

FL16 2.0 SEM Validator059_2 Installation Instructions

Product Family: Base Stations
Product: Flexi Multiradio BTS LTE
Release: FL16 2.0

Approval date: 29-Apr-2016



Nokia Solutions and Networks is continually striving to reduce the adverse environmental effects of its products and services. We would like to encourage you as our customers and users to join us in working towards a cleaner, safer environment. Please recycle product packaging and follow the recommendations for power use and proper disposal of our products and their components.

If you should have questions regarding our Environmental Policy or any of the environmental services we offer, please contact us at Nokia Solutions and Networks for additional information.

Table of Contents

1.Purpose	3
2.Summary	3
3.Configuration Information	3
4.Test Results.....	3
5.Installation Instructions.....	3
5.1 Copying software to Administration Server.....	4
5.1.1 Checking the Administration Server tools version	4
5.1.2 Copying the system software	4
5.2 Filling in commissioning workflow variables.....	5
5.3 Decrypting the configuration ZIP file	6
5.4 Updating the parameters.....	6
5.5 Enabling root login and syncing repository to nodes	7
5.6 Upgrading Product Software	8
5.6.1 Creating and executing the NetAct upgrade stacks.....	8
5.6.2 Creating the NetAct online upgrade stack	8
5.6.3 Executing the NetAct online upgrade stack	8
5.7 Copying the NetAct release information files	9
5.8 Verifying the system after installation	9
6.Completing Post upgrade actions.....	9
6.1 Running the NetAct post-upgrade actions with the Workflow tool.....	10
6.2 Deleting passwords of Workflow variables	10
6.3 Removing Workflow tool PRG files	10
6.4 Powering off the Administration Server.....	11
7.Troubleshooting.....	11
7.1 Cleaning the Administration Server	11
7.2 Continuing a failed upgrade stack execution	11
7.3 Continuing a failed Workflow execution	12
7.4 Continuing a failed online stack creation	12
8.Rollback instructions.....	12

Contact: Contact your local Nokia Networks support.

Summary of changes:

29-Apr-2016	1.0	Approved version
-------------	-----	------------------

1. PURPOSE

This document contains installation instructions and other information for a Priority Package (PP) or Service Package (SP) delivery for the Nokia NetAct product. Priority Package provides software corrections for major faults. Service Package provides new or enhanced functionality and possibly also major fault corrections. Changes delivered in this delivery will be merged in the later Release or Maintenance Package (MP) of the product.

2. SUMMARY

Corrected problems: None.

New functionality: This delivery brings the CM SEM validator of NetAct 16.2 to the same level with FL(F)16 2.0 and FL15A 1.2.

Other effects: This delivery does not bring any other effects on the NetAct usage or external interfaces.

3. CONFIGURATION INFORMATION

This delivery pre-requires Release / MP / SP / PP installed: NetAct 16.2

Changes to be merged in Release / MP: NetAct 16.5

Related problem IDs: PR139722, NA05909460

Is anything restarted during installation? Yes. As part of the related metadata editing, CM enterprise applications are restarted

Does this delivery bring any database changes? No

Installation time in R&D test lab: Upgrade time in the large configuration test lab is ~ 45 minutes.

Other information: None

Software package name: netact-PPValidator059-2-disc1.iso

Modified rpm files and versions included in this delivery:

NSN-BTSSiteElementManager-FL-15A-15A.0000_000164_000000.2478-1.noarch.rpm
 NSN-BTSSiteElementManager-FL-16-16.0000_000191_000000.1910-1.noarch.rpm
 NSN-BTSSiteElementManager-FLF-16-16.0000_000136_000000.1839-1.noarch.rpm

4. TEST RESULTS

Installation has been successfully verified by using the Installation Instructions presented in the chapter 5.

5. INSTALLATION INSTRUCTIONS

This delivery is installed by using the Administration Server and NetAct Deployment Configuration Automation (DCA). Steps before the chapter "Upgrade Product Software" can be executed before the actual software upgrade.

Verify system before installation by running Preventive Health Check, see Troubleshooting - Preventive Health Check - Running Preventive Health Check in NetAct Operating Documentation. Take full system backup in case rollback option is needed for this delivery.

Adding new optional nodes is not supported during the installation.

5.1 Copying software to Administration Server

5.1.1 Checking the Administration Server tools version

The Administration Server Tools version 16.2.0.151 installed during the NetAct 16.2 P8 upgrade or commissioning is pre-required installed.

For the systems upgraded from NetAct 15.5 P8, NetAct 15.5 MP1, NetAct 15.5 MP2 to NetAct 16.2 P8, check the version of the required `admin_server_tools` as follows:

```
root@<admin_server># cat /etc/admin_server-release
```

Expected output:

```
admin_server/product_na162 16.2.0.111
admin_server/developing_na162/16.2.0.124
admin_server_tools/product_na162/16.2.0.151
dca/dca/9.0.0.8258
ip0/nipe-n16-2/16.2.0.9
vse_tools/product_na162/16.2.0.29
```

For the systems upgraded from NetAct 16.2 P7 to NetAct 16.2 P8, check the installed `admin_server_tools` as follows:

```
root@<admin_server># yum repolist all | grep
admin_server_tools_na162_netact-product-16.2.0.151
```

Expected output:

```
admin_server_tools_netact-product-na162-16.2.0.151
admin_server_tools_n enabled: 5
```

If the `admin_server_tools` version 16.2.0.151 is not listed in the expected output, then update the `admin_server_tools` version as follows:

1. Download the `admin_server_tools` version 16.2.0.151 from NOLS.
2. Execute `product_copy.sh` to copy the `admin_server_tools` image to the Administration Server.

```
root@<admin_server># /opt/misserver/scripts/product_copy.sh -i
/var/tmp/isofiles/admin_server_tools-product_na162-16.2.0.151-
disc1.iso
```

3. Update `admin_server_tools` to the Administration Server.

```
root@<admin_server>#
/var/builds/admin_server_tools_na162_netact/product/16.2.0.151
/viis-tools/update_viis.sh
```

5.1.2 Copying the system software

The software (iso) image of this delivery includes the software assets (rpm files) and the configuration assets (xml files and templates) which will be copied to the Administration Server by executing the following steps:

1. Power on the Administration Server:
 - a. Log in as the root user to the Vcenter by using vSphere Client.
 - b. Select the Administration Server from navigation tree.
 - c. Select Inventory - Virtual Machine - Power - Power On from menu.
2. Download and copy software (iso) file from NOLS Software Supply Tool to Administration Server to `/var/` directory.
3. Execute the system software copying script `product_copy.sh`, enter:


```
/opt/misserver/scripts/product_copy.sh -i /var/netact-PPValidator059-2-disc1.iso
```
4. Download the updated `write_version_info_to_nodes.sh` file to Administration Server to `/opt/misserver/scripts/` directory. Then run the below command.


```
root@<admin_server># chmod +x /opt/misserver/scripts/write_version_info_to_nodes.sh
```

5.2 Filling in commissioning workflow variables

As preparation for the upgrade, fill in the appropriate values for the variables in the `commissioning_variables.txt` file.

1. Copy `upgrade_variables.txt` template file to the correct place to be used for `commissioningManager.sh` with the below command:


```
root@<admin_server># cp -pv /opt/commissioning/workflow/xmls/upgrade/upgrade_variables.txt /opt/commissioning/bin/commissioning_variables.txt
```
2. Open the file `/opt/commissioning/bin/commissioning_variables.txt` for editing.
3. Fill in the values of the following parameters (detailed information on the parameters can be found in the file):

Variable	Description
SYSTEMNAME	System name
NETACT_DB_VM_IP	IP address of the database VM
OMC_PASSWD	The password of the omc user
ROOT_PASSWD	The password of the root user
CONF_FILES_ZIP	Enter the exact name of the zip file using the format configuration_files_<systemname>_<date>_<time>.zip Ex: configuration_files_srnbnm_2016-01-19_11-05-37.zip
CONF_FILES_ZIP_PASSWD	The password of the ZIP file (decrypted in the beginning of upgrade)
NEW_CONF_FILES_ZIP_PASSWD	The new password of the ZIP file (encrypted at the end of upgrade)
BUILD	PPValidator059_2

Variable	Description
BUILD_PATH	NetAct product build path, usually /var/builds/NetAct/product
UPGRADE_TYPE	Type of upgrade. For normal upgrade, leave the value as empty, e.g. UPGRADE_TYPE= For cloned upgrade, enter the value as -cloning, e.g. UPGRADE_TYPE=-cloning

5.3 Decrypting the configuration ZIP file

It is expected that encrypted ZIP file is located in the Administration Server by default. If for some reason the file does not exist, it is also located in the target nodes in /opt/oss/install/conf/configuration_files_<systemname>_<date>_<time>.zip from where it can be transferred to the Administration Server.

1. Set SYSTEMNAME shell environment variable. Value for the SYSTEMNAME can be found from NIPE produced <systemname>_cluster_info.txt file, either from the parameter SYSTEMNAME inside the file or from the <systemname> part of the file name.

```
root@<admin_server># export SYSTEMNAME=<systemname>
```

2. Decrypt the latest configuration ZIP containing the system configuration. Enter the password that was given when encrypting the files.

```
root@<admin_server>#
/opt/misserver/scripts/decrypt_configuration_files.sh -z
/var/builds/hosts/${SYSTEMNAME}/configuration_files_${SYSTEMNAME}_<date>_<time>.zip
```

5.4 Updating the parameters

The upgrade may bring some changes to parameters used in the previous installation/upgrade. The parameters from the last installation and the new/updated ones need to be merged and exported with the NIPE tool.

The parameter files to be imported with the NIPE tool in the next phase are:

```
/var/netact/${SYSTEMNAME}_vmware_vconf.yml
/var/netact/${SYSTEMNAME}_cluster_info.txt
/var/netact/${SYSTEMNAME}_installation_attr.txt
/var/builds/NetAct/product/PPValidator059_2/nipe-conf/NetAct8_ini.xml
/var/builds/NetAct/product/PPValidator059_2/nipe-conf/NetAct8_upgrade_attrs.txt
```

Download the latest NIPE tools version from TPS from the installed release folder:

1. Extract the nipe.zip file to the appropriate location on your laptop.
2. In the extracted file folder, find and run the nipe.bat file.

NIPE GUI opens.

3. Select **File** → **New Configuration** → **Virtual machine config** and select the correct virtual machine configuration.
4. Select **File** → **Import Product** → **Browse** and open `NetAct8_ini.xml`.
5. Select **File** → **Import** → **VMware Configuration** → **Browse** and open `<systemname>_vmware_vconf.yml`.
6. Select **File** → **Import** → **Cluster Info** → **Browse** and open `<systemname>_cluster_info.txt`.
7. Select **File** → **Import** → **Installation Attributes** → **Browse** and open `<systemname>_installation_attr.txt`.
8. Select **File** → **Import** → **Installation Attributes** → **Browse** and open `NetAct8_upgrade_attrs.txt`.
9. In NIPE GUI, go to the **NetAct 16** tab → **Installation Attributes**. Check if there is any Attribute name without a value defined. Add the value if needed based on the info / description fields.

If the customer has changed any of the passwords listed in the **Installation Attributes** tab, you need to set those to correct ones in NIPE.

10. After parameter values have been filled, export the files. Select **File** → **Export** → **All...** and select a temporary directory (e.g `c:\temp`) directory to save the files and press **Export**.
11. After the export, transfer the exported files to `/tmp` directory on the Administration Server.
12. After the transfer, distribute the files to the Administration Server into the correct locations by running the following script:

```
/opt/misserver/scripts/create_configuration_files.sh -
system_name ${SYSTEMNAME} -config_dir /tmp
```

5.5 Enabling root login and syncing repository to nodes

Execute a script for creating SSH keys and syncing YUM repository files to nodes by executing the following steps.

1. Set `SYSTEMNAME` shell environment variable. Value for the `SYSTEMNAME` can be found from NIPE produced `<systemname>_cluster_info.txt` file, either from the parameter `SYSTEMNAME` inside the file or from the `<systemname>` part of the file name.

```
export SYSTEMNAME=<systemname>
```
2. Execute the script for enabling root login and creating SSH keys in the Administration Server. Place the passwords inside single quotes:

```
/opt/misserver/scripts/ssh_setup_authorization.sh -c
/var/${SYSTEMNAME}_cluster_info.txt -a '<omc user password>' -
p '<root user password>' -u
```
3. Synchronize repository files to the target nodes by entering the following command in the Administration Server:

```
/opt/misserver/scripts/transfer_repo_config.sh -A
"PPValidator059" -c /var/${SYSTEMNAME}_cluster_info.txt
```

The name of the repository file can be checked from `/etc/yum.repos.d/` in the Administration server.

5.6 Upgrading Product Software

This section provides instructions for the actual software upgrade.

5.6.1 Creating and executing the NetAct upgrade stacks

During the upgrade, restarts may occur depending on what is upgraded.

Before starting the online stack creation and execution, make sure that the correct `<systemname>_*.xml` and `<systemname>_*.csv` files are in the `/opt/skynet/dca/dca-install/config` directory, others must be deleted.

5.6.2 Creating the NetAct online upgrade stack

In this section, running the `commissioningManager.sh` script executes the following action which is needed for upgrading with the DCA:

- Creates the online upgrade stack.
1. Log in to the Administration Server as the `root` user.
 2. Create online upgrade stack.

```
root@<admin_server># commissioningManager.sh
file=/opt/commissioning/workflow/xmIs/upgrade/Create_And_Execute
_Online_Upgrade.xml operation=create_online_upgrade_stack
```

If the online upgrade stack creation fails, see the chapter **7.4 Continuing a failed online stack creation**.

5.6.3 Executing the NetAct online upgrade stack

In this section, running the `commissioningManager.sh` script executes the following actions which are needed for upgrading with the DCA:

- Checks the status of the services in the cluster by using `smanager.pl`
 - Executes the online upgrade stack
1. Run the following command:

```
root@<admin_server># commissioningManager.sh
file=/opt/commissioning/workflow/xmIs/upgrade/Create_And_Execute
_Online_Upgrade.xml operation=execute_online_upgrade_stack
```

Expected outcome:

```
Online upgrade triggered successfully. Monitor logs in:
/var/log/dca/
```

Any errors during the online upgrade needs to be handled manually.

2. Monitor the upgrade progress from the log files in the Administration Server.


```
root@<admin_server># tailf  
/var/log/dca/dca_stack_<systemname>_root.log
```

The installation is ready when the following message is visible in DCA log:

```
Installation ready.
```

If the online upgrade fails, see the chapter **7.2 Continuing a failed upgrade stack execution**.

5.7 Copying the NetAct release information files

Copy the NetAct release information files to the target nodes after the upgrade stack execution has been completed as follows.

1. Set the SYSTEMNAME shell environment variable, if it has not been set already:

```
export SYSTEMNAME=<systemname>
```

2. Execute the script that copies the release information files, enter:

```
/opt/misserver/scripts/write_version_info_to_nodes.sh -c  
/var/${SYSTEMNAME}_cluster_info.txt
```

5.8 Verifying the system after installation

Verify system after installation by running Preventive Health Check, see Troubleshooting - Preventive Health Check - Running Preventive Health Check in NetAct Operating Documentation.

6. COMPLETING POST UPGRADE ACTIONS

After the upgrade, the Workflow tool completes the following tasks:

- Disables SSH root access. Because of security reasons, SSH root access to the nodes needs to be disabled after the installation on Unify nodes.
- Encrypts upgrade configuration files in the Administration Server.

A script creates an encrypted ZIP archive of the cluster configuration files. The archive is stored in the Administration Server, and also in all cluster nodes.

The files include, for example:

DCA XML and CSV files under /opt/skynet/dca/dca-install/

Static and dynamic attributes from

/var/builds/hosts/<systemname>/attributes/

The encrypted archive is created to the Administration Server in:

```
/var/builds/hosts/<systemname>/  
configuration_files_<systemname>_<date>_<time>.zip
```

The encrypted archive is stored in all cluster nodes in:

```
/opt/oss/install/conf/configuration_files_<systemname>_<date>_<t  
ime>.zip
```

Even in a case where the Administration Server content would be lost, the archive can be decrypted with the same password and the configuration files can be restored back to the Administration Server.

- Makes and copies the following backup file(s) to the `/opt/oss/install/conf/` directory in the database node:
 - `backup.tgz` which includes data of the following directories in the Administration Server:
 - `/etc/ssh/`
 - `/root/.ssh/`
 - `/etc/hosts`
 - `/etc/sysconfig/clock`
 - `/etc/localtime`
 - `/var/www/html/ssh/authorized_keys`
 - `tsn.tgz` (if needed). Script checks if any Technical Support Notes (TSNs) have been applied to the system by checking and compressing the content of `/var/builds/hosts/<systemname>/tsn/` directory.
- Deletes passwords of Workflow tool variables.

6.1 Running the NetAct post-upgrade actions with the Workflow tool

1. Log in to the Administration Server as the root user.
2. Run the following command:

```
root@<admin_server># commissioningManager.sh
file=/opt/commissioning/workflow/xmles/upgrade/Post_Upgrade_Actio
ns_WF.xml
```

6.2 Deleting passwords of Workflow variables

Before deleting passwords from password file, store the encryption password of upgrade configuration ZIP file for future use.

1. Print out and store the password for future use.

```
root@<admin_server># grep ^NEW_CONF_FILES_ZIP_PASSWD
/opt/commissioning/bin/commissioning_variables.txt
```

2. Run the below command to delete all workflow clear-text passwords from the `commissioning_variables.txt` file.

```
root@<admin_server># commissioningManager.sh
file=/opt/commissioning/workflow/xmles/upgrade/Cleanup_WF_Passwor
ds_WF.xml
```

6.3 Removing Workflow tool PRG files

Workflow tool (`commissioningManager.sh`) makes `*.prg` files during the upgrade. Such files need to be removed from the `/opt/commissioning/progress` directory and transferred to the `/var/log/upgradewfprg` directory.

Run the following command:

```
root@<admin_server>#
/opt/commissioning/workflow/scripts/upgrade/clean_wf_prg_files.sh
-e
```

6.4 Powering off the Administration Server

Power off the Administration Server:

1. Log in as the root user to the Administration Server.
2. To shut down the Administration Server, enter:

```
poweroff
```

7. TROUBLESHOOTING

This section provides instructions for troubleshooting the upgrade.

7.1 Cleaning the Administration Server

If the Administration Server is used for several installation or upgrades it may be necessary to remove old NetAct software products first in order to free disk space so that `product_copy.sh` is able to extract the new product from media.

Products are extracted under the `/var/builds/` directory.

NetAct products are in `/var/builds/NetAct/product/<version>`

To free disk space, remove the products which are no longer needed. Also remove the corresponding NetAct repository (`.repo`) file from the `/etc/yum.repos.d/` directory.

7.2 Continuing a failed upgrade stack execution

If the upgrade stack execution fails, an error is visible in the logs and the problem must be investigated. In case the error was solved and there is no need to create the stack again, you can restart the stack execution.

Before starting a new stack execution, make sure that the old instance is finished.

1. Log in to the Administration Server as the root user.
2. To find out if the stack execution is finished, enter:

```
root@<admin_server># ps -ef |grep <stack_filename.csv>
```

3. If the given `<stack_filename.csv>` is not listed, start a new instance.

- 3.1. If the upgrade fails already in the stack verification phase, investigate and solve the problem and then restart the failing stack with the following command:

```
root@<admin_server># /opt/misserver/scripts/execute_stacks.sh
-stacks <stack_filename.csv>
```

- 3.2. If the stack fails in the actual upgrade phase, investigate and solve the problem and then restart the failing stack with the following command:

```
root@<admin_server># nohup /opt/skynet/dca/dca-install/dca.sh
-install <stack_filename.csv> -continuePrevious -verifyStack
2>&1 &
```

7.3 Continuing a failed Workflow execution

If the Workflow execution fails, an error is visible on the screen and in the logs of the scripts which were executed by `commissioningManager.sh`. When the problem is resolved, you can restart Workflow execution continuing from the previous with the same commissioning manager command that has failed.

7.4 Continuing a failed online stack creation

If the upgrade stack creation fails, an error is visible in the logs and the problem must be investigated. In case the error was solved, re-execute the stack creation as follows:

- If online stack creation fails, execute the following command:

```
root@<admin_server># commissioningManager.sh
file=/opt/commissioning/workflow/xmls/upgrade/Create_And_Execute
_Online_Upgrade.xml operation=create_online_upgrade_stack
```

8. ROLLBACK INSTRUCTIONS

There is no delivery specific rollback for this delivery. Restore full system backup if needed.

Disclaimer

The information in this document applies solely to the hardware/software product ("Product") specified herein, and only as specified herein.

This document is intended for use by Nokia Solutions and Networks' customers ("You") only, and it may not be used except for the purposes defined in the agreement between You and Nokia Solutions and Networks ("Agreement") under which this document is distributed. No part of this document may be used, copied, reproduced, modified or transmitted in any form or means without the prior written permission of Nokia Solutions and Networks. If you have not entered into an Agreement applicable to the Product, or if that Agreement has expired or has been terminated, You may not use this document in any manner and You are obliged to return it to Nokia Solutions and Networks and destroy or delete any copies thereof.

The document has been prepared to be used by professional and properly trained personnel, and You assume full responsibility when using it. Nokia Solutions and Networks welcome Your comments as part of the process of continuous development and improvement of the documentation.

This document and its contents are provided as a convenience to You. Any information or statements concerning the suitability, capacity, fitness for purpose or performance of the Product are given solely on an "as is" and "as available" basis in this document, and Nokia Solutions and Networks reserves the right to change any such information and statements without notice. Nokia Solutions and Networks has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions, and Nokia Solutions and Networks will correct errors that You identify in this document. But, Nokia Solutions and Networks' total liability for any errors in the document is strictly limited to the correction of such error(s). Nokia Solutions and Networks does not warrant that the use of the software in the Product will be uninterrupted or error-free.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA SOLUTIONS AND NETWORKS BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

This document is Nokia Solutions and Networks' proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia Solutions and Networks.

Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners, and they are mentioned for identification purposes only.

Copyright © 2016 Nokia Solutions and Networks. All rights reserved.