

Software Installation for Native Deployment

Ericsson Dynamic Activation 1

INSTALLATION INSTRUCTION

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	Typographic Conventions	1
1.2	Prerequisites	1
2	Installation Process	3
3	Installation	5
3.1	Prerequisites for Installing Dynamic Activation	5
3.2	Installing Software	5
3.2.1	Installation Verification	8
3.2.2	Installing HSS Validator Plug-in (Optional)	8
3.2.3	Creating Administrative Users	9
3.2.4	SSL Configuration (Optional)	9
3.2.5	Configurations	9
3.2.6	Modify Notification Rules (Optional)	9
3.2.7	Set Initial License Counters	10
3.2.8	External OpenID Connect Provider Configuration (Optional)	10
3.3	SNMP Configuration	10
3.4	Backup	10
4	Update and Rollback	11
4.1	Update Preparations	11
4.2	Update Instructions	12
4.2.1	All Nodes with Downtime	12
4.2.2	Node by Node without Downtime	13
4.2.3	Upgrade LDEwS and Evip	15
4.3	Rollback Instructions	16
5	Uninstall	17
5.1	Uninstallation of Software	17
	Reference List	19





1 Introduction

This document contains instructions regarding how to install the Ericsson Dynamic Activation (EDA).

1.1 Typographic Conventions

Typographic conventions are described in the document *Library Overview*, Reference [7].

For information about abbreviations used throughout this document, refer to *Glossary of Terms and Acronyms*, Reference [1].

1.2 Prerequisites

The following are the prerequisites to make full use of this document:

- Make sure to check the Delivery Report before using this document. The Delivery Report contains information about known problems, limitations and exceptions related to the system software that will be installed. It can contain complementary instructions and information, that may prevent system failure and damage.
- To get an overview of the system and deployment scenarios, see *Product Overview*, Reference [9].
- The documents *Customer Questionnaire for Native Deployment*, Reference [14], and *Parameter List for Native Deployment*, Reference [15] are available with all values of the installation parameters.





2 Installation Process

This section gives an overview of the whole installation process, from setting up the hardware to installing and configuring Dynamic Activation.

Table 1. lists the installation steps (both for GEP3 and GEP5), including an estimation of the time needed to perform them.

Table 1 Installation Process Using GEP3 or GEP5

Installation Step	Time Estimation
Configuring Installation/Kickstart Server	Customer environment dependent: About two hours If using GEP5, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5</i> , Reference [3]. If using GEP3, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3</i> , Reference [2].
Installing BSP, SCX, and CMX	About two hours If using GEP5, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5</i> , Reference [3]. If using GEP3, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3</i> , Reference [2].
BSP Configuration	About one hour If using GEP5, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5</i> , Reference [3]. If using GEP3, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3</i> , Reference [2].
Installing Linux Distribution Extensions (LDE)	Cluster environment: About two hours If using GEP5, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5</i> , Reference [3]. If using GEP3, refer to <i>Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3</i> , Reference [2].
Installing evip	Less than 15 minutes For details, refer to Section 3.2 on page 5.
Installing Dynamic Activation Software	Less than 30 minutes. For details, see Section 3.2 on page 5.
SNMP Configuration	For details, see Section 3.3 on page 10.
Backup	For details, refer to <i>Backup and Restore Guideline for Native Deployment</i> , Reference [10]





3 Installation

This section covers how to install the software to be used for Dynamic Activation.

3.1 Prerequisites for Installing Dynamic Activation

This section lists the Dynamic Activation installation prerequisites:

- Installation of the Dynamic Activation software requires the hardware and operating system to be installed and configured.

If using GEP3, refer to *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [2].

If using GEP5, refer to *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [3].

- Make sure to have a valid Dynamic Activation 1 license in Ericsson License Information System (ELIS).
- Make sure to have the system software accessible (EDA System Base SW).
- If a Validator Plug-in is to be used (optional), make sure to have the HSS Validator Plug-in software accessible.

Contact [Ericsson support](#) for details about the applicable HSS Validator Plug-in version.

- Make sure the evip configuration file, `evip.xml`, has been prepared. See section **Installation and Configuration** in *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [2] if using GEP3 or, if GEP5, section **Installation and Configuration** in *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [3].

3.2 Installing Software

This section contains instructions on how to install the software.

Note: Check that the prerequisites are fulfilled, as stated in Section 3.1 on page 5.

Installation of Dynamic Activation is performed as user `root`.

On the first control node (SC1):



1. Create the `/var/log/installfiles/` directory:

```
# mkdir -p /var/log/installfiles/
```

2. Transfer the software package (EDA System Base SW) to the `/var/log/installfiles/` directory. For example, by using SFTP.

3. Change directory:

```
# cd /var/log/installfiles/
```

4. Untar the software package (EDA System Base SW):

```
# tar -zxvf <Software_Package>.tar.gz
```

5. Change directory:

```
# cd <Prod_Number>-<Version>
```

6. Obtain the license locking codes for the system.

From SC-1:

```
# /var/log/installfiles/<Prod_Number>-<Version>/ema  
licenseCodes
```

Output:

```
INFO - *** Locking codes for <SC-1>:
```

```
INFO - ***
```

```
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Inform  
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1NE URGH T85R V4K4
```

```
Locking Code 1 (Old Style) : 2008-292BD
```

```
INFO - *** Locking codes for <SC-2>:
```

```
INFO - ***
```

```
Sentinel RMS Development Kit 8.6.2.0053 Host Locking Code Inform  
Copyright (C) 2015 SafeNet, Inc.
```

```
Locking Code 1      : 2008-*1PW 65F3 8ABD KJET
```

```
Locking Code 1 (Old Style) : 2008-66063
```

7. Provide all Locking Code for the Ericsson License Information System (ELIS) and get the license file.



8. Untar the `evip` package:

```
# tar -xvf evip/<Prod_Number>-<Rev>.sdp -C evip/
```

9. Change directory:

```
# cd evip
```

10. Copy the `evip.xml` file, that was previously prepared, to the `/var/log/installfiles/<Prod_Number>-<Version>/evip/` directory. For information about this preparation, refer to section **Configuration File Preparation** in *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP3*, Reference [2] if using GEP3, or if using GEP5, section **Configuration File Preparation** in *Hardware Installation and IP Infrastructure Setup for Native Deployment GEP5*, Reference [3].

11. Install the `evip` package:

```
# ./bundle install_standalone evip.xml
```

12. Reboot the cluster:

```
# cluster reboot --all
```

13. Check the network setup. For instructions, see section **Network Setup Check** in *System Administrators Guide for Native Deployment*, Reference [5].

14. Transfer (SFTP) the license file to the `/var/log/installfiles/` directory on SC1, and rename the file to `license.txt`. This will automatically install all license files when running the `./ema install -p EMA` script.

Note: It is possible to proceed with the installation without installing the licenses at this stage. If this is the case, the licenses need to be manually installed at a later occasion. For detailed information on how to manually install the licenses, see section **License Administration** in *System Administrators Guide for Native Deployment*, Reference [5].

15. Install the software:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema install -p EMA
```

16. Run the following command to receive the environment variables:

```
# su -
```

17. Installation is completed.



3.2.1 Installation Verification

Follow below instruction for information on how to verify the installation.

1. On SC1, check that there are no errors and failed parts in the installation logs:

```
# grep -Ei "RPM_Install.*(error|failed)" /var/log/*/messages
```

```
# grep -Ei "error|failed" /var/log/ema/*.log
```

3.2.2 Installing HSS Validator Plug-in (Optional)

This section contains information on how to install the HSS Validator Plug-in.

1. Make sure to have the correct Plug-in available.
 - If the file to download has `.tgz` as filename extension, it needs first to be unzipped, and then zipped again as `tar.gz` before renaming it.
 - The file needs to have the name `<HSS Plugin>-<R-state>.tar.gz`, for example `HssProvisioningValidator-R4A.tar.gz`. If it does not, it needs to be renamed.
 - The correct `<R-state>` version is found in the `tar.gz` file, on `.jar` level.
2. Copy the HSS Validator Plug-in software to the `/home/bootloader/repository/` directory on one of the SC nodes.

3. Change owner and group of the HSS Plug-in file.

```
# chown actadm:activation /home/bootloader/repository/<HSS Plugin>-<R-state>.tar.gz
```

4. From an SC node, run the following command for all PL nodes in the cluster, one by one, to add the plug-in as submodule.

For example, on a four node cluster it is the `<hostname>` of nodeId 3 and 4, on a six node cluster it is the `<hostname>` of nodeId 3, 4, 5 and 6:

```
# bootloader.py submodule add -n <HSS Plugin>-<R-state>.tar.gz -t lib-ext -p dve-application --host <hostname>
```

`<hostname>` is the hostname of the PL node to which the submodule is being added.

5. From an SC node, run the following command for all PL nodes, one by one, to activate the plug-in as submodule.



Attention!

Wait for each PL node to be activated before starting with the next one, otherwise traffic disturbances occur. The `all` parameter should only be used when no provisioning traffic is running.

```
# bootloader.py node activate --host <hostname>
```

`<hostname>` is the hostname of the PL node to which the submodule is being activated.

3.2.3 Creating Administrative Users

Create non-root users for administering purposes, such as log file reading, process monitoring, managing Dynamic Activation processes, installation of modules, and more. For information on how to create administrative users, see section **Users > Create Administrative User** in *System Administrators Guide for Native Deployment*, Reference [5].

3.2.4 SSL Configuration (Optional)

For information on how to configure SSL, follow the instructions in *System Administrators Guide for Native Deployment*, Reference [5].

3.2.5 Configurations

Before Dynamic Activation is fully operational, the different application services need to be configured. Refer to *Configuration Manual for Resource Activation*, Reference [8].

For information on how to import the default NE groups and routing methods to the Dynamic Activation system, refer to **Load Default NE Groups and Routing Methods** in *System Administrators Guide for Native Deployment*, Reference [5].

For information on exchange of SSH keys between Dynamic Activation clusters to enable synchronization of license counters and configuration between clusters, refer to *System Administrators Guide for Native Deployment*, Reference [5].

3.2.6 Modify Notification Rules (Optional)

For HSS and DAE provisioning, the application notification rules files need to be deployed to Dynamic Activation in order to send the notification message to the relevant FE. The application notification rules file needs to be retrieved from each application.



For more information, refer to section **Notification Rules File Administration** in *System Administrators Guide for Native Deployment*, Reference [5].

3.2.7 Set Initial License Counters

Note: This section is only valid when migrating subscribers from monolithic NEs to User Data Consolidation (UDC).

For more information, refer to *License Counter Management*, Reference [12].

3.2.8 External OpenID Connect Provider Configuration (Optional)

For information on how to configure External OpenID Connect Provider, follow the instructions in *System Administrators Guide for Native Deployment*, Reference [5].

3.3 SNMP Configuration

This section includes information on SNMP protocol configuration.

For information on how to configure SNMP, refer to section about **Configuring ESA** in *System Administrators Guide for Native Deployment*, Reference [5].

3.4 Backup

When the system is installed and properly configured, make a full backup to be able to revert to the original state when needed. Create a full backup as described in *Backup and Restore Guideline for Native Deployment*, Reference [10].



4 Update and Rollback

Note: Update of the Dynamic Activation software is performed as user `root`.

An update is an upgrade of all RPMs and modules on the current system to a newer software version, for example update the software to a new Correction Package (CP) or Product Customization Package (PC).

Note: Check the **Delivery Report** for details about supported update paths. Contact [Ericsson support](#) for further instructions.

The update is proceeded node by node without downtime, or all nodes at once, with downtime. If any previously modified configuration files are affected by the update, they may need to be modified again.

To see if a configuration file is replaced in platform RPMs, and where the backup of the original file is placed, look in the `/home/actadm/config/log/config.log` file. Search for `<date>` [INFO] Replacing `<file>` with new config file, and `<date>` [INFO] Backing up `<file>` to `<file>`.

To see if a configuration file is replaced in the software modules, and where the backup of the original file is placed, look in the `/home/bootloader/config/module_config_files/log/config.log` file. Search for `<config file>` replaced due to new original file, old file renamed to `<config file>.save`

Note: If the installed LDEwS or evip are not on the correct software level, the whole cluster needs to be rebooted. This will result in downtime.

If a Validator Plug-in is to be used (optional), make sure to check needed applicable version.

Contact [Ericsson support](#) for details about the applicable HSS Validator Plug-in version.

New provisioning features need to be configured. For instructions, refer to *Configuration Manual for Resource Activation*, Reference [8].

4.1 Update Preparations

On the first SC node, SC1:



Caution!

Make sure there is enough free disk-space (4 GB minimum) in `/var/log/`, to be able to copy and untar the new tar file.

1. Transfer the software (EDA System Base SW) to the `/var/log/installfiles` directory on SC1.

2. Change directory:

```
# cd /var/log/installfiles/
```

3. Untar the software (EDA System Base SW):

```
# tar -zxf <Software_Package>.tar.gz
```

Note: It is recommended deleting all untared files after update procedure. For rollback purpose, archive the software to another disk.

4.2 Update Instructions

To update all nodes in the cluster at the same time, resulting in downtime, follow the steps in Section 4.2.1 on page 12. To update the cluster node by node, without any downtime, follow the steps in Section 4.2.2 on page 13.

4.2.1 All Nodes with Downtime

The fastest way to update the whole cluster is to update all nodes at the same time, resulting in downtime.

Attention!

Make sure all traffic is down. Ongoing traffic will cause inconsistency.

Note: The update needs to be performed as user `root` and from the first SC node (SC1).

1. Update the cluster:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

```
# ./ema update --host all
```




Depending on whether LDEwS and evip are on the correct software level:

- If no, the following is prompted:

```
Updating all nodes at the same time means ongoing
provisioning will fail.
Not supported version of LDE or eVIP found, please
upgrade LDE/eVIP before executing update Use this
command to upgrade: "./ema osupdate"
Are you sure you want to continue (y/n)?
```

Enter **n** and press **Enter**. Then upgrade the LDEwS or evip. See Section 4.2.3 on page 15 for instruction.

- If yes, the following is prompted:

```
Updating all nodes at the same time means ongoing
provisioning will fail.
Are you sure you want to continue (y/n)?
```

Enter **y** and press **Enter** to continue.

2. Check the `/home/actadm/config/log/config.log` and `/home/bootloader/config/module_config_files/log/config.log` files for replaced configuration files that may need to be re-configured, as described in Section 4 on page 11.
3. Log out and log in again to receive all the updated environment variables.
4. Run CAI3G test traffic.

Run test traffic to verify the updated nodes. If traffic does not work as expected, perform a rollback.

4.2.2

Node by Node without Downtime

Start with updating one SC node and one PL node. Verify that the updated nodes work as expected by executing traffic on test ports. After verification, enable the nodes to take regular traffic, and then update the rest of the nodes.

During update, both SC1 and PL3 is temporarily disabled from regular traffic. This can cause some performance decrease.

Note: The update needs to be performed as user `root`, and from the first SC node (SC1).

1. Set the Services to only register test services when activated:

```
# bootloader.py config set --parameter @REGISTER_SERV
ICES@ --value false

# bootloader.py config set --parameter @REGISTER_TEST_S
ERVICES@ --value true
```



2. Update the first SC node, SC1:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
# ./ema update --host <hostname SC1>
```

3. If LDEwS or evip is not on the correct software level, the following is prompted:

```
Not supported version of LDE or eVIP found, please
upgrade LDE/eVIP before executing update Use this
command to upgrade:  "./ema osupdate"
Are you sure you want to continue (y/n)?
```

- a. Abort the update by entering **n** and pressing **Enter**.
- b. Set the Services back to register real services when activated:

```
# bootloader.py config remove --parameter
@REGISTER_SERVICES@

# bootloader.py config remove --parameter
@REGISTER_TEST_SERVICES@
```

- c. Upgrade the LDEwS or evip. See Section 4.2.3 on page 15 for instruction.

4. If LDEvS and evip is on the correct software level, continue updating SC1.
5. Update the first PL node, PL3:

```
# ./ema update --host <hostname PL3>
```

6. Check the /home/actadm/config/log/config.log and /home/bootloader/config/module_config_files/log/config.log files for replaced configuration files that may need to be re-configured, as described in Section 4 on page 11.
7. Log out and log in again to receive all the updated environment variables.
8. Check the status on the updated nodes.

Run the following commands:

```
# 3ppmon status --host <hostname>

# bootloader.py node status --host <hostname>

<hostname> is the hostname of the node that is to be checked.
```

9. Run CAI3G test traffic.

Run test traffic on test ports (8888, 8989) to verify the updated nodes.



10. Set the Services to register real services when activated:

```
# bootloader.py config remove --parameter @REGISTER_S
SERVICES@

# bootloader.py config remove --parameter @REGISTER_TES
T_SERVICES@
```

11. Restart the services on SC1 and PL3 so they can take regular traffic:

```
# bootloader.py node activate --host <hostname SC1>

# bootloader.py node activate --host <hostname PL3>
```

12. Update the rest of the nodes in the cluster, one by one:

Note: Wait until the update on the current node is finished before updating the next node.

```
# ./ema update --host <hostname>
```

<hostname> refers to the hostname of the SC and PL nodes in the cluster not yet updated.

13. When all nodes in the cluster, SC and PL are updated, the update to a new software level is completed.

14. Remove the old product folder in /var/log/installfiles/:

```
# rm -rf /var/log/installfiles/<Old_Prod_Number>--<Version>
```

4.2.3

Upgrade LDEwS and Evip

When upgrading LDE or evip, the whole cluster needs to be rebooted. This will result in downtime (ongoing provisioning will fail):

1. Upgrade LDEws or evip on the cluster:

```
# cd /var/log/installfiles/<Prod_Number>--<Version>

# ./ema osupdate
```

The following is prompted:

```
Note: This update includes reboot(ongoing provisioning
will fail),
do you wish to continue (y/n)?
```

Enter **y** and press **Enter**

2. The cluster will automatically reboot, wait until the system is up and running.



After the LDEwS or evip is upgraded, perform all-nodes update (see Section 4.2.1 on page 12) or node-by-node update again (Section 4.2.2 on page 13).

4.3 Rollback Instructions

The rollback procedure rolls back Dynamic Activation to the software level that was installed before the last update.

1. To prepare for rollback, perform the procedure described in Section 4.1 on page 11, using the archived software of the previous version that should be rolled back to.
2. Follow the instruction described in Section 4.2 on page 12, running commands from the *<Prod_Number>-<Version>* that should be rolled back to.



5 Uninstall

This section contains information on how to uninstall the software.

5.1 Uninstallation of Software

For an uninstallation, log in to the first SC node, SC1, as user `root` and follow the step-list:

1. Change directory to `/var/log/installfiles/<Prod_Number>-<Version>`:

```
# cd /var/log/installfiles/<Prod_Number>-<Version>
```

2. Uninstall the package (EDA System Base SW):

```
# ./ema uninstall
```

A question is displayed:

```
Are you sure you want to uninstall: (y/n)
```

Answer `y`

3. When uninstallation is completed, remove the `ema dir/logs` from SC-1:

```
# rm -rf /var/log/ema
```

```
# rm -rf /var/log/installfiles
```

4. To complete the uninstall process, a cluster reboot is needed. Perform the following on one of the SC nodes:

```
# cluster reboot -a
```





Reference List

Ericsson Documents

- [1] *Glossary of Terms and Acronyms*, 0033-CSH 109 628 Uen
- [2] *Hardware Installation and IP Infrastructure Setup for Native Deployment
GEP3*, 2/1531-CSH 109 628 Uen
- [3] *Hardware Installation and IP Infrastructure Setup for Native Deployment
GEP5*, 3/1531-CSH 109 628 Uen
- [4] *Parameter List for Native Deployment*, 5/1057-CSH 109 628 Uen
- [5] *System Administrators Guide for Native Deployment* , 1/1543-CSH 109
628 Uen
- [6] *User Guide for Resource Activation*, 1/1553-CSH 109 628 Uen
- [7] *Library Overview*, 18/1553-CSH 109 628 Uen
- [8] *Configuration Manual for Resource Activation*, 2/1543-CSH 109 628 Uen
- [9] *Product Overview*, 1550-CSH 109 628 Uen
- [10] *Backup and Restore Guideline for Native Deployment*, 2/1553-CSH 109
628 Uen
- [11] *LDE Management Guide* , 1/1553-CAA 901 2978/1 Uen
- [12] *License Counter Management*, 1/197 21-CSH 109 628 Uen
- [13] *Hardening Guideline for Native Deployment*, 1/154 43-CSH 109 628 Uen
- [14] *Customer Questionnaire for Native Deployment*, 4/1057-CSH 109 628
Uen
- [15] *Parameter List for Native Deployment*
5/1057-CSH 109 628 Uen