

Security and Privacy Management

Ericsson Dynamic Activation 1

SECURITY INSTRUCTIONS

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 Groups	1
1.3	Typographic Conventions	1
2	Overview	1
3	Network Security Configuration	2
3.1	Allowed Ports	2
3.2	Switch and Router Configuration for Native Deployment	2
3.3	VM Network Configuration for Virtual and Cloud Deployment	3
4	User Management	3
4.1	System Users	3
4.1.1	Locking Mechanism	4
4.1.2	User Policies	5
4.1.3	Password Expiration Policy	6
4.1.4	Password Strength Policy	7
4.2	Dynamic Activation Users	7
4.2.1	GUI Users	7
4.2.2	External GUI Users	7
4.2.3	Provisioning Clients	8
4.3	General Password Recommendations	8
5	Log Files	9
6	Configuring Firewall and IPtables Rules	9
6.1	Activating and Deactivating - Native Deployment Only	9
6.2	Custom IPtables Rules - Native Deployment Only	10
6.3	IPtables - Virtual and Cloud Deployment Only	10
7	Certificate Handling	12
7.1	Configuring SSL	13
8	Privacy	14
8.1	Notice	14
8.2	Consent	14



Reference List

15



1 Introduction

This document provides a description for the security functions available in the nodes of Ericsson Dynamic Activation (EDA).

1.1 Purpose and Scope

The purpose of this document is to provide an overview on the Dynamic Activation security functions available in the nodes, and describe the guidelines of configuring the system to the security level requested by Dynamic Activation operators.

1.2 Target Groups

The target groups for this document are as follows:

- Network Administrator
- System Administrator
- Application Administrator
- Network Supervision Administrator

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

1.3 Typographic Conventions

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

2 Overview

This document provides instructions on how to secure Dynamic Activation network interfaces and the Dynamic Activation node itself, to protect the system from malicious attacks and prevent unauthorized access to the system, and connected network elements.



The document offers security guidelines for the following topics:

- Network configuration.
- Node administration and user management.
- SSL/SSH traffic encryption and authentication.

The topics listed above are described in the following sections in more detail.

This document also provides the Dynamic Activation privacy-related statements.

3 Network Security Configuration

This section describes, in a security aspect (by use of VLAN, and traffic separation), the external connectivity configuration between Dynamic Activation and external customer network. For further information about external connectivity, refer to section **Networks** in *Network Description and Configuration for Virtual and Cloud Deployment*, Reference [2] for Virtual and Cloud deployment, or section **Networks** in *Network Description and Configuration for Native Deployment*, Reference [3] for Native deployment (using GEP3 or GEP5 blades).

3.1 Allowed Ports

For information about the different ports to use, refer to *System Administrators Guide for Native Deployment*, Reference [8] for Native deployment, or *System Administrators Guide for Virtual and Cloud Deployment*, Reference [9] for Virtual and Cloud deployment.

3.2 Switch and Router Configuration for Native Deployment

The System Control Switch Board (SCXB) can be configured by means of a Secure Shell (SSH) interface. If needed consult the next level of maintenance support.

For information about how to configure the switches and the routers, see *Network Description and Configuration for Native Deployment*, Reference [3].



3.3 VM Network Configuration for Virtual and Cloud Deployment

For information about how to configure the Virtual Machines (VMs) in a Virtual environment, see section **Physical and Logical Network Setup in Network Description and Configuration for Virtual and Cloud Deployment**, Reference [2].

4 User Management

Dynamic Activation offers the following user management tools from a security perspective:

- Linux Distribution Extensions (LDE) user management.
- Router and the switch user management.
- Remote user authentication management.
- Red Hat Enterprise Linux (RHEL).

These tools are described in the following sections, in more detail.

4.1 System Users

The following are the default system users for Dynamic Activation:

- `actadm` - belongs to the group `activation` and is used for administering Dynamic Activation.
- `dvecli` - belongs to the group `activation` and is used for fetching massive result-files.
- `casadm` - belongs to the group `activation` and is used for administering the Cassandra database.
- `zooadm` - belongs to the group `activation` and owns the ZooKeeper application.
- `syncuser` - belongs to the group `activation` and is used for synchronization of license counters and configurations by SFTP.



Note: For Native Deployment, the system users can be administered with LDE operations. For more information on LDE, refer to **LDE Management Guide**, Reference [4].

For Virtual and Cloud Deployment, the system users can be administered with RHEL operations. For more information about System User handling, see *Hardening Guideline for Virtual and Cloud Deployment*, Reference [10].

4.1.1 Locking Mechanism

For detailed information about Locking Mechanism, refer to *System Administrators Guide for Native Deployment*, Reference [8] for Native deployment, or *System Administrators Guide for Virtual and Cloud Deployment*, Reference [9] for Virtual and Cloud deployment.

4.1.1.1 Locking Mechanism Native Deployment

Failed login attempts for the all system users are logged in `/var/log/<hostname>/auth` on the SC node and in `/var/log/auth` on each server.

If too many sequential login attempts fail, the user is locked and an event is raised. For more information about alarms and events, refer to *Event and Alarm Handling*, Reference [5].

To view the failed login attempts status of a user, enter the following command as user `root`:

```
# pam_tally2 --file /home/faillog
```

If a user is locked, it can be unlocked by entering the following command as user `root`:

```
# pam_tally2 --file /home/faillog --user <user_name> --reset
```

The number of unsuccessful login attempts required before an event is raised can be edited in the files `/etc/pam.d/common-auth` and `/etc/pam.d/common-account`

Change the value of the parameter `deny=<deny_value>`

Caution!

A customer adaptation will be needed to make the configuration changes persistent and not lost on reboot.



4.1.1.2 Locking Mechanism Virtual and Cloud Deployment

Failed login attempts for the all system users are logged in `/var/log/secure` on each Virtual Machine (VM).

If too many sequential login attempts fail, the user is locked and an event is raised. For more information about alarms and events, refer to *Event and Alarm Handling*, Reference [5].

To view the failed login attempts status of a user, enter the following command as user `root`:

```
# pam_tally2
```

If a user is locked, it can be unlocked by entering the following command as user `root`:

```
# pam_tally2 --user <user_name> --reset
```

The number of unsuccessful login attempts required before an event is raised can be edited in the file `/etc/puppet/modules/pam_tally2/files/password-auth-ac`

Change the value of the parameter `deny=<deny_value>`

Note: This must be performed on the puppet master node. Check `/etc/hosts` on any node to find the puppet master.

Caution!

A customer adaptation will be needed to make the configuration changes persistent and not lost on reboot.

4.1.2 User Policies

Dynamic Activation offers several user account settings to enhance the security of session establishment. The steps for configuring these settings are described in the following sub-sections.

4.1.2.1 Configuring Idle Session Timeout

The following options control the time-out of SSH sessions. These can be added to `/etc/ssh/sshd_config`:

- `ClientAliveInterval` (recommended: 300)
- `ClientAliveCountMax` (recommended: 0)



Caution!

A customer adaptation will be needed to make the configuration changes persistent and not lost on reboot.

4.1.2.2

Configuring the Maximum Number of Failed Login Attempts

For Native deployment:

For details on password creation parameters used for Native deployment, refer to *Hardening Guideline for Native Deployment*, Reference [11].

Default is 10 retries allowed.

For Virtual and Cloud deployment:

Set the `pam_pwquality.so` parameters as follows in `/etc/pam.d/system-auth`:

```
password requisite pam_pwquality.so  
try_first_pass local_users_only retry=3 authtok_type=
```

`try_first_pass` - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.

`retry=3` - allow three tries before sending back a failure.

Caution!

A customer adaptation will be needed to make the configuration changes persistent and not lost on reboot.

4.1.3

Password Expiration Policy

For Native deployment:

For information on how to configure password aging for system users, refer to **LDE Management Guide**, Reference [4].

For Virtual and Cloud deployment:

For information on how to configure password aging for system users, refer to https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Security_Guide/index.html, Reference [12].



4.1.4 Password Strength Policy

When new user accounts are created, the Dynamic Activation system applies the default password settings on them. It is recommended to configure the password strength according to the desired behavior by following the instructions in *Hardening Guideline for Native Deployment*, Reference [11] for Native deployment, or *Hardening Guideline for Virtual and Cloud Deployment*, Reference [10] for Virtual and Cloud deployment.

4.2 Dynamic Activation Users

From both perspectives of administration and authentication, GUI Users and Provisioning Clients are separated. Two different sets of password rules are applied independently.

4.2.1 GUI Users

A GUI user is a human user that uses one or more GUI applications in Dynamic Activation.

Dynamic Activation GUI users can be administered through the **User Management** GUI. For the details, refer to *User Guide for Resource Activation*, Reference [6].

A default System Administrator user `admin` is created at installation. This user cannot be deleted or locked out, and is protected by a Brute Force Protection Algorithm.

Password rules of the GUI users and input parameters of the Brute Force Protection Algorithm are administrated as `bootloader` parameters. For more information, refer to:

- *System Administrators Guide for Native Deployment*, Reference [8]
- *System Administrators Guide for Virtual and Cloud Deployment*, Reference [9]

All login events and user management events of GUI Users are logged in `/var/log/dve/oauth.log`.

4.2.2 External GUI Users

An external GUI user is a human user that is administrated in external OpenID Connect Provider. External GUI users can log in Dynamic Activation and use one or more GUI applications in Dynamic Activation. For more information, refer to the following documents:

- *User Guide for Resource Activation*, Reference [6]



- *User Guide for Resource Configuration*, Reference [7]

Failed login attempts for Dynamic Activation users can be logged by external OpenID Connect Provider. For more information, refer to documents in related OpenID Connect Provider product.

4.2.3 Provisioning Clients

A provisioning client is an entity that initiates provisioning requests towards Dynamic Activation. For example, an OSS/BSS system, an in-house tool/script, a network element, embedded provisioning tool such as Batch Handler.

Provisioning Clients can be administered through the **Operation & Management>Access Control** GUI.

Password rules for the provisioning clients are administered through **Operation & Management>System>Options** GUI.

For the details, refer to *User Guide for Resource Activation*, Reference [6].

Failed login attempts for Dynamic Activation users are logged in `/var/log/dve/tomcat-server-audit.log`

Note: Native deployment:

On the SC nodes, for the GUI, the respective `dve-<module_name>-audit.log` is created the first time a failed login attempt is performed.

On the PL nodes, for inbound interfaces (MML, CLI, CAI, and CAI3G), the respective `dve-<module_name>-audit.log` is created the first time a failed login attempt is performed.

Virtual and Cloud deployment:

On each VM, for the GUI, the respective `dve-<module_name>-audit.log` is created the first time a failed login attempt is performed.

On all VMs, for inbound interfaces (MML, CLI, CAI, and CAI3G), the respective `dve-<module_name>-audit.log` is created the first time a failed login attempt is performed.

4.3 General Password Recommendations

Dynamic Activation users are strongly advised to abide by the following password handling recommendations:

- Keep passwords confidential.
- Avoid keeping record of the passwords either on paper, or in digital format (such as in software files, hand-held devices, and so on), unless the list can be stored securely, and it has been approved to do so.



- Change passwords whenever there is any indication that the system or a password is compromised.
- Do not include passwords in any automated logon process (for example stored in a macro or function key), unless it is strictly necessary.
- Use the lowest level access account to perform an action. For example, do not use the `root` account unless the action requires `root` access.
- If shared accounts are used, users must login with their own account, and then switch to the user account (such as the `root` user) that must be used to perform an action. User switch is initiated with the `su` or `sudo` command.

5 Log Files

For information about different log files in the Dynamic Activation system, refer to section **Log Files** in *System Administrators Guide for Native Deployment*, Reference [8] for Native deployment, or *System Administrators Guide for Virtual and Cloud Deployment*, Reference [9] for Virtual and Cloud deployment.

6 Configuring Firewall and IPtables Rules

This section describes the basic firewall operations and IPtables Rules for both Native, Virtual and Cloud deployment.

6.1 Activating and Deactivating - Native Deployment Only

Note: The firewall is activated by default on all nodes. The firewall applies to all external interfaces parsed from `cluster.conf` and is automatically appended to `iptables-rules.cfg`

To activate the firewall on a node, enter the following command as user `root`::

```
# /etc/init.d/firewall start
```

To deactivate the firewall, enter the following command as user `root`::



```
# /etc/init.d/firewall stop
```

6.2 Custom IPtables Rules - Native Deployment Only

Custom iptables rules are supplied by `/home/actadm/config/iptables-rules-custom.cfg` and are automatically appended to the existing iptables rules upon activation of the firewall.

Refer to the `/home/actadm/config/iptables-rules-custom.cfg.example` file.

Example on how to add custom iptables rules.

As user `root`:

```
# /etc/init.d/firewall stop
```

```
# sudo -u actadm cp /home/actadm/config/iptables-rules-custom.cfg.example /home/actadm/config/iptables-rules-custom.cfg
```

Edit `/home/actadm/config/iptables-rules-custom.cfg` accordingly.

Restart the firewall:

```
# /etc/init.d/firewall start
```

The following printout is displayed:

```
Starting iptables firewall
Appending custom iptables
```

6.3 IPtables - Virtual and Cloud Deployment Only

This section describes the basic IPtables configuration.

The IPtables configuration is managed by Puppet and changes are done in the Puppet module.

To print all active IPV4 rules, login as an administrator and run the following command as user `root`:

```
# iptables -L -vn
```

To print all active IPV6 rules, login as an administrator and run the following command as user `root`:

```
# ip6tables -L -vn
```



To add or delete a port in IPtables, login as user `root` or puppet user and edit the firewall config file:

```
# vi /etc/puppet/modules/firewall/files/config/iptables-
pg-product-rules.cfg
```

Example

This is an example of adding an IPV4 rule to accept a new port 3011.

As user `root`:

1. Print the current IPV4 rules:

```
# iptables -L -vn

...
..
.
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:70
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:30
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:90
0      0 DROP        all -- *      *      0.0.0.0/0      0.0.0.0/0
.
..
...
```

2. On node-1, which is the puppet master, open the firewall config file to edit.

```
# vi /etc/puppet/modules/firewall/files/config/iptables
-pg-product-rules.cfg
```

3. Add a line in the firewall config file and save the change.

```
# -A input_ext -p tcp -m tcp --dport 3011 -j ACCEPT
```

4. Print all IPV4 rules again. A new rule is listed in the IPtable to allow the new port.

Note: It can take up to 30 seconds for the new port to be added.

```
# iptables -L -vn

...
..
.
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:70
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:30
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:30
0      0 ACCEPT      tcp -- *      *      0.0.0.0/0      0.0.0.0/0      tcp dpt:90
0      0 DROP        all -- *      *      0.0.0.0/0      0.0.0.0/0
.
..
...
```

7 Certificate Handling

Certificates are generated to secure and encrypt communication on interfaces used in Dynamic Activation. Interfaces used for internal communication among Dynamic Activation components are encrypted using certificates and Transport Layer Security (TLS) 1.2, as shown in Figure 1.

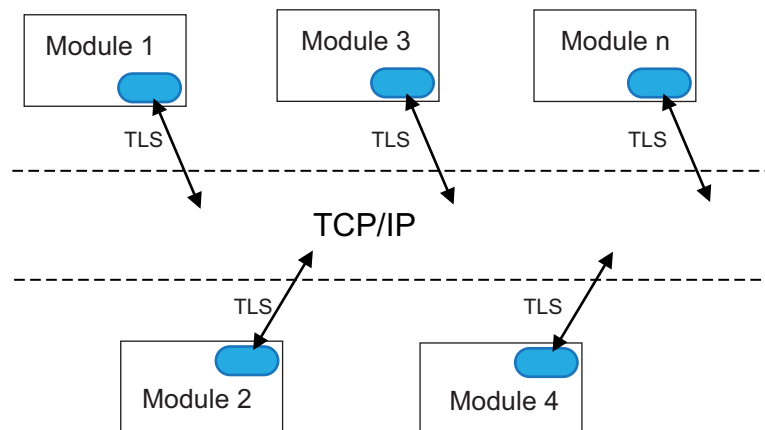


Figure 1 Internal Communication

For external interfaces shown in Figure 2, there is a default self-signed certificate that can be used for all northbound interfaces. If necessary, the self-signed certificate can be replaced by a signed certificate.

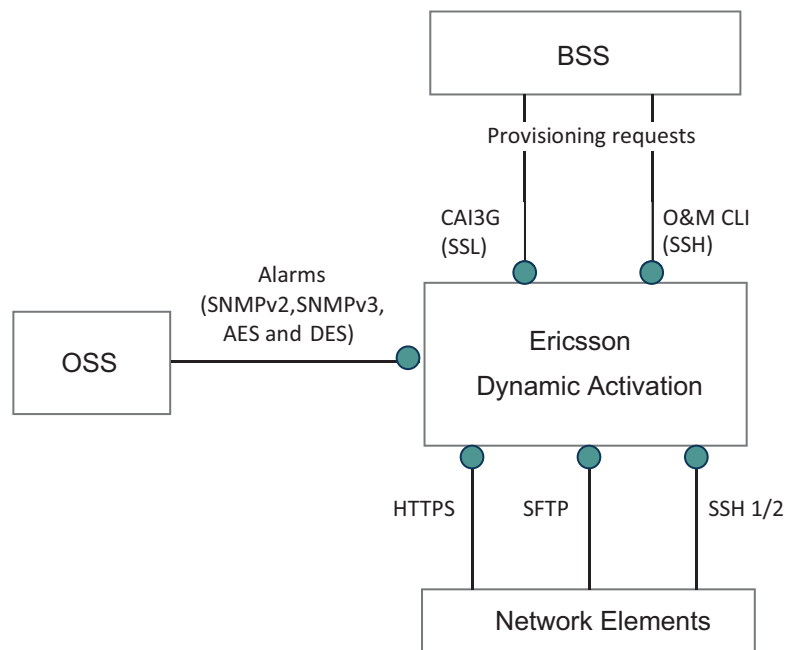


Figure 2 Secured External Interfaces



The external interface used for communication between the OSS and Dynamic Activation can use Advanced Encryption Standard (AES) or Data Encryption Standard (DES) for encryption.

Certificates can also be used on southbound communication protocols supporting it.

Interface used for external OpenID interface between Dynamic Activation and OpenID Connect Provider is encrypted using certificates, as shown in Figure 3.

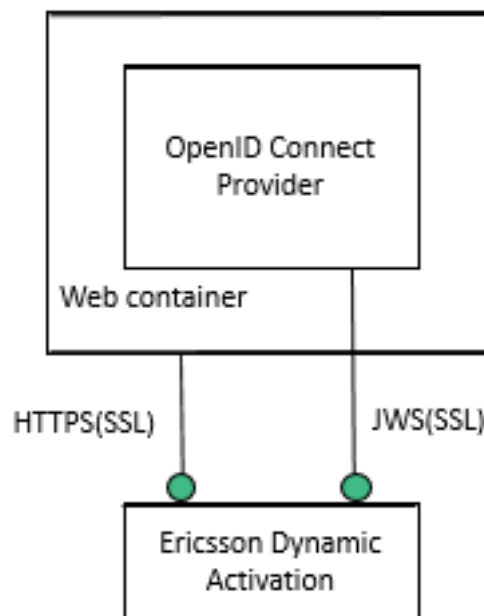


Figure 3 External OpenID Interface

7.1 Configuring SSL

For information about how to configure SSL, refer to section **Configuring SSL** in *System Administrators Guide for Native Deployment*, Reference [8] for Native deployment, or *System Administrators Guide for Virtual and Cloud Deployment*, Reference [9] for Virtual and Cloud deployment.



8 Privacy

This section contains privacy-related statements regarding the Dynamic Activation system.

8.1 Notice

Dynamic Activation may store personal information, and may impact the right to privacy of the data subjects (that is, subscribers) whose data is stored. The specific data items to be stored depend on the application(s)/operators using the Dynamic Activation system.

When operating the Dynamic Activation system as a data controller, ensure that personal information is stored in a fair and lawful manner, and in accordance to the local data protection regulation in effect. This can be achieved by providing notice to the subscribers about the privacy policies of the operator, for example at the moment of establishing the subscription.

It is also advised to provide comprehensive and understandable information to subscribers prior to, or at the time of collecting the personal information.

8.2 Consent

Dynamic Activation may also store sensitive personal data in addition to basic personal data. The local data protection regulations where Dynamic Activation is operated may require obtaining subscriber consent to process this kind of personal information. Such consent must be obtained to allow the following activities:

- Collecting and maintaining personal data of the subscriber, aimed at holding securely this information.
- Fulfilling the purpose of installing, upgrading, and administrating the Dynamic Activation system.
- Disclosing personal information to third parties.



Reference List

- [1] *Library Overview*, 18/1553-CSH 109 628 Uen
- [2] *Network Description and Configuration for Virtual and Cloud Deployment*, 1/1551-CSH 109 628 Uen
- [3] *Network Description and Configuration for Native Deployment*, 2/1551-CSH 109 628 Uen
- [4] *LDE Management Guide*, 1/1553-CAA 901 2978/1 Uen
- [5] *Event and Alarm Handling*, 3/1553-CSH 109 628 Uen
- [6] *User Guide for Resource Activation*, 1/1553-CSH 109 628 Uen
- [7] *User Guide for Resource Configuration*, 11/1553-CSH 109 628 Uen
- [8] *System Administrators Guide for Native Deployment*, 1/1543-CSH 109 628 Uen
- [9] *System Administrators Guide for Virtual and Cloud Deployment*, 3/1543-CSH 109 628 Uen
- [10] *Hardening Guideline for Virtual and Cloud Deployment*, 2/154 43-CSH 109 628 Uen
- [11] *Hardening Guideline for Native Deployment*, 1/154 43-CSH 109 628 Uen

Other References

- [12] *Red Hat Enterprise Linux 7 - Security Guide*, https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html-single/Security_Guide/index.html