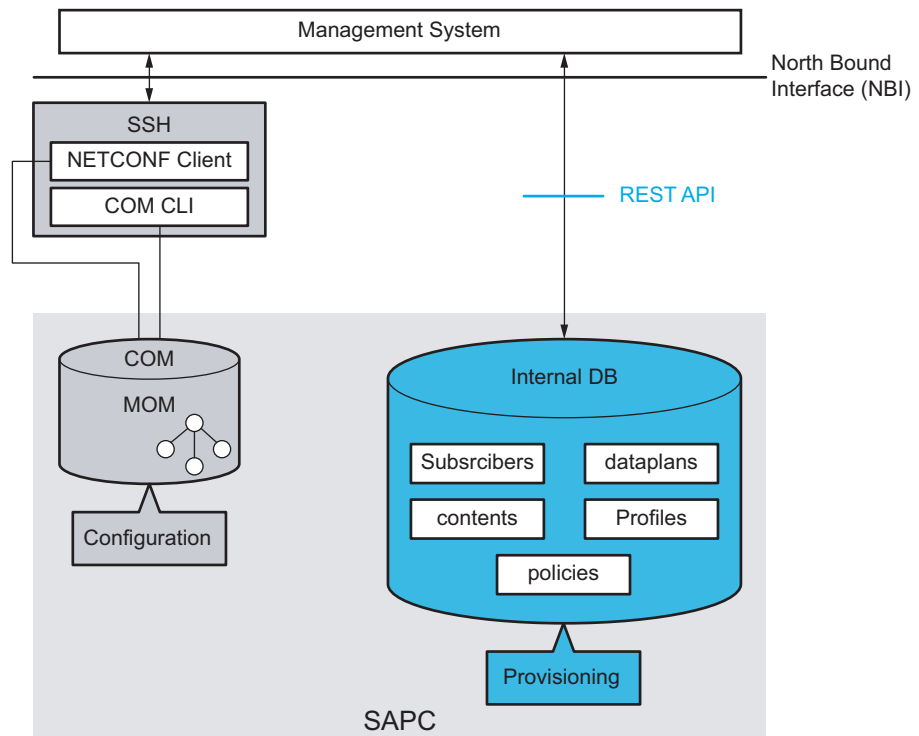


Figure 2 The SAPC Configuration and Provisioning

**Configuration** Management is the process where a configuration entity, or in general, a network management entity, issues orders to provide the parameters and information necessary for the correct operation of a network element, in terms of both software and hardware.

The **Provisioning** function is the supplying of all the data necessary for the use of that a user or a set of users make of a service. It comprises both service and user-related data. For details of the SAPC provisioning related data and provisioning tools, refer to [Provisioning REST API](#) and [Provisioning Tools](#).



## 3.1 Configuration through COM

The SAPC uses COM to configure some of the application data, offering a Managed Object Model (MOM).

There are two ways of accessing to the MOM:

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

An example of the NETCONF command (executed from an external machine) to configure an object included in the “filename.xml” file is the following:

```
netconf-console -u sapcadmin -p <password> --proto=ssh  
--port=830 --host=<OAM VIP> -s raw --rpc=RPC filename.xml
```

**Note:** The netconf-console is only an example of the NETCONF client. The SAPC does not provide any NETCONF clients. It is the operator's responsibility to use any NETCONF clients.

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

To read the attribute values of an object in COM, refer to the **Display MO instances** chapter in [Ericsson Command-Line Interface](#).

For details of the SAPC data that can be configured using COM, refer to [Managed Object Model \(MOM\)](#).



## 4 Performance Measures Management

For information referring to the Performance Measurement Management, refer to [Measurements](#).





## 5 Fault Management

Perform a daily verification of the active alarms and notifications. There are two ways to do it:

- Through any external system configured to collect SNMP traps.
- Through the COM CLI tool provided inside the SAPC.

To verify the alarms and notifications through the COM CLI tool, follow these steps:

1. Access the COM CLI according to Section 2.2.2 on page 5
2. Execute the following command (more information in [Ericsson Command-Line Interface](#)):

```
show-table ManagedElement=1,SystemFunctions=1,Fm=1 -m FmAlarm  
-p fmAlarmId, specificProblem
```

```
=====
| fmAlarmId | specificProblem |
=====
| 139       | Policy Control, Number of Gx Session |
|           | Rejections Reached                   |
=====
```

For information about procedures related to alarms and notifications, see the Fault Management folder in the library.







## 6 Logging Management

For information about the SAPC logging management, refer to [Logging Events](#).





## 7 Security Management

Table 1 lists the SAPC administrators and their corresponding roles created at installation time.

The root user who is created in the LDE domain has authorization to do any action on the SAPC. All the other administrators are created and managed through the COM domain. See more information in [Security Management Guide](#).

Table 1 SAPC Administrators and Roles

Administrator	Role	Role definition	COM NBI Access and Permission <sup>(1)</sup>	Provisioning/Analytics Access and Permission <sup>(2)</sup>	Linux File System Access and Permission
sapcadmin	Super User <sup>(3)</sup>	Has complete access to all resources within a system and the applications residing on that system (for example, root for UNIX systems).	ManagedElement (RWX)	Provisioning REST (RW)  Analytics REST (R)	SSH port 22 enabled  Linux group sapcgrp  SFTP port 22,115 access



Administrator	Role	Role definition	COM NBI Access and Permission <sup>(1)</sup>	Provisioning/Analytics Access and Permission <sup>(2)</sup>	Linux File System Access and Permission
sapcp prov	SapcProvisioningAdministrator	Only provisioning access is permitted.	Default authorization permissions	Provisioning REST (RW) Analytics REST (R)	-
systemread only	SapcSystemRead Only	Has the possibility to monitor the configuration of non-security-related attributes and capabilities of a managed element.	ManagedElement except SecM (R)	Provisioning REST (R) Analytics REST (R)	FileMtree (R) SFTP port 22,115 access

(1) The SSH port for COM NBI access is 830. R: the administrator can read MOs and get attribute values; RW: the administrator can create and delete MOs as well as get and set attribute values; RWX: the administrator can create and delete MOs, set and get attribute values, as well as execute all actions in the MOM.

(2) R: the administrator can perform GET operation on Provisioning or Analytics REST API; RW: the administrator can perform GET, PUT, and DELETE operations on Provisioning REST API.

(3) The administrator created with the SuperUser role does not match the same privileges owned by sapcadmin. But this will be fully supported in the next version SAPC 1.4: where the SuperUser will have the same access and permission as the sapcadmin default user.



## 8 Startup and Shutdown

This section describes the start and stop procedures. Before performing any of these actions, it is recommended to perform a backup.

---

---

### Caution!

All these operations affect traffic performance.

---

---

### 8.1 SAPC Restart

To restart the SAPC, execute the following steps:

1. Access the SAPC according to Section 2.2.3 on page 5.
2. `sapcadmin@SC-X>sudo sapcApplication -a restart`
3. Check the SAPC status:

```
sapcadmin@SC-X>sudo sapcApplication -a status
```

### 8.2 SAPC Stop

To stop the SAPC, execute the following steps:

1. Access the SAPC according to Section 2.2.3 on page 5.
2. `sapcadmin@SC-X>sudo sapcApplication -a stop`
3. Check the SAPC status:

```
sapcadmin@SC-X>sudo sapcApplication -a status
```

### 8.3 SAPC Start

To start the SAPC, execute the following steps:

1. Access the SAPC according to Section 2.2.3 on page 5.
2. `sapcadmin@SC-X>sudo sapcApplication -a start`
3. Check the SAPC status:

```
sapcadmin@SC-X>sudo sapcApplication -a status
```



## 8.4 Processor Restart

A processor on the SAPC can be restarted individually.

1. Access the SAPC according to Section 2.2.3 on page 5.
2. Restart the processor in the SAPC.

```
sapcadmin@SC-X>sudo cmw-node-reboot <processor>
```

3. Wait until the processor is back.
4. Check the SAPC status:

```
sapcadmin@SC-X>sudo sapcApplication -a status
```



## 9 Directory Structure

Table 2 shows the directories which contain configuration and storage files:

Table 2 Directory Structure

Directory Path	Comment
/cluster/storage/system/config/sapc	Directory containing the configuration files. It is in the SC-1 and SC-2.