

# Security Management Guide

Ericsson Service-Aware Policy Controller

USER GUIDE

**Copyright**

© Ericsson España S.A. 2017,2018. 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>Security Management Guide Introduction</b>	<b>1</b>
1.1	Security Management Prerequisites	2
1.2	Security Management Environment	3
1.3	Security Management Definitions	3
<b>2</b>	<b>Security Management Overview</b>	<b>7</b>
2.1	Threats	7
2.2	Defense	8
<b>3</b>	<b>Product Security Functionality</b>	<b>9</b>
3.1	Network Security Level	9
3.2	Node Security Level	10
3.3	OAM Security Level	10
<b>4</b>	<b>Security Configuration</b>	<b>13</b>
4.1	Network Security Level	13
4.2	Node Security Level	13
4.3	OAM Security Level	17
<b>5</b>	<b>Security in the Cloud</b>	<b>27</b>
<b>6</b>	<b>Default Parameter Values</b>	<b>29</b>
<b>7</b>	<b>Services, Ports, and Protocols</b>	<b>31</b>





# 1 Security Management Guide Introduction

This instruction describes the security functions available in the SAPC.

Internet Protocol (IP) networks are vulnerable to various types of attacks, and exposure to these threats has increased since IP is used at various parts of the mobile networks. The SAPC provides functions for withstanding and preventing different forms of attacks.

Strong security awareness is a must for any product either directly connected to the Internet or indirectly connected (such as, behind a firewall).

For this reason, the information contained in any product must be protected, which is not an exception, in the case of SAPC. The type of subscriber information contained in SAPC to protect comprises:

- IP address
- MSISDN
- IMSI
- IMEI
- Mobile number
- User Id
- Email address
- Location: cell identity, Location Area code, routing area code, routing area identity, and service area code

IP networks are vulnerable to various types of attacks:

- Eavesdropping
- Data modification
- Identity Spoofing
- Password-based attacks
- Denial of Service
- Man-in-the-middle
- Compromised-Key
- Sniffer
- Application-Layer



Therefore, mobile networks are highly vulnerable since IP protocol is one of the most used protocols in the mobile networks. The number of internet threats exposed to hosts, routers, servers, and other network-connected equipment are overwhelming and constantly growing. As a result, network systems must support security precautions that safeguard the operation, service, and functions of all supported services.

The operator is responsible for implementing and deploying the proper countermeasures in networks to prevent any security intrusion, although the SAPC provides functions for resisting and preventing different forms of attacks.

In case, a security incident happens in a network where the SAPC is deployed, the operator investigates the issue, tracing back the problem to find the root cause of the security breach. If the security incident is related to a flaw in SAPC product, this is communicated timely and diligently.

This document covers the following issues:

- An overview presenting the context of Security in the SAPC.
- Potential threats to the systems interacting with the SAPC.
- Description of the security functions provided by the SAPC at end user, network, and node levels.
- Technical specification.
- Information on security configuration procedures can be found in [6].
- Parameters. For a description of each parameter, see [10].
- Counters. For a description of each counter, see [9].
- Alarms. For description of any alarm raised by the SAPC, consult the CPI documentation (Operation and Maintenance, Fault Management, Alarms).
- Information on logs related to the SAPC application can be found in ref. [3].

### **Target Groups**

This instruction is intended as an introduction to security functions for network operation and network optimizing personnel as well as system engineers and system administrators. It assumes a basic knowledge of telecommunications.

## **1.1 Security Management Prerequisites**

### **Conditions**

Before performing the procedures in Section 4 on page 13, ensure that the following conditions are met:

- The required software is available.



- The required hardware (equipment) has been checked.
- The SAPC has been hardened.
- The administrator (user) has the required access privileges.
- The administrator username and passwords are known.
- The IP Addresses and ports used by the system are known.

## 1.2 Security Management Environment

The SAPC must be deployed behind a firewall, which offers protection from external attacks. Also, different types of traffic are separated in different VLANs.

## 1.3 Security Management Definitions

### 1.3.1 Basic Terms and Concepts

The basic terms and concepts listed are of paramount importance (For further details, refer to <https://tools.ietf.org/html/rfc2196>)

<b>Availability</b>	It is the system ability to withstand a Denial of Service.
<b>Accountability</b>	It is the system ability to withstand tampering or manipulation.
<b>Attack</b>	It is an action taken against a network system with the intention of doing harm.
<b>Authentication</b>	It is the system ability to validate the user identity.
<b>Authorization</b>	It is the system ability to validate the user access rights.
<b>Basic Elements</b>	<p>The three basic elements to protect in any systems are: software, hardware, and data / information.</p> <p>Essentially, the most important item to protect is information, since it constitutes one of the major assets of any organization.</p>
<b>Distributed Denial of Service</b>	It is a DoS attack using distributed resources over the network.



### Denial of Service

It is an attempt to make a machine or network resource unavailable to its intended users. It generally consists of efforts to interrupt or suspend services of a host connected to a network.

### Reliable System

In general, a system is said to be **reliable** if it satisfies the following properties:

- **Confidentiality:** It concerns the protection of system resources from unauthorized disclosure. Preservation of confidentiality is defined as ensuring that resources are accessible only to elements authorized to have access.
- **Integrity:** system resources are modified or changed by those elements that have authorization (these operations include creation, deletion, modification, and so on). Preservation of integrity is defined as safeguarding the accuracy and completeness of resources and processing methods.
- **Availability:** system resources are always accessible by the authorized elements. It also concerns the safeguarding of necessary resources and associated capabilities. Preservation of availability is defined as ensuring that the authorized elements have access to resources and associated assets when required.

### Risk

Risk is a combination of the probability of an event and its consequence. Risk is a quantitative concept. Therefore it is possible to estimate the value of the risk: Expected value = estimated loss from risk (\$) x likelihood of loss (%)





<b>Secure network</b>	<p>A secure network is one that fulfills the following conditions:</p> <ul style="list-style-type: none"> <li>• The traffic keeps passing legitimate customer traffic (availability).</li> <li>• Traffic goes where it is supposed to go, and only where it is supposed to go (availability, confidentiality).</li> <li>• The Network Elements remain manageable (availability).</li> <li>• Only authorized users can manage Network Elements (authentication, authorization).</li> <li>• There is a record of all security-related events (accountability).</li> <li>• The network operator has the necessary tools to detect and respond to illegitimate traffic.</li> </ul>
<b>Threat</b>	It is the potential for the occurrence of a harmful event to the network system, such as an attack.
<b>Value</b>	The Security concept is associated to another concept from which it gets the sense: value. The SAPC only protects those assets that have an important value for the customer, and therefore, security is intimately associated to the value SAPC provide to the assets.
<b>Vulnerability</b>	It is a weakness that makes the network system susceptible of an attack.

## 1.3.2

### Security Pillars

All elements that are implemented in an organization/product must be based on these three pillars:

- Principles and objectives of the organization
- Risk Assessment
- Legal Framework

### 1.3.2.1

#### Risk Assessment

This process allows SAPC to detect which security deficiencies have the product and to analyze which would be the best form to protect the product against these risks that have been detected. An analysis of risks provides the organization with reasonable evidences from security point of view. An analysis of risks can be considered a photo of the security inside the organization or the product.



The elements to be considered in the process of risk assessment are the following:

- **Assets:** These are all those elements which hold the organization or product that are analyzed during the process. This statement includes any type of item the organization / product needs to do business activities.
- **Threats:** The situations that could happen in an organization / product that could hurt its assets, causing them not working properly or not being used in the correct way to do the activity of the business organization.
- **Vulnerabilities:** These are the various weaknesses that present the assets previously identified and that are exploited by the threats to cause harm.
- **Impacts:** These are the consequences that occur in the organization / product when a threat exploits a vulnerability to harm an asset.



## 2 Security Management Overview

The security mechanism and functions in the SAPC are designed with the following perspective in mind:

- **End-user security** or the integrity and security of the End User.
- **Node security** or the integrity of the SAPC itself, such as authentication of the management operations and prevention of Denial of Service (DoS) attacks (Node administration and user management).
- **Network security**, comprising any security function to protect the integrity of the Packet Core and traffic from / to the UE.
- **Operation and maintenance (OAM)** security.

For information about the interfaces supported by the SAPC, refer to [Service-Aware Policy Controller](#).

The SAPC provides two main mechanisms for perimeter defense:

- **IP Packet Filtering**: It allows only certain types of traffic over individual interfaces.
- **User Access Control**: The SAPC secures that only authorized users have access to the node.

Also, the SAPC provides the following surveillance mechanisms:

- **Counters**: There are numerous counters in the SAPC, which count an event in the SAPC, for example the number of correctly processed incoming requests.
- **Alarms**: The alarm handling mechanism alerts when a fault has occurred or when a given counter exceeds a predefined value.
- **Logging**: The logging mechanism logs certain events to files on the SAPC. By reading these files, it is possible to track passed events in the SAPC.

### 2.1 Threats

There are several potential threats to SAPC, but only few of these threats have large risk of occurring and causing damage, such as DoS attack and / or fraud.

The following are examples of actors that pose a threat:

- Internet users
- Corporate users



- Corporate Local Area Network (LAN) users (using a fixed workstation on a LAN that also provides intranet access).
- Operation and Maintenance users on the backbone network (operator staff).
- Other users on the backbone network (staff of roaming partners).

## 2.2 Defense

The SAPC Security, based on the perimeter defense principle, provides protection at the following levels:

- End-user level. The SAPC secures the MS or UE user information.
- Network level. The SAPC secures the communication between the SAPC and network hosts. See Section Network Security Level.
- Node level. The SAPC provides security functions on node level. See Section Node Security Level.
- OAM level. The SAPC secures communication with OAM nodes. See Section OAM Security Level.



## 3 Product Security Functionality

### 3.1 Network Security Level

The SAPC provides a set of functions securing the communications between the SAPC and the nodes it interacts with. Most network security configuration can be done on each interface.

#### 3.1.1 ICMP Reply

The Internet Control Message Protocol (ICMP) is allowed by default, since it use does not pose any risk and the SAPC is not supposed to be exposed to external networks. However, to prevent the SAPC from being flooded with ICMP messages, other network infrastructure elements (such as firewalls or routers) must be configured.

#### 3.1.2 Traffic Separation

The SAPC provides traffic separation among all the interfaces. The following list depicts the interfaces supported in the SAPC which are not interconnected among them:

- DIAMETER: Gx, Rx, Sy
- NetConf, REST, SOAP (Web Services)
- SMPP
- SNMP, SFTP

The SAPC is connected to several external IP networks through several interfaces. On important aspect, from security point of view is that the SAPC does not route traffic between different interfaces (that is, acting as proxy).

#### 3.1.3 Denial of Service Attacks

DoS attacks can prevent legitimate clients from accessing the SAPC. An attacker floods the system with traffic that blocks the entry for others clients or consumes all available resources. To protect the SAPC from such DoS attacks, configure the firewall / router connected to the SAPC (that isolates the SAPC from the outer network) to limit the request rate which the clients use when connecting to the node.



## 3.2 Node Security Level

This section describes the node security, or the integrity of the node itself, such as authentication of management operations and prevention of DoS attacks. The SAPC offers the following user management tools from a security perspective:

- NETCONF / ECLI User Management
- Linux user management

### 3.2.1 Ericsson Command-Line Interface

Details on the security features provided by Ericsson Command-Line Interface (ECLI) can be found at [Ericsson Command-Line Interface User Guide](#). Any ECLI session is running securely over SSH protocol.

### 3.2.2 NETCONF User Management

Details on the security features provided by NETCONF can be found at [Ericsson Command-Line Interface User Guide](#). User authentication and secure NETCONF connection and transport over the Secure Socket Layer (SSL) is provided by the SSH daemon or the Transport Layer Security (TLS) proxy component.

## 3.3 OAM Security Level

### 3.3.1 Confidentiality and Integrity Protection of OAM Traffic

Concerning security, the communication between the NBI user and the SAPC is encrypted with SSH.

### 3.3.2 Node Operator Authentication and Access Control

When logging on to the SAPC, the SAPC makes an authentication check of the username and password. It is possible to log on to the SAPC through either one of the following domains: the Common Management domain, through the OAM (LDE) domain, and through the Provisioning (REST) domain.

At initial start of the SAPC, the only configured administrators are the following:

- NefConf domain: sapcadmin.
- COM domain: root (failsafe accounts).
- REST domain: sapcprov.

The root administrator is a superuser who has authorization to do any action on the SAPC.



The administrator can manually log off from the system. An inactive user is automatically logged off after a certain time has elapsed.

### **3.3.3 Logging**

The SAPC sends system-important events to syslog.







## 4 Security Configuration

### 4.1 Network Security Level

#### 4.1.1 Denial of Service Attack Prevention Configuration

So as to prevent Denial of Service (DoS) attacks, the iptables utility can be used. The iptables utility is a framework available in the SAPC, which allows intercepting and manipulating packets. Additionally, not only does iptables filter packets but also it logs any action on the packets handled.

Configuration of iptables utility is described in [LDE Management Guide](#).

### 4.2 Node Security Level

#### 4.2.1 Ericsson Command-Line Interface

Details on how to facilitate the encryption of OAM protocols with TLS can be found at [Security Management for ECLI, NETCONF, and File Transfer Protocols](#).

#### 4.2.2 NETCONF User Management

Details on how defining and configuring the different administrators in the NETCONF domain can be found at [Security Management for ECLI, NETCONF, and File Transfer Protocols](#).

#### 4.2.3 Linux User Management

The SAPC administrators are based on Linux users, which are managed on node level. This means that all servers where the SAPC has been deployed contain the same set of existing administrators. Several procedures for configuring and administering administrators in SAPC can be found at [System Administrator Guide](#).

##### 4.2.3.1 Administrator Password Expiration Policy

The password expiration policy in Linux can be configured with the `chage` command.

For example, to force a user to change their password every 30 days warning the needed change 10 days before, the following command can be used:



```
chage <account> --mindays 0 --maxdays 30 --expiredate -1  
--warndays 10
```

The default password validity of SAPC administrator is infinite days, with password change reminder 10 days before password expiration. The recommended value for the password expiration policy is 30 days.

#### 4.2.3.2 Idle Session Time-out

The idle time-out for any Linux session can be set through editing the `/etc/profile` file and adding the following lines:

— Bash shell

```
# set a 5 min timeout policy for bash shell  
  
TMOUT=300  
  
readonly TMOUT  
  
export TMOUT
```

— Tsch shell

```
# set a 5 min timeout policy for bash shell  
  
autologout=5
```

The recommended value for the idle session time-out is 5 minutes.

To enable the inactivity timer for logon through the SSH interface, edit the `/etc/ssh/sshd_config` file on both SC-1 and SC-2 and add the following text:

```
ClientAliveInterval 1800  
ClientAliveCountMax 0
```

15 minutes is the recommended value.

#### 4.2.3.3 Maximum Number of Failed Logon Attempts

The Maximum Number of Failed logon Attempts for any Linux session can be set through editing the `/etc/ssh/sshd_config` file in both SC and adding the following lines:

```
MaxAuthTries 3
```

The maximum number of failed logon attempts has been set to 3.

The recommended maximum number of failed logon attempts is 3.



#### 4.2.3.4 Password Strength Policy

The password strength policy can be changed by editing the `/etc/pam.d/login` file and adding (if not existing) the following line as required according to the policy rules:

```
password requisite pam_cracklib.so difok=3 maxrepeat=3
retry=3 minlen=8 lcredit=-1 ucredit=-1 dcredit=-1 ocredit=-1
reject_username
```

The recommendation is that the password contains at least one character of the following groups: alpha lower characters, alpha upper characters, numeric characters, punctuation characters (that is, `'?*`').

Refer to the following documentation for more information on the options available: `/usr/share/doc/packages/pam/README.cracklib` , `/usr/share/doc/packages/pam/modules/README.pam_cracklib`.

#### 4.2.3.5 Lockout Period

The lockout period for any administrator account can be set by editing the `/etc/pam.d/common-password` file and adding the following text at the beginning of the auth section in the pam file:

```
auth required pam_tally2.so file=/var/log/tallylog deny=3
even_deny_root unlock_time=1200
```

This locks the root account for 60 seconds and anyone else is locked for 1200 seconds.

The recommended value for the lockout period is 1800 seconds.

#### 4.2.3.6 Emergency Access

Local Linux users belonging to the `com-emergency` Linux group can authenticate locally and get complete Management Information Base (MIB) access through the ECLI and NETCONF interfaces.

To configure a new emergency user, the following procedure is followed in the Linux environment:

1. Log on to one of the system controllers as root: `ssh -l <user> <address>`.
2. Add an emergency account: `useradd -G com-emergency <emergency_user> --home-dir <home_directory>`
3. Assign an initial password for the newly created emergency user: `passwd <emergency_user>`. The system prompts the user to enter a password.
4. Enter a password. The system prompts the user to repeat the selected password.



5. Enter the password again.
6. Allow the user account to log on to all nodes in the cluster by editing the `login.allow` file. Add `<emergency_user>` to the `/cluster/etc/login.allow` file.
7. Check logon permissions for the emergency user: `cat /cluster/etc/login.allow`. The `login.allow` file now also includes the following row:  
`<emergency-user> all`
8. Add the user globally to the cluster: `lde-global-user --user <emergency_user>`
9. Verify that this emergency user works by logging on to the system controller through SSH and through the Northbound Interface (NBI).

#### 4.2.4 Node Log On

When an operator (administrator) attempts to log on to SAPC, the node by default verifies the operator username and password (Individual authentication of OAM accesses). Username and password must be configured by a system administrator. For instruction on configuring username and password, refer to [System Administrator Guide](#).

Configure strong passwords for accessing the SAPC product. Strong passwords are eight or more characters long and consist of a series of upper / lower case letters, numbers, punctuation marks, and special characters. These recommendations are summarized in the following list:

- Force a password change every 30 days for administrative accounts.
- Implement a minimum password length of eight characters consisting of at least one alpha character, one numeric character, and one non-alphanumeric character.
- Configure services to disconnect clients after three invalid logon attempts.
- Implement account lockout where possible: Be aware of potential DoS issues with accounts being locked out intentionally by an attacker.
- Ensure that default accounts such as `root` and `sapcadmin` do not have a default password

**Note:** Change the root password immediately after installation of the SAPC.

##### 4.2.4.1 Disabling remote SSH root login

Remote logon for the root user is enabled by default. Remote logon for the root user can be disabled:

1. Replace the line `ssh.rootlogin control on` with `ssh.rootlogin all off` in `cluster.conf`.



2. Reload the configuration on both SC-1 and SC-2: `cluster config -r -a`

#### 4.2.4.2

#### Enabling remote SSH root logon

If remote logon for the root user has been disabled, remote logon for the root user can be enabled:

1. Connect to either SC-1 or SC-2 (console logon).
2. Replace the line `ssh.rootlogin all off` with `ssh.rootlogin control on` in `cluster.conf`.
3. Reload the configuration on both SC-1 and SC-2: `cluster config -r -a`

## 4.3

## OAM Security Level

### 4.3.1

### Logging

Full personal accountability entails the ability to log watch OAM actions are taken by users logged in to the system. This is accomplished through enabling the Linux auditing framework.

The pam configuration files `/etc/pam.d/common-session-lde` (symlinked from `/etc/pam.d/common-session`) are modified to add the following line:

```
session required pam_tty_audit.so enable=*
```

The common audit dispatch daemon configuration file `/etc/audit/plugins.d/syslog.conf` is modified to contain the following:

```
active = yes

direction = out

path = builtin_syslog

type = builtin

args = LOG_INFO LOG_LOCAL0

format = string
```

Sending the audit logs to syslog local facility 0.

Also, on SLES, the audit daemon configuration file `/etc/audit/audit.rules` is filled with the following content:

```
# First rule - delete all

-D

# Increase the buffers to survive stress events.
```



```
# Make this bigger for busy systems  
-b 320  
  
# Feel free to add below this line. See auditctl man page  
-e 1
```

Which enables the audit daemon.

When logs are written to the syslog, each line typically receives a header consisting of the time stamp and the issuing host/machine that sent the log. To read this logs with aureport for further investigation, one has to remove this header. Recommended way to do this is using sed:

```
$ sed 's/^.*audispd: //' /path/to/log_file > outputfile  
$ aureport --tty -i outputfile
```

## 4.3.2 Certificates Management

The configuration of the certificate to use in a secure communication involving the HTTPS protocol, such as in REST interface, is described in [Certificate Management](#). This document provides instructions on how to install and update any Server Certificate and/or any Client Certificate.

For security reasons, both Server and Client certificates should be updated regularly. A self-signed certificate can be used but intended only for demonstrations or testing environments. Do not use this certificate in a production environment. It is recommended to use a certificate obtained from an external trusted Certification Authority.

There are two ways of generating or installing a self-signed signed certificate:

- A manual procedure, as described in chapter Section 4.3.2.1 on page 18 for generating the certificate , and / or as described in chapter Section 4.3.2.3 on page 23 for installing the certificate.
- An automatic procedure, as described in chapter Section 4.3.2.2 on page 21 for generating the certificate, and / or as described in chapter Section 4.3.2.4 on page 23 for installing the certificate.

Additionally, the operator has the opportunity to generate and install a self-signed certificate in one step, as described in Section 4.3.2.5 on page 24.

### 4.3.2.1 Manual Generation of a self-signed certificate

A self-signed certificate can be generated by the sapcadmin administrator:

1. Generate an RSA private key: `openssl genrsa -out <Key Filename> <Key Size>`



Where:

- <Key Filename> is the desired filename for the private key file
- <Key Size> is the desired key length of either 1024, 2048, or 4096

For example: `openssl genrsa -out my_key.key 2048`

2. Generate a Certificate Signing Request: `openssl req -new -key <Key Filename> -out <Request Filename> -config <config.cnf>`

Where:

- <Key Filename> is the input filename of the previously generated private key
- <Request Filename> is the output filename of the certificate signing request
- <config.cnf> is a file containing the following information:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req
[req_distinguished_name]
countryName = Country Name (2 letter code)
countryName_default = ES
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Spain
localityName = Locality Name (eg, city)
localityName_default = Madrid
organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Ericsson
commonName = <SAPC_VIPP_FQDN> or <SAPC_VIPP_Address> or <SAPC_VIPO_FQDN>
commonName_max = 64
[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names
[alt_names]
IP.1 = <SAPC_VIPP_Address> or <SAPC_VIPO_Address>
```

The following list gives an overview of the fields used in the config.cnf file.

- countryName: This field contains the two-code country code defined in ISO 3166.
- stateOrProvinceName: This field contains the state or province name of the organization which this certificate has been issued to.
- localityName: This field contains the city of the organization which this certificate has been issued to.



- **organizationalUnitName:** This field contains the organization which this certificate has been issued to.
- **basicConstraints:** The basic constraints extension identifies whether the subject of the certificate is a Certification Authority (CA) and how deep a certification path may exist through that CA. For the generation of the self-signed certificate, this field is set to FALSE.
- The values to use in the **keyUsage** field are: **digitalSignature**, **nonRepudiation**, **keyEncipherment**, **dataEncipherment**, **keyAgreement**, **keyCertSing**, **cRLSign**, **encipherOnly**, **decipherOnly**. Depending on the usage of the certificate, the specific value should be used. For the generation of the self-signed certificate, which is aimed to provide encryption to the SAPC clients, the **nonRepudiation**, **digitalSignature** and **KeyEncipherment** should be used.
- **subjectAltName** The subject alternative name extension allows additional identities to be bound to the subject of the certificate (alternative IP Addresses, DNS, etc.). Whenever any additional identity is to be bound into a certificate, the subject alternative name extension must be used. If the subject field contains an empty sequence, the **subjAltName** must contain a valid **subjectAltName**. When the alt name is the only identity used, then the **subjAltName** must be present and the **Subject Name** must be left empty.

**Note:** **subjectAtName** field is optional. It should be included if additional identifies needs including in the certificate.

For example: `>openssl req -new -key my_key.key -out my_request.csr -config config.cnf`

3. Follow the on-screen prompts for the required certificate request information. It is recommended to use a Fully Qualified Domain Name (FQDN) in the CN field of the certificate, or alternatively using an IP address in the **altName** field of the certificate.
4. Create a **v3.ext** file containing the following information:

```
subjectAltName = @alt_names
[alt_names]
IP.1 = <SAPC OAM VIP Address>
```

**Note:** Optional file if FQDN is provided, but mandatory in other case.

5. Generate a self-signed public certificate (X509 v3) based on the request:  
`openssl x509 -req -days 3650 -in <Request Filename> -signkey <Key Filename> -out <Certificate Filename> -extfile <v3_ext Filename>`

Where:

- **<Request Filename>** is the input filename of the certificate signing request





- <Key Filename> is the input filename of the previously generated private key
- <Certificate Filename> is the output filename of the public certificate
- <v3\_ext Filename> is the filename of the file generated at previous step.>

**Note:** The `-extfile v3.ext` option is mandatory if the SAPC FQDN has not been provided, but optional in any other case.

For example: `openssl x509 -req -days 3650 -in my_request.csr -signkey my_key.key -out my_cert.crt -extfile v3.ext`

6. Generate a PKCS#12 file: `openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in <Public Certificate Filename> -inkey <Private Key Filename> -out <PKCS#12 Filename> -name "<Display Name>"`

Where:

- <Public Certificate Filename> is the input filename of the public certificate, in PEM format
- <Private Key Filename> is the input filename of the private key
- <PKCS#12 Filename> is the output filename of the pkcs#12 format file
- <Display Name> is the desired name that will sometimes be displayed in User Interfaces.

For example: `openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in my_cert.crt -inkey my_key.key -out my_pkcs12.p12 -name "SAPC API"`

An example of a self-signed certificate can be found at the following path:

`/cluster/storage/system/software/coremw/repository/ERIC-SAPC_RestServer-CXP9032712_7-R2C53/sapc-demo.p12`

This self-signed certificate is provided as reference, but it cannot be used at production since the certificate was generated using an internal IP of the SAPC cluster as Domain Name (DN).

#### 4.3.2.2

#### Automatic generation of a self-signed certificate

The SAPC provides an easy way to create a simple self-signed certificate that may be used in most of scenarios. The `sapcadmin` administrator can automatically generate the self-signed certificate running the `sapcRestCertificate` script in any of the SCs.

The IP(s) and the DNS can be added to the generated self-signed Certificate depending on the URL used by the client when connecting to the SAPC.



If the URL used for connecting to the SAPC is similar to the following pattern:

```
https://135.203.12.35:8443/provisioning/v1
```

Then the self-signed certificate must be generated using the following command:

```
sapcRestCertificate simple-cert certname -i 135.203.12.35
```

if the URL used for connecting to the SAPC is similar to the following pattern:

```
https://sapc.internal.com:8443/provisioning/v1
```

Then the self-signed certificate must be generated using the following command:

```
sapcRestCertificate simple-cert certname -d sapc.internal.com
```

Where:

- name name of the certificate, name of the files created for this certificate
- -i, --ips comma-separated list of IP(s) for this certificate.
- -d, --dns comma-separated list of DNS for this certificate.

At least one IP or one DNS must be specified. Multiple IP(s) and DNS can be specified at the same time using a comma separate list. For instance,  
**sapcRestCertificate simple-cert certname -d sapc.internal.com,policyserver.local.com -i 135.203.12.35,120.77.56.33**

Further details about the supported options of the sapcRestCertificate script can be obtained using the -h option: sapcRestCertificate -h

An example of the output of the command is shown:

```
sapcadmin@SC-1:~> sapcRestCertificate simple-cert my-cert -d
sapc.internal.com
# Creating self-signing key
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
# Creating certificate
Signature ok
subject=/C=SE/ST=SAPC-Demo-State/L=SAPC-Demo-City/OU=SAPC-Demo-Sec
tion/CN=sapc.internal-com
Getting Private key
# Sign the certificate
Enter Import Password:
Verifying - Enter Import Password:
# Certificate created with files
my-cert.crt
my-cert.pl2
```



```
# Extract the fingerprint
SHA224(my-cert.p12)=
10:20:03:47:34:ec:f6:5a:3f:0d:1c:38:68:13:15:3f:d1:31:7f:6b:ad:38
:5d:50:9a:14:d7:be
```

### 4.3.2.3 Manual Installation of a self-signed certificate

A self-signed certificate or a certificate obtained from a Trusted Certification Authority can be installed by the sapcadmin administrator:

1. Stop the SAPC REST process:
  - Log on to SC-1 as SAPC administrator and execute the command:  
sapcadmin@SC-1:~> **sapcRestServer stop**

**Note:** The sapcRestServer script will log on in to every PL requesting the sapcadmin password at every PL.
2. Delete the current Node Credential for sapc-rest-server, as described in [Delete Node Credential](#).
 

**Note:** Only if a previous certificate has been generated and installed.
3. Create a Node Credential for sapc-rest-server, as described in [Install or Renew Node Credential by PKCS 12](#). The value for the new NodeCredential MO has to be NodeCredential=sapc-rest-server.
4. Start the SAPC REST process:
  - Exit from the ECLI (but maintaining the connection with the SC).
  - Execute the command:  
sapcadmin@SC-1:~> **sapcRestServer start**

**Note:** The sapcRestServer script will log on in to every PL requesting the sapcadmin password at every PL.

Once the certificate is installed, the attribute certificateContent of the NodeCredentialMO contains the X.509 content of the certificate (public key of the certificate), which can be exported to any other client for trusting purposes.

### 4.3.2.4 Automatic installation of a self-signed certificate

Once, the self-signed certificate has been generated, the sapcadmin administrator can automatically install the self-signed certificate running the sapcRestCertificate script in any of the SCs:

```
sapcRestCertificate install my-cert.p12
```

Where my-cert.p12 is the name of the file containing the self-signed certificate, and it can be substituted by the actual name of the generated self-signed certificate.



The following text shows an example of the command output:

```
sapcadmin@SC-1:~> sapcRestCertificate install my-cert.p12
A certificate already exists in the Sapc Provision Server.
If the command continues, the existing certificate will be
overwritten continue? [y/N] y
Enter Import Password:
Verifying - Enter Import Password:
Stopping RestServer in PL-3 ...
Stopping RestServer in PL-4 ...
/usr/local/bin/sapcRestServer action -stop- finished.
Starting RestServer in PL-3 ...
Starting RestServer in PL-4 ...
/usr/local/bin/sapcRestServer action -start- finished.
SUCCESS: installed from the container file
```

#### 4.3.2.5 Automatic generation and installation of a self-signed certificate

Automatic generation and installation of a self-signed certificate can be done at the same time using the following command:

```
sapcRestCertificate simple-cert certname -d sapc.internal.com -I
```

or

```
sapcRestCertificate simple-cert certname -i 135.203.12.35 -I
```

The following text shows an example of the command output:

```
sapcadmin@SC-1:~> sapcRestCertificate simple-cert my-cert -d
sapc.internal.com -I
# Creating self-signing key
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
# Creating certificate
Signature ok
subject=/C=SE/ST=SAPC-Demo-State/L=SAPC-Demo-City/OU=SAPC-Demo-Sec
tion/CN=sapc.internal-com
Getting Private key
# Sign the certificate
Enter Import Password:
Verifying - Enter Import Password:
# Certificate created with files
my-cert.crt
my-cert.p12
# Extract the fingerprint
SHA224(my-cert.p12)=
```



```
63:98:37:d4:0d:41:4d:db:25:c2:9e:5a:38:3e:93:fe:3b:60:3c:c7:d9:15
:e4:ca:e2:56:1a:f3
# Install the certificate
Stopping RestServer in PL-3 ...
Stopping RestServer in PL-4 ...
/usr/local/bin/sapcRestServer action -stop- finished.
Starting RestServer in PL-3 ...
Starting RestServer in PL-4 ...
/usr/local/bin/sapcRestServer action -start- finished.
SUCCESS: installed from the container file
```

### 4.3.3 Recommended Periodic Operations

The following activities are recommended to be done regularly (weekly or monthly):

- Take System Backups monthly.
- Take a User Data backup after having modified the subscription database.
- Run password checkers periodically, for example, John the Ripper, with word lists to find weak passwords.
- Monitor periodically file system integrity using tools for such purpose (that is, Tripwire), either manually or as a scheduled task.
- Ensure that no unnecessary services are running.
- Ensure that no unnecessary listening open ports are open.
- Ensure that the ports for the insecure protocols Telnet and FTP are closed.
- Ensure that no share administration accounts are used.
- Ensure that administrator rights are assigned only to real needs.
- Ensure that audit for accountability is set up properly.

### 4.3.4 Handling of Patches

Patches to security vulnerabilities and alerts are delivered in the form of Correction Packages (CP) or Emergency Packages (EP).





## 5 Security in the Cloud

The Virtual SAPC is only deployed in trusted clouds to protect security information contained in it and to avoid information leakage to non-authorized third parties.

The following requirements are applicable when deploying the SAPC in the Cloud:

- The cloud infrastructure shall protect memory locations where the Virtual SAPC Virtual Machine is deployed inside the cloud. For this reason, the cloud infrastructure shall provide enough tenant isolation security measures.
- The cloud infrastructure shall provide hardware rooted security mechanisms (TPM, vTPM, HSM).
- It is assumed that the perimeter L2 and L3 firewalls / switches, which are deployed by the cloud infrastructure, can deny incoming IP traffic with the VLAN encapsulation.
- Any 3PP included in the cloud infrastructure shall be tested / verified, checking that they do not contain any Vulnerability / Risk.
- The cloud infrastructure shall provide a means for the user to specify the bindings used for all listening services. The cloud infrastructure shall support binding to any address or net-block associated with any interface local to the node. This shall include addresses bound to physical or non-physical (for example, loopback) interfaces.
- The cloud infrastructure shall separate the different IP-based traffic types (for example, OAM, control plane, data storage, and user plane traffic) by dedicating a logical or a physical network interface for each of them.
- The cloud infrastructure shall provide a means to disable processing of all packets utilizing IP Options. This option shall be available on a per-interface basis. It shall be possible to individually configure which options are processed.
- The cloud infrastructure shall have the ability to introduce an anti-malware solution that protects against viruses, worms, Trojans, and spyware.
- A proper DoS protection in the cloud environment is assumed to be present for application secure functioning in the cloud.

The following recommendations shall be provided to prevent any kind of DoS or (D)DoS attack from happening:

- Rate limiting per vDC.
- Domain separation within the cloud.
- The cloud infrastructure shall provide Network Element authentication.



- The cloud infrastructure shall provide OAM Server authentication.
- The cloud infrastructure shall provide the capability to log all security relevant events to a security event log to track any security activity performed on the Virtual SAPC.
- The cloud infrastructure shall provide the operator with a security event logon Syslog format. If the original, native log format is other, it shall be possible to output the security event logon Syslog format.
- The cloud infrastructure shall support transmission of security event logs over protected protocols to one or more remote OAM servers for permanent secure storage or for further analysis.
- The cloud infrastructure shall protect the confidentiality and data integrity of the OAM traffic.
- The cloud shall protect the confidentiality and data integrity of the control plane traffic.
- The cloud infrastructure, when providing encryption for securing the management traffic, shall use key lengths and algorithms “strong” by current definitions.
- The cloud infrastructure shall provide capabilities for secure key generation, distribution, storage, replacement/recovery, and discontinuation.
- The cloud shall protect the confidentiality and data integrity of the data storage traffic by cryptographic means.





## 6 Default Parameter Values

The default values for the security parameters are listed in the following table:

Table 1 Parameters and Default Values

Parameter	Default Value
Minimum Password Age	0
Maximum Password Age	99999
Password Expiration Warning	7
Password Inactive	-1
TMOUT	0
ClientAliveInterval	0
ClientAliveCountMax	3
MaxAuthTries	6





## 7 Services, Ports, and Protocols

Keep the number of open ports in the SAPC to the minimal necessary for the node to be operational.