Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 9.0 R2

MIGRATION FROM XMS LA2.0.2

3HE 06519 AAAC TQZZA Edition 01

Alcatel-Lucent Proprietary
This document contains proprietary information of Alcatel-Lucent and is not to be disclosed or used except in accordance with applicable agreements.

Copyright 2011 © Alcatel-Lucent. All rights reserved.

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, Lucent, Alcatel-Lucent, the Alcatel-Lucent logo, and TiMetra are registered trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2011 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical
or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent
tries to ensure that this information accurately reflects information provided by the supplier, please refer
to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

CONTENTS

CONTENTS **3**

1. INTRODUCTION **5**

1.1. OBJECTIVE 5

1.2. SCOPE OF THIS DOCUMENT 5

1.3. AUDIENCE FOR THIS DOCUMENT 5

2. RELATED DOCUMENTS **6**

2.1. APPLICABLE DOCUMENTS 6

2.1.1 Release Notes 6

2.2. REFERENCE DOCUMENTS 6

2.2.1 Installation Methods 6

2.2.2 XMS Documentation 6

2.2.3 WPS Documentation 6

3. ABBREVIATIONS AND DEFINITIONS **7**

3.1. ABBREVIATIONS 7

3.2. DEFINITIONS 8

3.3. WPS VERSION 8

3.4. MODELS VERSION 8

3.5. NPO VERSION 8

4. CONTENT **9**

4.1. REQUIRED INFORMATION 9

4.2. GENERAL OVERVIEW 9

4.3. PREREQUISITES 11

4.4. RESTRICTIONS 11

4.4.1 Wireless License Manager 11

4.5. LIMITATIONS 12

4.5.1 UNIX Users and Groups 12

4.5.2 Non-UNIX Users 13

4.5.3 CRONTAB Entries 13

4.5.4 Customer Scripts 13

4.5.5 Server Security 14

4.5.6 IPSec Configuration 14

4.5.7 NE Backup Configuration 14

4.5.8 eDat Interface 14

4.5.9 Historical Information 14

4.5.10 WICL 14

4.5.11 Data Sharing 14

4.5.12 Citrix Environment 14

4.5.13 SANE Tool 15

4.6. 5620 SAM SERVER: PREPARATION 15

4.6.1 Open 5620 SAM Client 15

4.6.2 LTE RAN licensing 15
4.6.3 SNMP User Creation for eNodeB Management 16
4.6.4 Mediation Policies Creation 18
4.6.5 Self Config Policies Creation 21
4.7. XMS SERVER 22
4.7.1 Prerequisites 22
4.7.2 Check XMS Server 22
4.7.3 Actions on the XMS Server 22
4.8. WPS TOOL 27
4.8.1 Transfer snapshot file to local machine 27
4.8.2 Import snapshot file using WPS 28
4.9. 5620 SAM SERVER: MANAGE ENODEB 34
4.9.1 Open 5620 SAM Client 34
4.9.2 WorkOrder Activation 34
4.9.3 eNodeB Discovery 36
4.10. ALARM MANAGEMENT 40
4.10.1 Get XMS Information 40
4.10.2 Configure 5620 SAM Alarm Management 41
4.11. PERFORMANCE MANAGEMENT MIGRATION 42
4.11.1 Action on XMS Server 42
4.11.2 Configuration on 5620 SAM Server 42
4.12. EXPORT NETWORK ELEMENTS 42
4.13. NPO DATA SOURCE MANAGEMENT 43
4.13.1 Undeclare the XMS server 43
4.13.2 Declare the 5620 SAM server 43
4.14. REVERSE PROCEDURE 44
4.14.1 Unmanage eNodeB(s) in 5620 SAM 44
4.14.2 Start eNodeB Supervision from XMS 45

5. LIST OF KNOWN PROBLEMS 46

1. INTRODUCTION

1.1. OBJECTIVE

This document is a general procedure for migrating device management of the eNodeB from an XMS server to a 5620 SAM server.

This document describes the general methodology, prerequisites, required prechecks, and known limits for migrating the eNodeB from an XMS to a 5620 SAM server.

1.2. SCOPE OF THIS DOCUMENT

The following items are covered in this document:

- Prerequisites of the migration procedure.
- All unsupported items.
- Steps to migrate management of eNodeB(s) from XMS to the 5620 SAM.

The network elements managed by XMS are eNodeB LA2.0, LA2.1 (FDD LA2.0.2) and TLA2.1 (TDD).

1.3. AUDIENCE FOR THIS DOCUMENT

This document is intended for LTE network administrators.

2. RELATED DOCUMENTS

2.1. APPLICABLE DOCUMENTS

[A1] 5620 SAM, Release 9.0 R2 User Guide 3HE 05719 AAAB TQZZA Edition 01

[A2] 5620 SAM | 5650 CPAM, Release 9.0 R2 Installation and Upgrade Guide 3HE 05718 AAAB TQZZA Edition 01

[A3] 5620 SAM, Release 9.0 R2 LTE RAN User Guide 3HE 06262 AAAB TQZZA Edition 01

> **NOTE**: You can obtain the 5620 SAM Release 9.0 documentation from the 5620 SAM Release 9.0 R2 software installation.

[A4] NPO Administration User Guide | Release M4
Available at: FPDM4-02B

A wide range of documentation, including product manuals and documentation updates, is accessible from the Alcatel-Lucent Customer Support Center at http://www.alcatel-lucent.com/myaccess.

2.1.1 Release Notes

[A5] LTE RAN Release Notes. https://services.support.alcatel-lucent.com/services/lte/?path=/Documents/Notes/LE3.0

2.2. REFERENCE DOCUMENTS

2.2.1 Installation Methods

The 5620 SAM server must be installed or upgraded to 9.0 R2 using the [A2] document.

2.2.2 XMS Documentation

XMS documentation can be obtained on OLCS at: https://support.alcatel-lucent.com/portal/productContent.do?productId=&entryId=1-0000000003456

2.2.3 WPS Documentation

9452 WPS documentation can be found here: https://support.alcatel-lucent.com/portal/productContent.do?productId=&entryId=1-0000000003703

3. ABBREVIATIONS AND DEFINITIONS

3.1. ABBREVIATIONS

ALTP	Alcatel-Lucent Technical Publication
CM XML	XML for Configuration Management
EP	Emergency Patches
FAP	Feature Application Procedure
FCS	First Customer Shipment
FOA	First Office Application
KPI	Key Performance Indicators
MO	Managed Object
MOI	Managed Object Instance(s)
MNCL	Maintenance Non Core module Load
NCL	Non Core module Load
NE	Network Element
NPO	Network Performance Optimizer
OMC	Operation Maintenance Center
RLN	Release Note
RTU	Rights To Use
SAM	Service Awareness Manager
XMS	eXtended Management System
WPS	Wireless Provisioning System
WA	WorkAround
WICL	Wireless Internet Command Line
WO	Work Order
WS	Work Space
XML	eXtensible Markup Language

3.2. DEFINITIONS

The 5620 SAM load naming conventions used in the following sections of the document is:

SAM 90_R2

3.3. WPS VERSION

The LA3.0.1 WPS version used in this document is WPS_LTE3.0.1-39-019.

3.4. MODELS VERSION

The MIM version used in this document is MIM.5.3.8.

3.5. NPO VERSION

The NPO server version must correspond to the correct 5620 SAM/WPS versions for model alignment. For the procedures in this document, the NPO version must be NPO 4.1 R3.

4. CONTENT

4.1. REQUIRED INFORMATION

You must have the following information and conditions in order to perform the migration:

XMS SERVER:

- XMS server IP address
- root user password
- oamops user password
- initial_snm password on the eNodeBs
- Administrator password

5620 SAM SERVER:

- 5620 SAM server IP address
- root password
- 5620 SAM Client password

PC CLIENT:

- All required software installed
- Connection to the XMS and 5620 SAM servers from a PC client.

You must be able to manage and unmanage all eNodeBs.

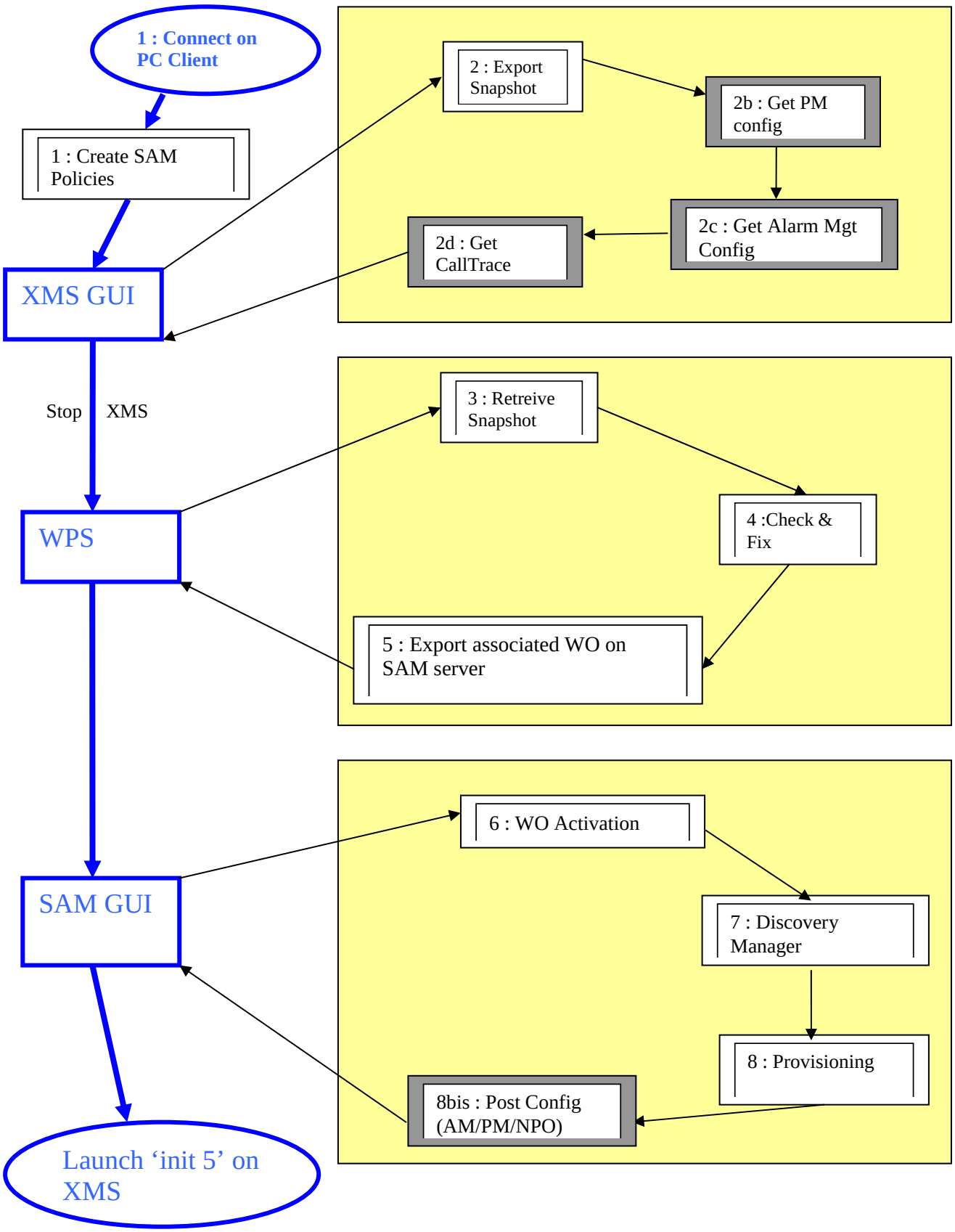
4.2. GENERAL OVERVIEW

This section describes a workflow for migrating eNodeB management from XMS to the 5620 SAM.

Legend:

Example of mandatory step:

Example of optional step:


1 : Connect on PC Client
1 : Create SAM Policies
XMS GUI
2 : Export Snapshot
2b : Get PM config
2c : Get Alarm Mgt Config
2d : Get CallTrace
Stop XMS
WPS
3 : Retreive Snapshot
4 :Check & Fix
5 : Export associated WO on SAM server
SAM GUI
6 : WO Activation
7 : Discovery Manager
8 : Provisioning
8bis : Post Config (AM/PM/NPO)
Launch 'init 5' on XMS

4.3. PREREQUISITES

- The NPO server must be upgraded to NPO LA3.0.
- All call trace sessions on all eNodeBs must be stopped.
- You must verify that all eNodeBs can connect to the 5620 SAM server (ping from the 5620 SAM server to each eNodeB is valid). If the eNodeB management IP cannot be pinged from the 5620 SAM, then you must configure a static route between the eNodeB and the 5620 SAM by using an NEM connection to the eNodeB.
- All eNodeB(s) for discovery and management by the 5620 SAM must have unique D2U serial numbers (contact your Alcatel-Lucent customer support representative for more information).

4.4. RESTRICTIONS

The following restrictions are applicable:

4.4.1 Wireless License Manager

WLM is not taken into account in this version. License entitlements for eNodeBs are handled by the RAN License Manager tool of the 5620 SAM.

4.5. LIMITATIONS

4.5.1 UNIX Users and Groups

- Migration of XMS UNIX groups and users is not covered by this procedure.

Most XMS groups and users are not used on the 5620 SAM server.

On XMS SERVER:

- The customer unix users and groups are defined in the following files:
  - /etc/group
  - /etc/passwd
  - /etc/shadow

You can save these files on the XMS server. As the root user, enter the following commands on the XMS server:

cat /etc/group > /home/customer/groupFile.tmp

cat /etc/passwd > /home/customer/passwdFile.tmp

cat /etc/shadow > /home/customer/shadowFile.tmp

ON 5620 SAM SERVER:

- Example of unix groups/users creation for 5620 SAM:
  - To create a group on the 5620 SAM server, enter the following command as the root user (enter the man groupadd command for more information):

  # groupadd <GroupNameToAdd>

  - To create a user on the 5620 SAM server, enter the following command as the root user (enter the man useradd command for more information):

  # useradd -s /bin/csh -m -d /home/oamops -g oamgroup oamops

  For this entry /etc/passwd “oamops:x:100:100::/home/oamops:/bin/csh”

  With groupid 100 is oamgroup entry on /etc/group file

  Check that the dedicated home directories are created.

4.5.2 Non-UNIX Users

Migration of non-UNIX users from the XMS server to the 5620 SAM server is outside the scope of this procedure. All CSA/Ngsec users are not migrated.

4.5.3 CRONTAB Entries

XMS crontab migration is outside the scope of this procedure.

If required, the customer can save it by entering the following command as the root user on the XMS server:

```
# crontab -l > /home/customer/crontFile
```

Please refer to the EXPORT chapter for more information about migrating XMS crontab entries to 5620 SAM.

4.5.4 Customer Scripts

XMS scripts migration is outside the scope of this procedure.

ON XMS SERVER:

If you want to save any scripts, go to the dedicated path (/home/customer for example) and tar/zip them.

As the root user on the XMS server, launch following commands:

```
# cd /home/customer
# tar cvf customerScripts.tar script2.wcl script1.sh
# gzip customerScripts.tar
# sftp root@<SamServer@IP>
```

Enter the root password for the 5620 SAM server.

```
% put customerScripts.tar.gz
% exit
```

4.5.5 Server Security

All security server configuration perfomed on the XMS will not be migrated to the 5620 SAM server.

Part of OS-Hardening is providing security to the 5620 SAM server. Please refer to the dedicated 5620 SAM documentation ([A1]) to understand what is required for 5620 SAM server security.

4.5.6 IPSec Configuration

The IPSEC migration from the XMS server to the 5620 SAM server is outside the scope of this procedure.

4.5.7 NE Backup Configuration

The NE Backup migration from the XMS server to the 5620 SAM server is outside the scope of this procedure.

4.5.8 eDat Interface

The eDat interface migration from the XMS server to the 5620 SAM server is outside the scope of this procedure.

4.5.9 Historical Information

Migration of historical information (alarms, events, PM data) from the XMS server to the 5620 SAM server is not supported.

4.5.10 WICL

WICL scripts cannot be used on the 5620 SAM server.

4.5.11 Data Sharing

Workorders cannot be retrieved by WPS from the XMS server.

ON XMS SERVER:

You must apply WPS patches in order to use the Live repository function.

4.5.12 Citrix Environment

It is not the goal of this procedure to explain how to use the CITRIX environment with a 5620 SAM server.

4.5.13 SANE Tool

It is not the goal of this procedure to explain how to use SANE tools with a 5620 SAM server.

4.6. 5620 SAM SERVER: PREPARATION

The goal of this chapter is to prepare 5620 SAM server. The procedures in this chapter only need to be performed once.

The 5620 SAM server must be installed as or nominally upgraded to 5620 SAM Release 9.0 R2.

The 5620 SAM client must be installed on a client PC.

For more information about the following procedures, please refer to the [A3] document.

4.6.1 Open 5620 SAM Client

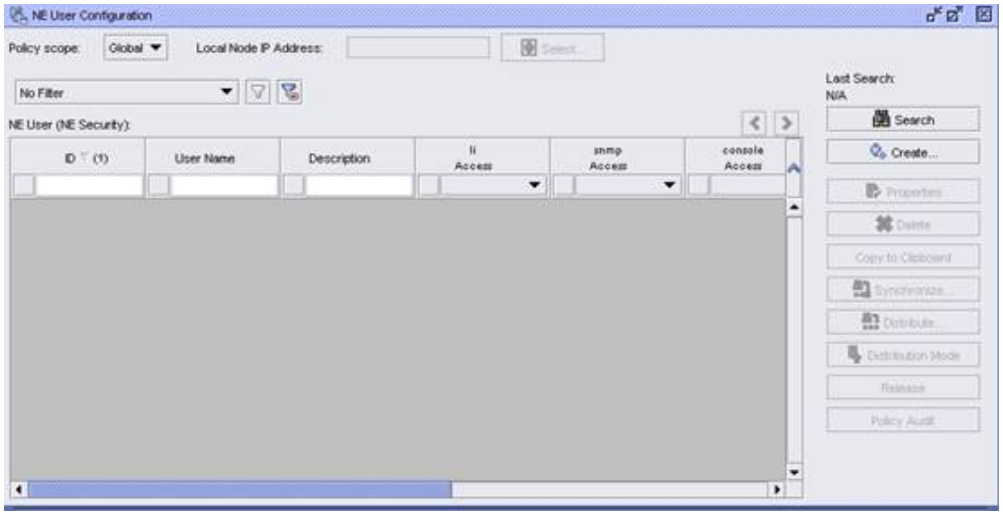
On a PC client, open the 5620 SAM client application and enter the admin login and password to log on. Once the 5620 SAM client window is opened, you must create the required snmp user for eNodeB management.

4.6.2 LTE RAN licensing

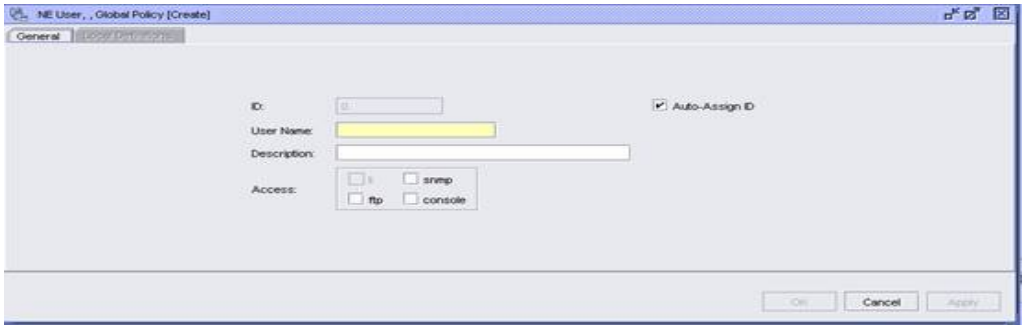
Perform the procedures in the [A3] document, section 8.3, to import LKDI license file(s) into the 5620 SAM to prepare for eNodeB management. Failing to import sufficient license entitlements will not prevent eNodeB discovery, but it will cause the 5620 SAM to raise license violation alarms and prevent eNodeB feature activation and workorder deployment.

4.6.3 SNMP User Creation for eNodeB Management

1. In the 5620 SAM client, select Administration → Security → NE User Configuration from the main menu.



2. Click on the Create button.



3. Configure the following parameters:

   ID: Enter an incremental value for this new user.

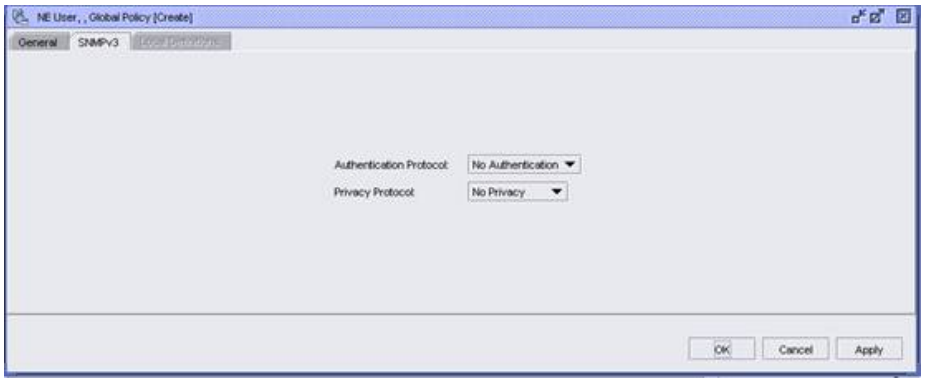
   Note: When creating the first user, this field is greyed-out.

   User Name*: initial_snm*

   Description*: <Description at user's discretion>*

   Access: select the snmp checkbox.

4. Click on the SNMPv3 tab.



5. Configure the following parameters:

   New Authentication Password*: <eNodeB password for initial_snm>*

   Confirm New Auth Password*: <eNodeB password for initial_snm>*

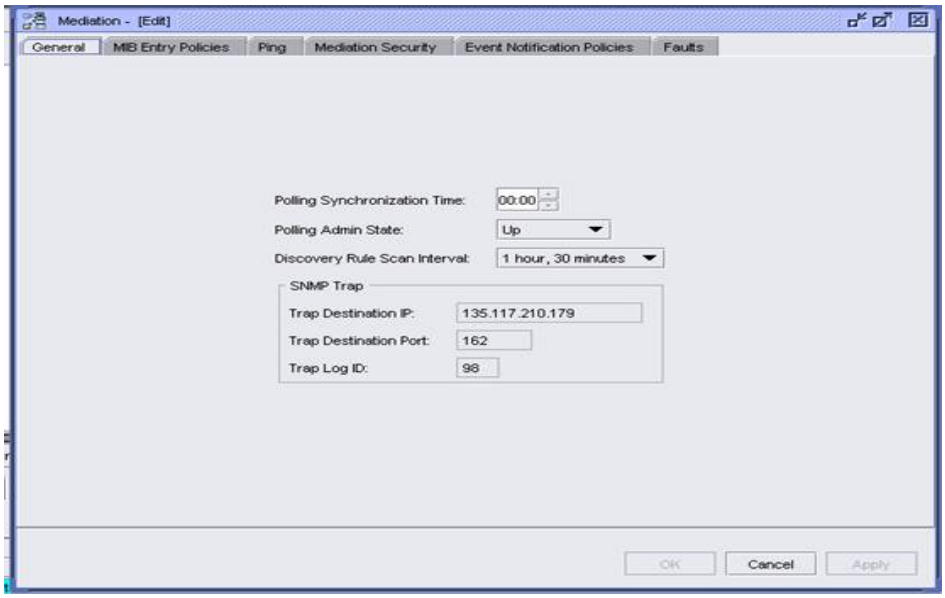
   New Privacy Password*: <eNodeB password for initial_snm>*

   Confirm New Privacy Password*: <eNodeB password for initial_snm>*

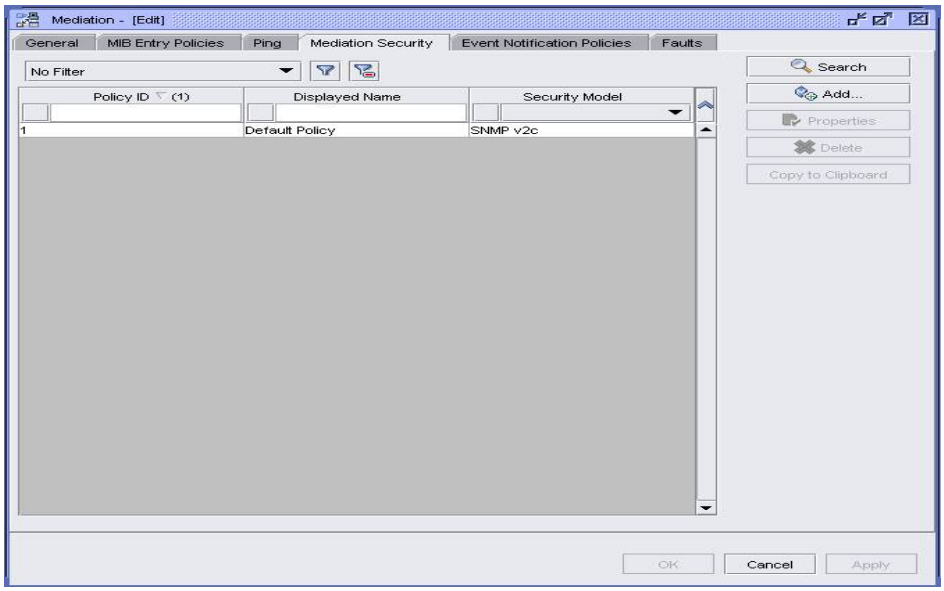
6. Click on the OK button.

4.6.4 Mediation Policies Creation

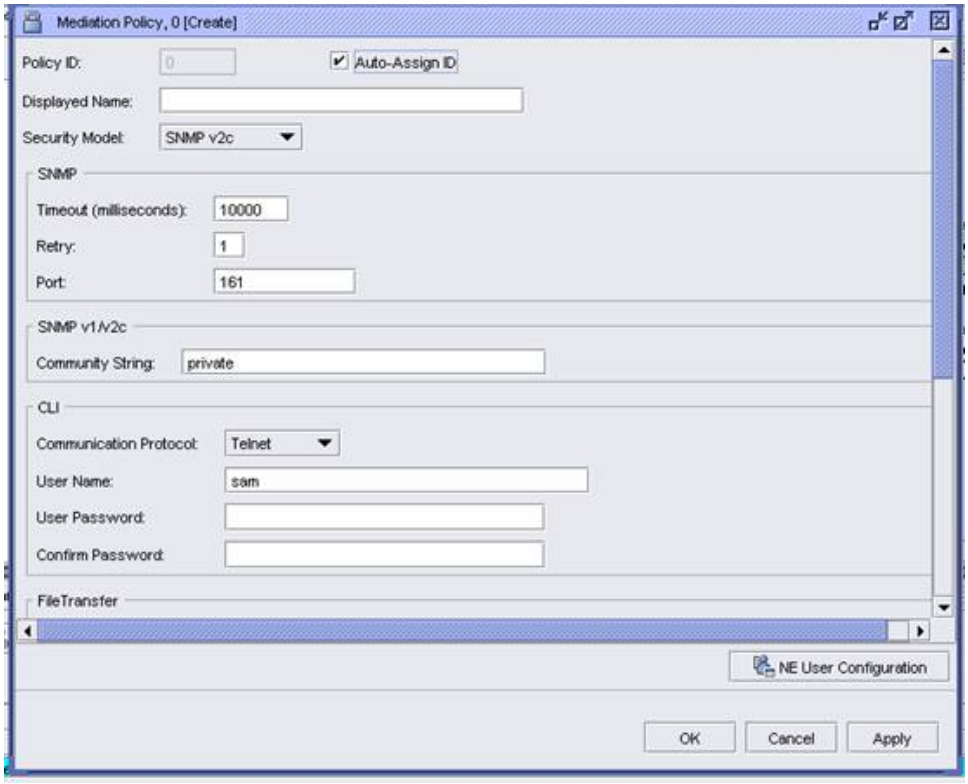
1. In the 5620 SAM client, choose Administration → Mediation from the main menu



2. Click on the Mediation Security tab.



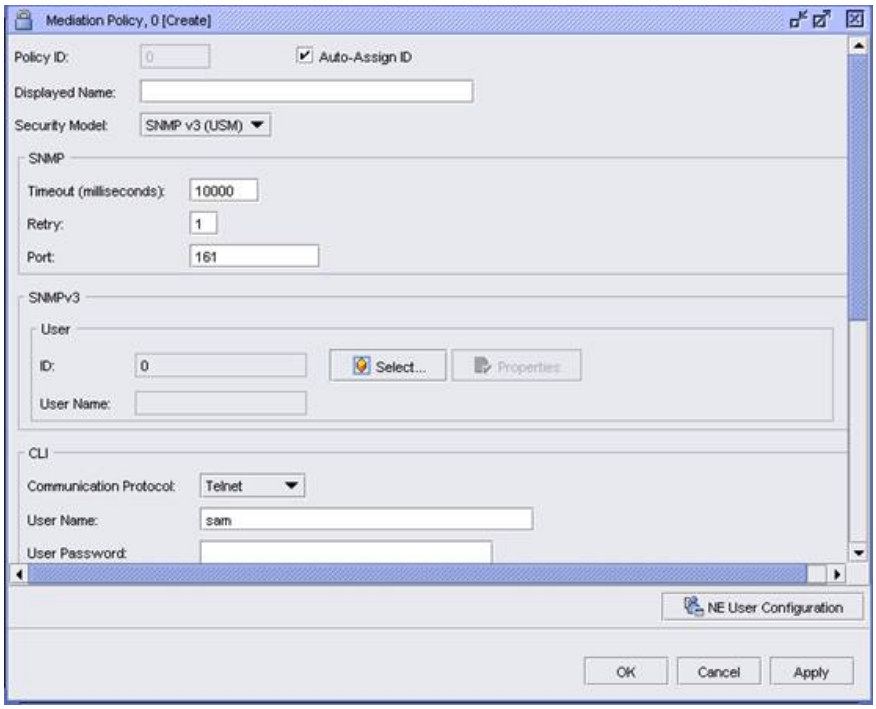
3. Click on the Add button.



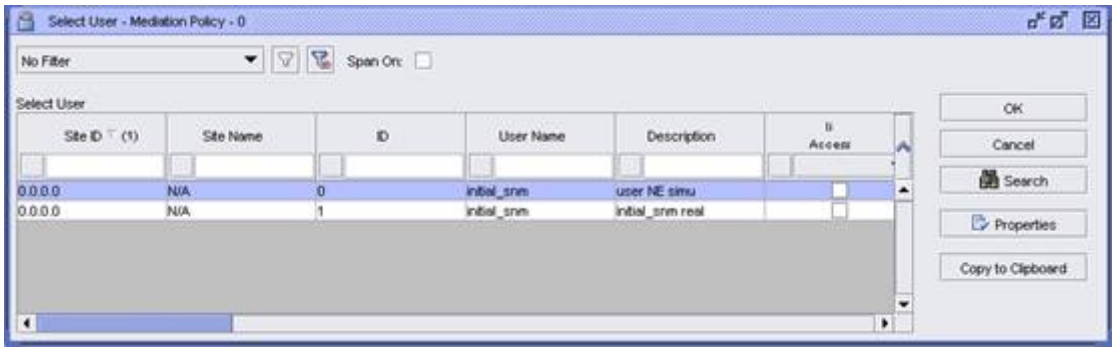
4. Configure the following parameters:

   Displayed Name: **<***Name at user's discretion***>**

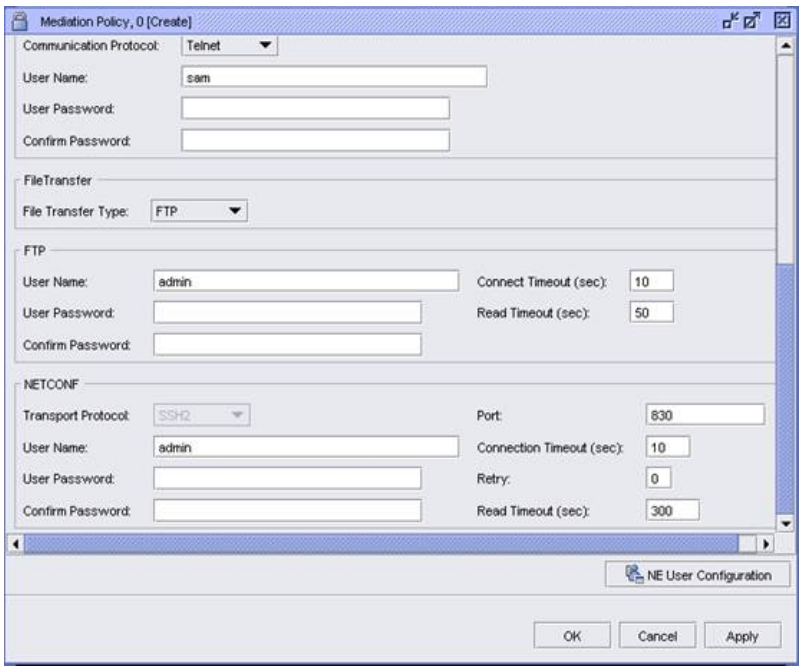
   Security Model*: Choose SNMPv3 (USM) from the drop-down list.*



5. In the SNMPv3 panel, click on the Select button.



6. In Select User panel, select the SNMP user that corresponds to the current mediation and click on the OK button.



7. Configure the following parameters in the NETCONF panel:
   User Name: *initial_snm*

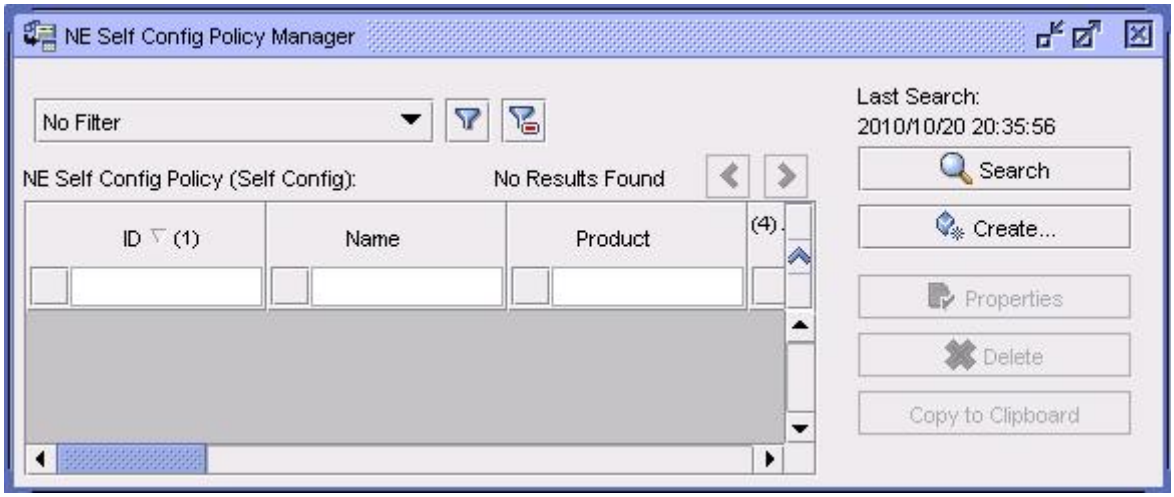
   Port*: 830*

   User Password*: <eNodeB password for initial_snm>*

   Confirm Password*: <eNodeB password for initial_snm>*
8. Click on the OK button.
9. Click on the OK button.

4.6.5 Self Config Policies Creation

1. In the 5620 SAM client, choose Administration → NE Self Config Policy Manager from the main menu.



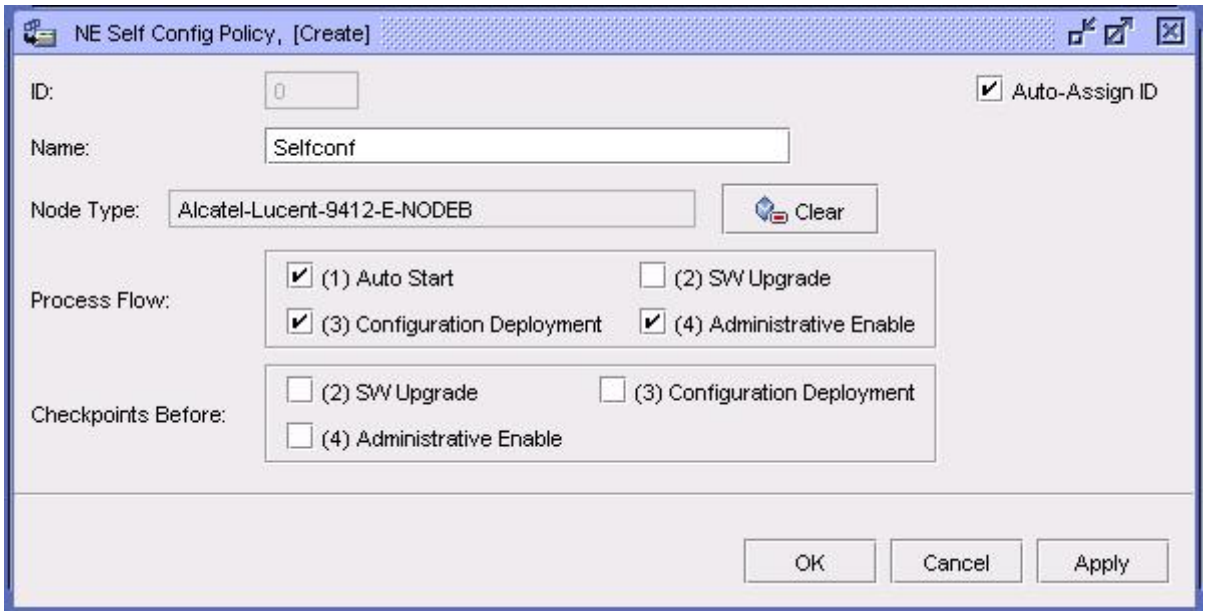
2. Click on the Create button.
3. Configure the following parameters:

   Name: *<name at user's discretion>*

   Node Type: Click on Select, and choose Alcatel-Lucent-9412-E-NODEB from the drop-down menu.

   Process Flow: Unselect SW Upgrade. Select Auto Start, Configuration Deployment, and Administrative Enable.

   CheckPoints Before: Unselect ALL checkpoints.



4. Click on the OK button, then close the NE Self Config Policy Manager form.

4.7. XMS SERVER

This section describes how to retreive eNodeB information from XMS and stop eNodeB supervision.

4.7.1 Prerequisites

- The XMS server version must be LA2.0.2.
  Please check the dedicated RLN to be sure all conditions are met.

- All eNodeBs must be supervised by the XMS server.
  The supported model of eNodeB is MIM.5.3.8, FM model edition 6 and MIB Ed2P05.

4.7.2 Check XMS Server

- Following the XMS procedures, connect with a PC client and open an XMS WiBox.
- Open the supervision GUI in order to verify that all eNodeBs are supervised by the XMS server.
- It is the responsibility of the operator to verify that the XMS server is fully operational before starting this procedure.

4.7.3 Actions on the XMS Server

NOTE: If you need to only migrate a cluster of eNodeBs, perform the steps that are hightlighted in the following format: To migrate an eNodeB cluster

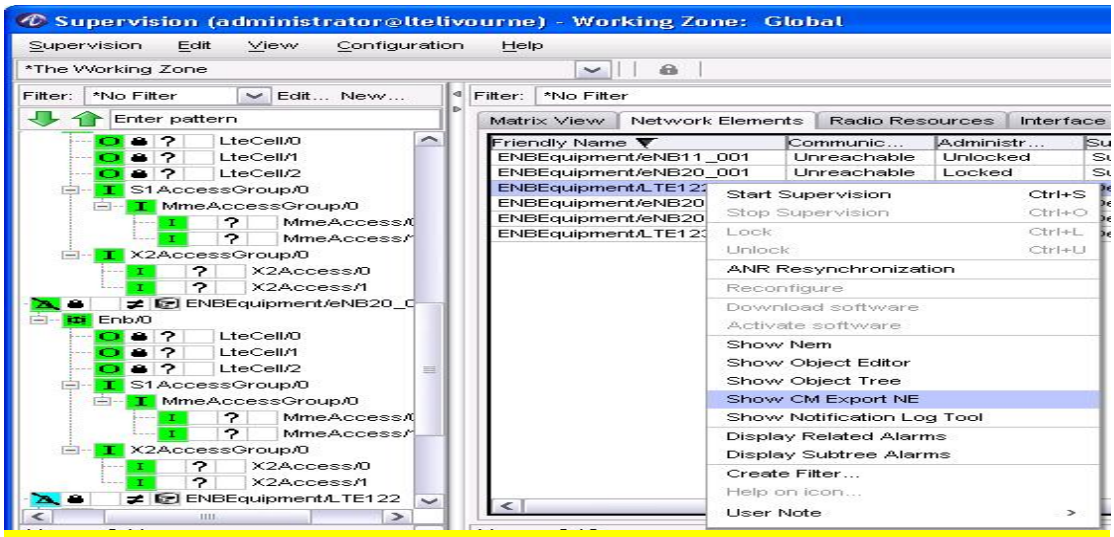
The following steps are mandatory. You must have the UNIX root user password and the Wibox password for XMS.

You must get the IP addresses of all eNodeBs.

1. Export a snapshot of one eNodeB
   a. Open XMS Wibox and enter the default administrator login and password.

b. In XMS WiBox, click on the Supervision icon and use the dedicated windows to verify that all eNodeBs are supervised and reachable.

c. Right click on an eNodeB (For an eNodeB cluster, select all applicable eNodeBs) and choose Show CM Export NE from the contextual menu.



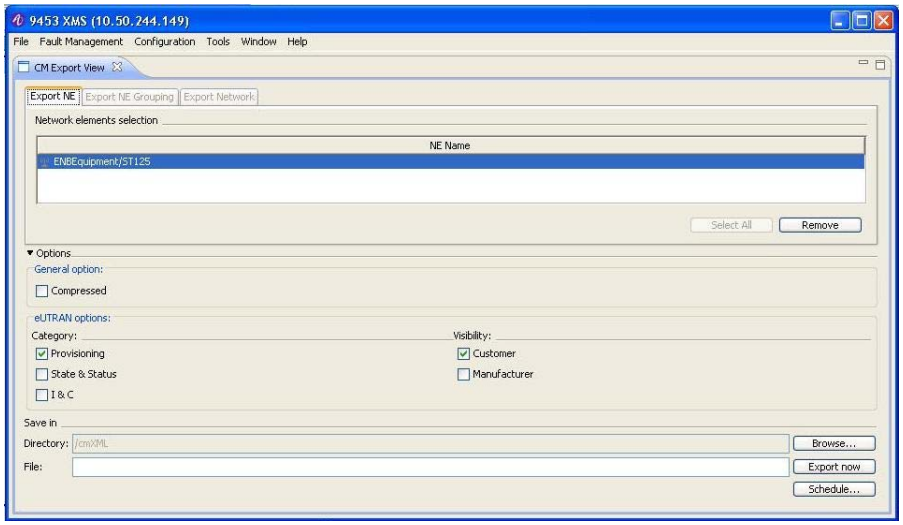
d. In the CM Export View window, select the NE Name (For an eNodeB cluster, select all applicable eNodeBs).

Perform the following steps:

a. In the General Option panel, do not enable the Compressed checkbox.

b. In the Category panel, enable the following checkboxes only:

- Provisioning
- Customer

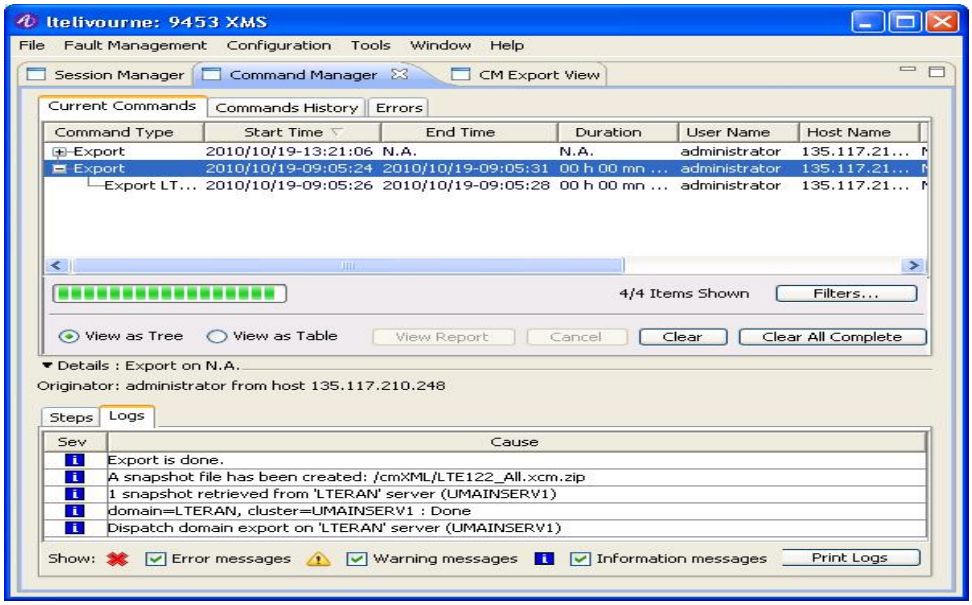


c. In the Save in panel, enter the eNodeB name (or cluster name) in the File field.

d. Click on the Export now button.

e. Click on the Command Manager button in the WiBox GUI.

f. Verify that the export displays in the Command Manager Window.



2. Export a snapshot of all eNodeBs

a. In the WiBox GUI, click on the CM XML Export button.

b. In the CM Export View window, select LTERAN.

c. In the General Option panel, do not enable the Compressed checkbox.

d. In the Category panel, enable the following checkboxes only:

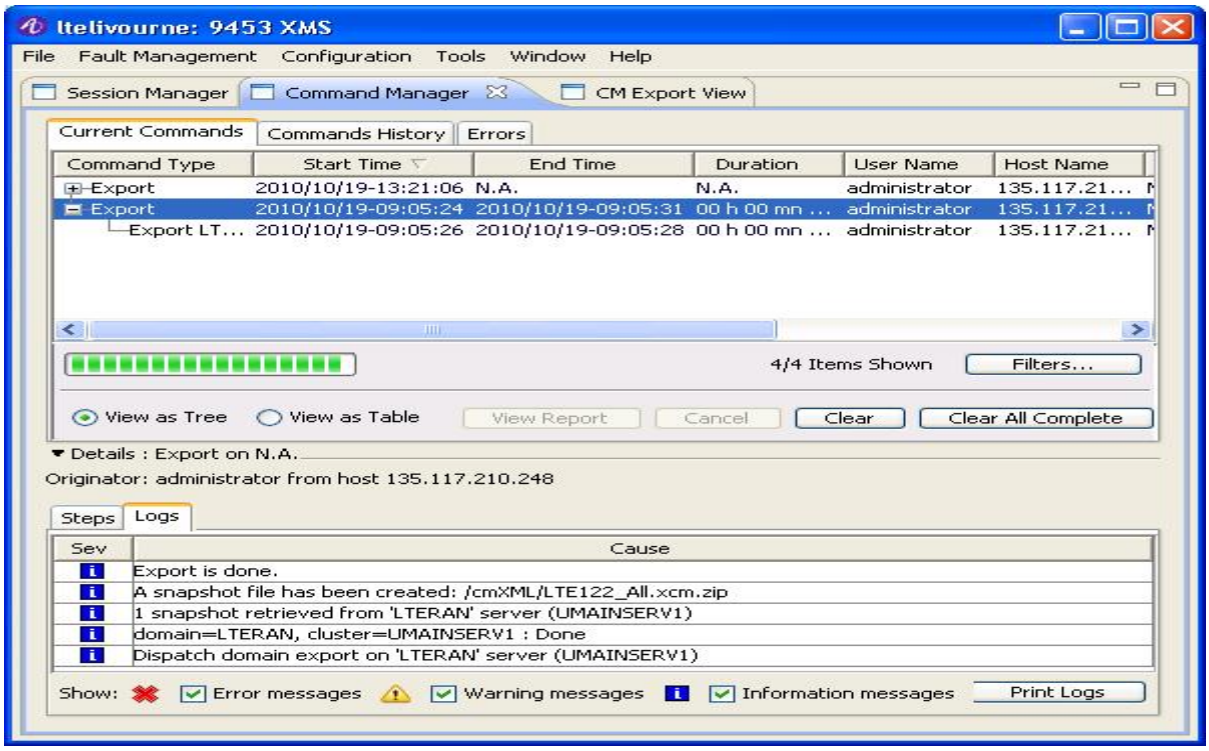
- Provisioning
- Customer

e. In the Save in panel, enter the network name in the File field.

3. Verify the export result

Click on the Command Manager button in the WiBox GUI.

Verify that the export displays in the Command Manager window.



4. Lock the link:

In the XMS Supervision GUI, right click on the dedicated eNodeB(s) (select all the eNodeBs for an eNodeB cluster) and choose Lock from the contextual menu.

5. Stop supervision

In the XMS Supervision GUI, right click on the dedicated eNodeB(s) (select all the eNodeBs for an eNodeB cluster) and choose Stop Supervision from the contextual menu.

A Confirmation window opens. Click on the OK button.

XMS supervision of the eNodeB(s) stops.

6. To migrate XMS alarm management configuration, see section 4.9.

7. To migrate XMS Performance management configuration, see section 4.10.

8. To migrate NPO from XMS server to the 5620 SAM server, see section 4.12.1.

9. Stop the XMS server (only perform this step if all eNodeBs are migrated and XMS is no longer needed)
   - Close all the XMS GUIs.
   - Log on to the XMS server as the oamops user and enter the following command:

     (oamops) % /opt/oam/exe/pmgt/svcadm.x disable /application/xms/xms

   - Verify that the XMS services are stopped by entering the following command:

     (oamops) % svcs –a |grep xms

   - Repeat the command until all the services are disabled.

4.8. WPS TOOL

4.8.1 TRANSFER SNAPSHOT FILE TO LOCAL MACHINE

This section describes how to generate the required Workorder file by using the exported snapshot file.

First, you must transfer the snapshot from the XMS server to a local client machine by using filezilla, or FTP (windows ftp command is described below):

1. On a local client machine, choose Start → Run from the Windows desktop.
2. Enter cmd and click on the OK button. A command prompt window opens.
3. Navigate to the local directory where you want to store the snapshot file.
4. Enter the following command (path is an example only):

   D:\XMS\snapshot>ftp <XMS server IP Address>

5. Log in as the root user and enter the following commands:

   ftp> cd <path to snapshot file>

   ftp> get <SnapshotName>

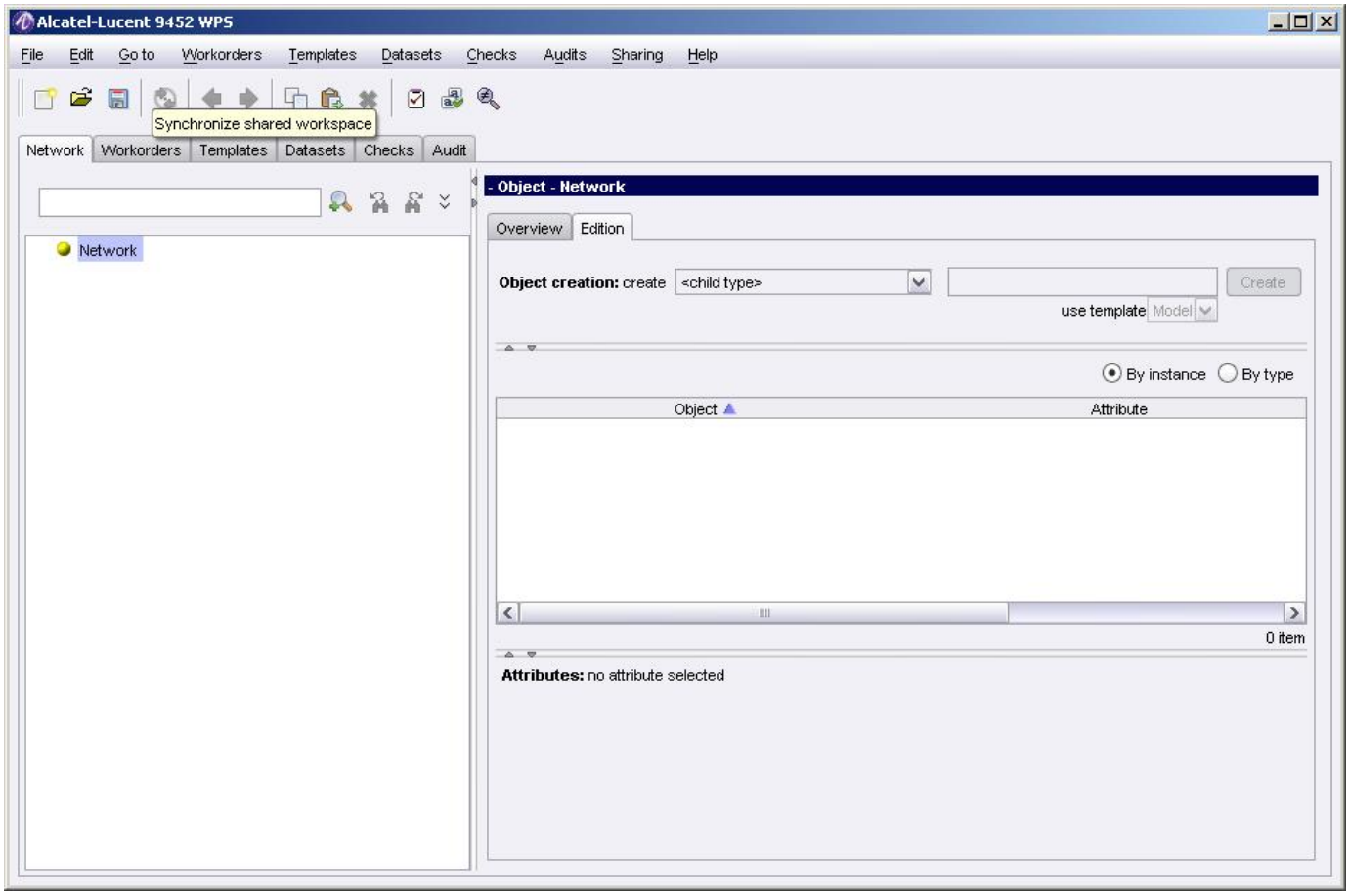
6. When the transfer is complete, enter the following command:

   ftp> quit

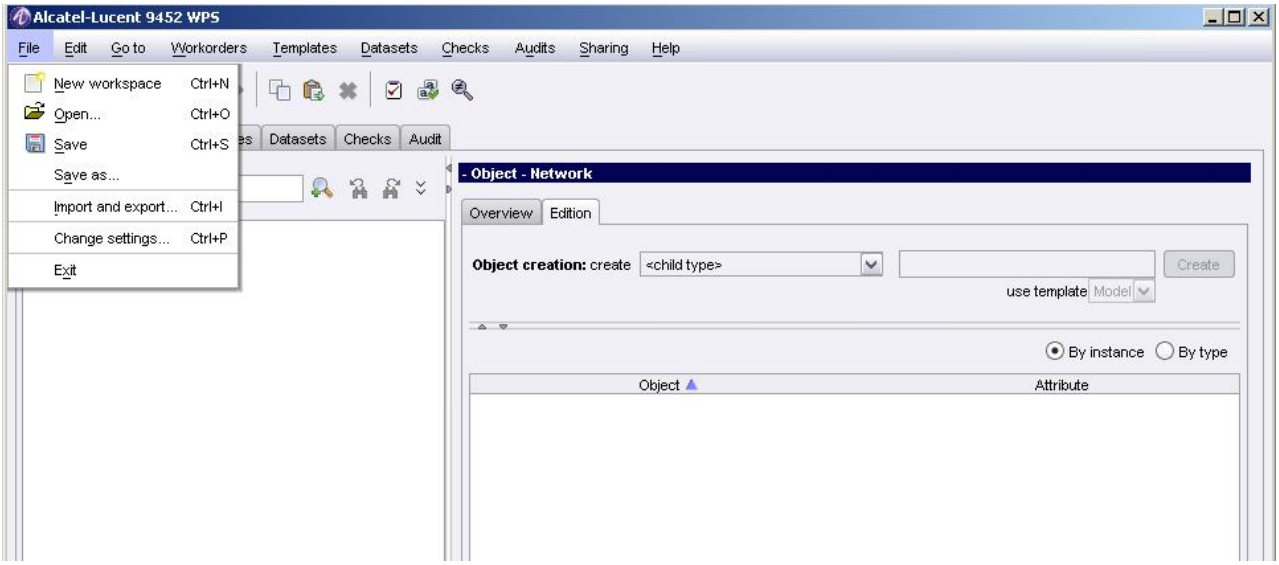
4.8.2 IMPORT SNAPSHOT FILE USING WPS

The WPS tool must be installed nominally on your PC Client.

1. Open WPS tool on your PC client with a new workspace.



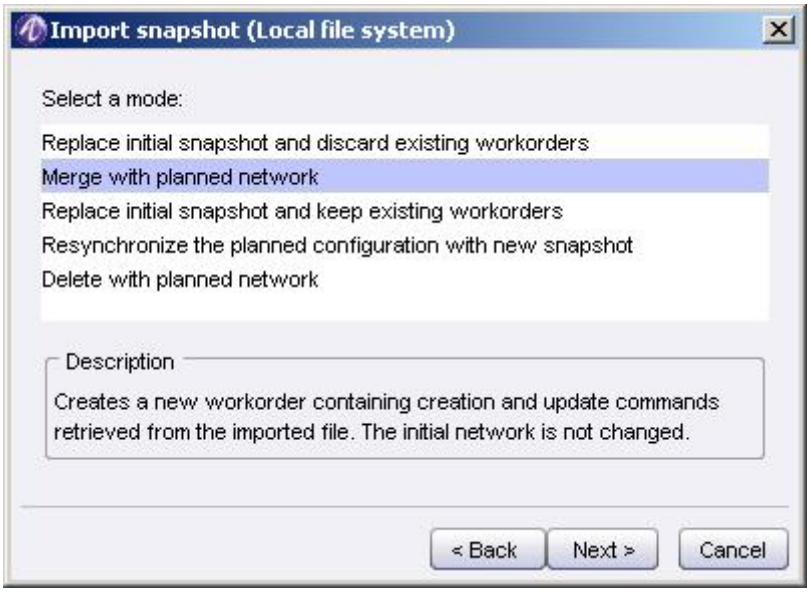
2. Choose File → Import and Export from the main menu. The Import and Export Wizard window opens.



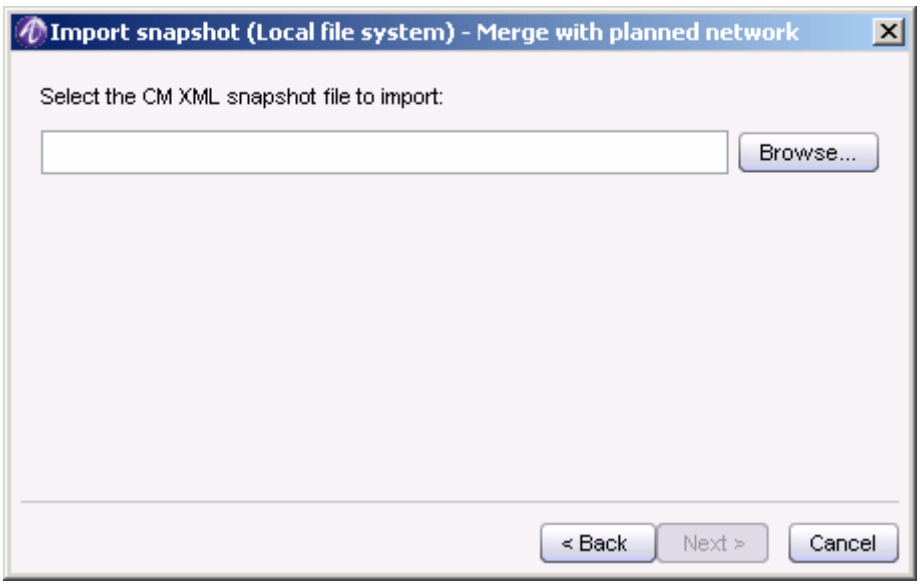
3. Perform the following steps:
    - In the Select an action to perform panel, choose Import Snapshot.
    - In the Source panel, select Local file system.
    - Click on the Next button.

4. In the Import Snapshot (Local file system) window, choose Merge with planned Network.

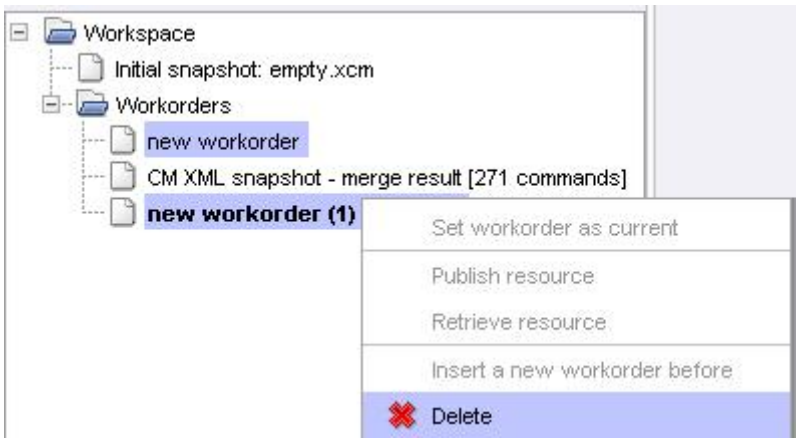
   Caution: Merge with planned Network is not the default option, and must be selected.



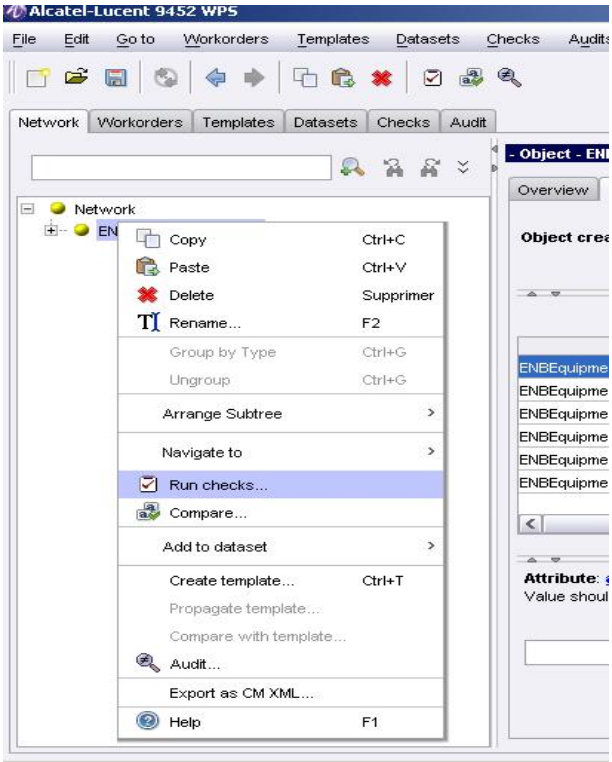
5. Click on the Browse button.



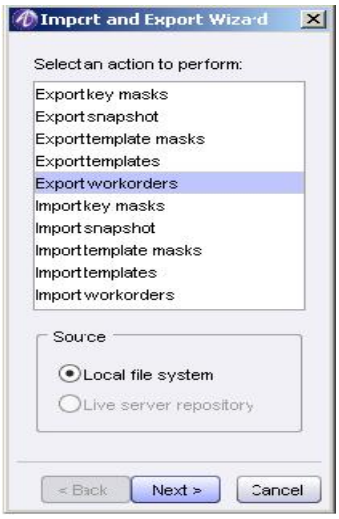
6. The Select a CM XML snapshot window opens. Navigate to the folder on your local machine where the CM XML file is located. Choose the file and click on the Open button.
7. Click on the Next button.
8. Click on the Next button to skip the optional filter step.
9. Select No, proceed without saving (cancel available) and click on the Start button.
10. Click on the Close button.
11. In the 9452 WPS main window, click on the Workorders tab.
12. Expand the Workorders folder and right-click on new workorder(s). Choose Delete from the contextual menu.



13. Click on the Yes button to close the confirmation popup. The delete workorder window opens.
14. Click on the Close button.
15. Click on the Network tab.
16. Right-click on Network (or an eNodeB) and choose Run Check from the contextual menu.



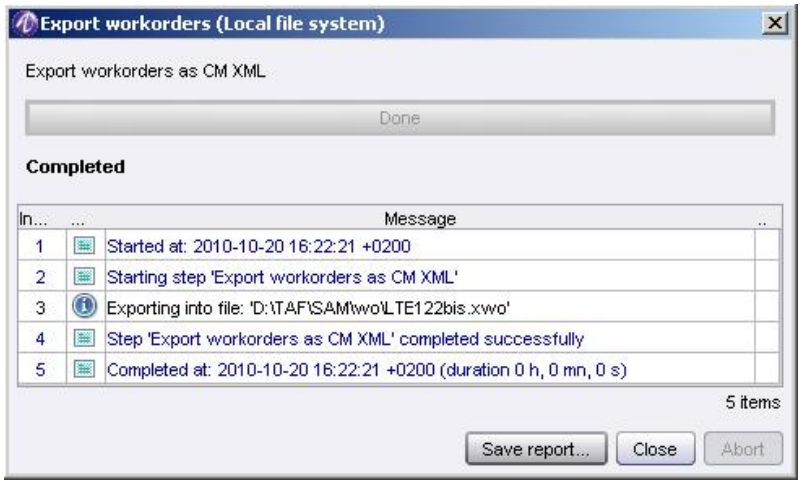
17. **IMPORTANT**: You must fix all Model and Engineering errors in WPS! You can ignore Warning messages. Only Error messages must be fixed in order to import the WO into the 5620 SAM server.
18. You can now use your local PC client to export the associated Workorder. Choose File → Import and Export from the main menu.



19. Choose Export Workorders from the list and click on the Next button.
20. Enter the name of workorder file to save, or click on the Browse button to specify a path and filename for the exported workorder.

21. Click on the Start button.

22. When the action has completed successfully, click on the Close button.



23. You must now transfer the generated workorder to the 5620 SAM server.

    In order to do that you can use a tool such as filezilla, or the sftp windows command (described below):

    ON PC CLIENT:

    Choose Start → Run from the Windows desktop.

    Enter cmd and click on the OK button. A command prompt window opens.

    Navigate to the local directory where you saved the workorder.

    Enter the following commands:

    D:\SAM\wo>sftp root@<SAM IP Address>

    Connecting to <SAM IP Address>...

    The authenticity of host '<SAM IP Address> (<SAM IP Address>)' can't be established.

    RSA key fingerprint is 64:41:86:51:11:9f:80:5f:ed:57:c8:74:5e:86:71:a9.

    Are you sure you want to continue connecting (yes/no)? yes

```
Warning: Permanently added '<SAM IP Address>' (RSA) to the list of known hosts.
Password: <SAM Root Password>
sftp> cd /opt/5620sam/server/nms/activation/wo_import
sftp> put <WorkorderName>
Uploading <WorkorderName> to
/opt/5620sam/server/nms/activation/wo_import/LTE122bis.xwo
<WorkorderName>  100%  174    0.2KB/s   00:00
sftp> exit
D:\SAM\wo>
```

The workorder is now in the proper directory in the 5620 SAM server.

4.9. 5620 SAM SERVER: MANAGE ENODEB

Verify that the steps in section 4.6 5620 SAM SERVER: PREPARATION have been performed successfully.

The 5620 SAM Client must be installed on PC client.

For more information about the following procedures, please refer to the [A3] document.

4.9.1 Open 5620 SAM Client

Open the 5620 SAM Client application and enter the admin login and password.

NOTE: You must create the SNMP user required for eNodeB management. See section 4.5.2.

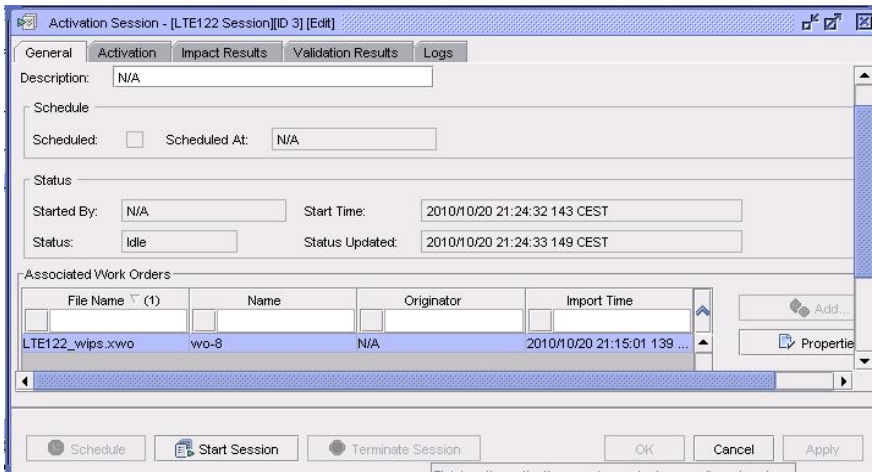
4.9.2 WorkOrder Activation

In the 5620 SAM client, choose Manage → Mobile Access → Activation from the main menu. The Activation form opens.

1. Click on the Create Activation Session button. The Activation Session (Create) form opens.
2. Configure the following parameters:

   Name: *<session name>*

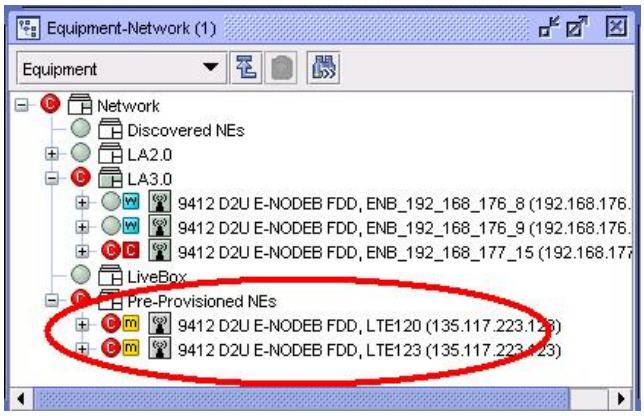
   Description: *<description>*
3. Click on the OK button to close the window and save the activation session.
4. Click on the Search button to display the activation session.
5. Double-click the activation session. The Activation Session form opens with the General tab displayed.
6. In the Associated Work Orders panel, click on the Add button. The Add window opens.
7. Click on the Search button.
8. Choose the dedicated Workorder from the list (flagged as CM XML snapshot - merge result in the Workorder Name column).
9. Click on the OK button to close the Add window. You are returned to the Activation Session form with the Activation tab displayed.
10. Click on the Start Session button.



11. Click on the eNodeB(s) displayed in the activation window. If the workorder contains several eNodeBs, you can multi-select by holding down the CTRL key and clicking on multiple eNodeBs.
12. In the Stages panel, choose Validation.
13. Click on the Validate button.
14. In the Stages panel, choose Activation.
15. Click on the Activate button. The workorder is activated.
16. In the Stages panel, choose Release.
17. Click on the Release button.
18. Click on the Terminate Session button.

NOTE: You can delete the activation session when workorder activation has been completed successfully. The workorder can only be associated with a single activation session at one time.

When these steps are performed without issue, the eNodeB(s) contained in the workorder appear under the Pre-provisionned NEs group in the Equipment-Network window.



4.9.3 eNodeB Discovery

In the 5620 SAM client, create the group(s) in which the discovered NE must be displayed.

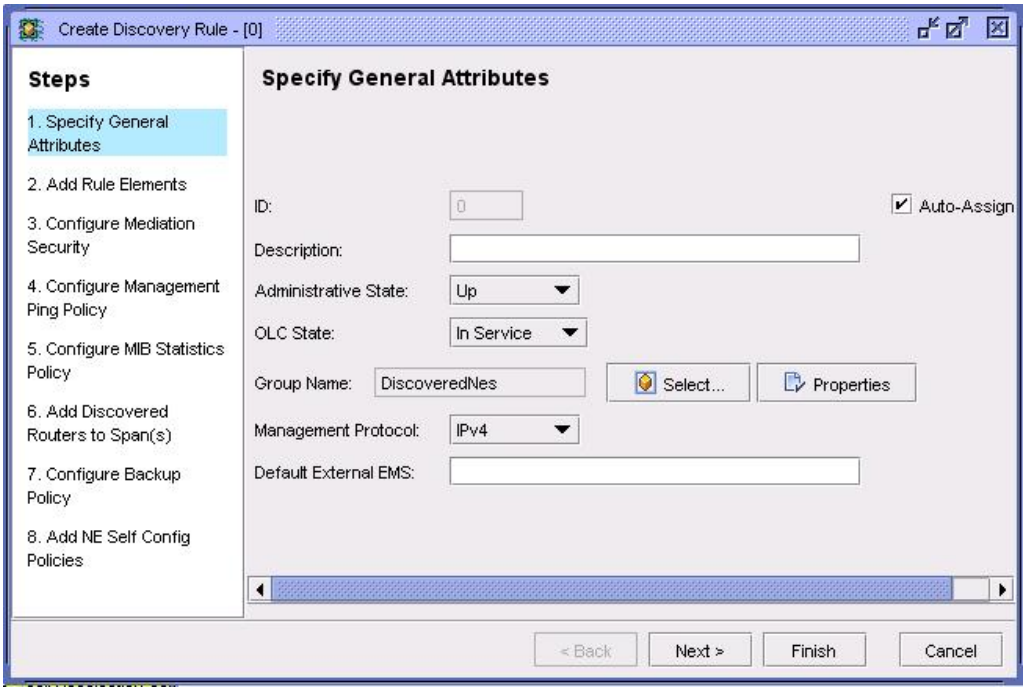
1. Select Equipment-Network view.
2. Right-click on Network and choose Create group from the contextual menu.
3. Configure the following parameters:

   Goup Name*: <Group name at user's discretion>*

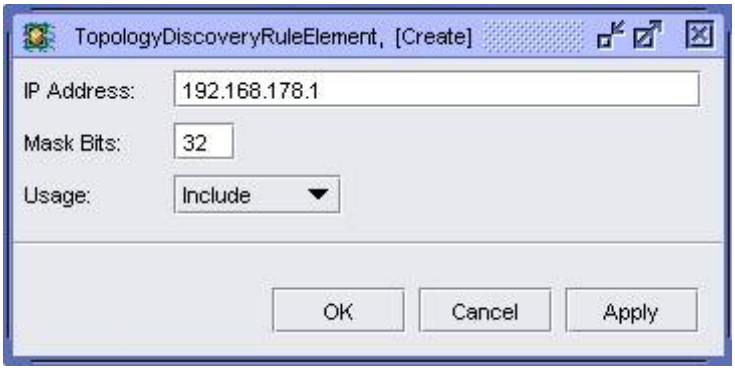
   Description*: <Group description at user's discretion>* (optional)
4. Click on the OK button**.**

In the 5620 SAM client, create the discovery rule for eNodeB management.

5. Choose Administration → Discover Manager from the main menu**.**
6. Click on the Create button.

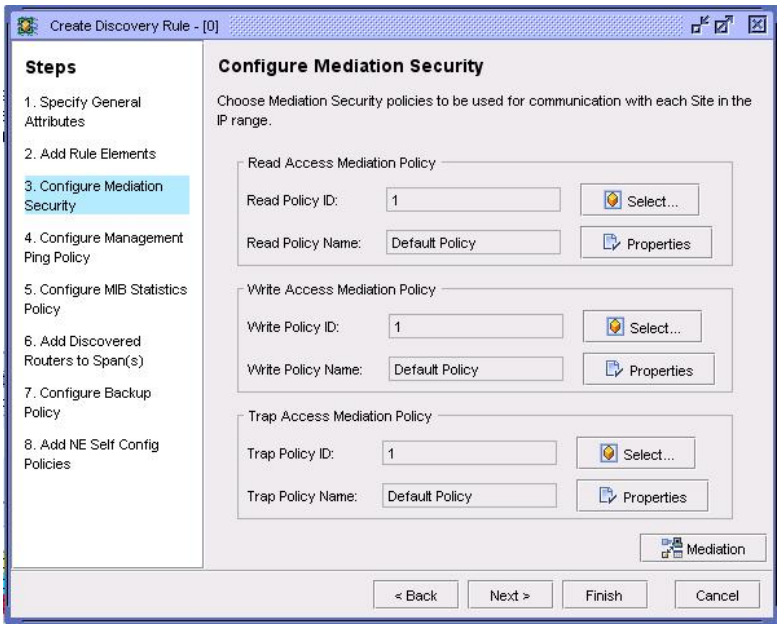


7. Specify General Attributes step:
   - Enter a description in the Description field.
   - In Group Name section, click on the Select button and choose the group that you created in step 3.
   - Click on the OK button.
   - Click on the Next button.
8. Add Rule Elements step:
   - Click on the Create button.



- Enter the management IP address of an eNodeB in the *IP Address field.*
- Click on the Apply button and enter more IP addresses**,** as required, to enter all the eNodeB management IPs. If the activated WorkOrder includes more than one eNodeB, (when migrating an eNodeB cluster), you must enter all the eNodeB IP addresses that are defined in the WorkOrder.
- Click on the OK button when all the required NEs are created.
- Click on the Next button**.**

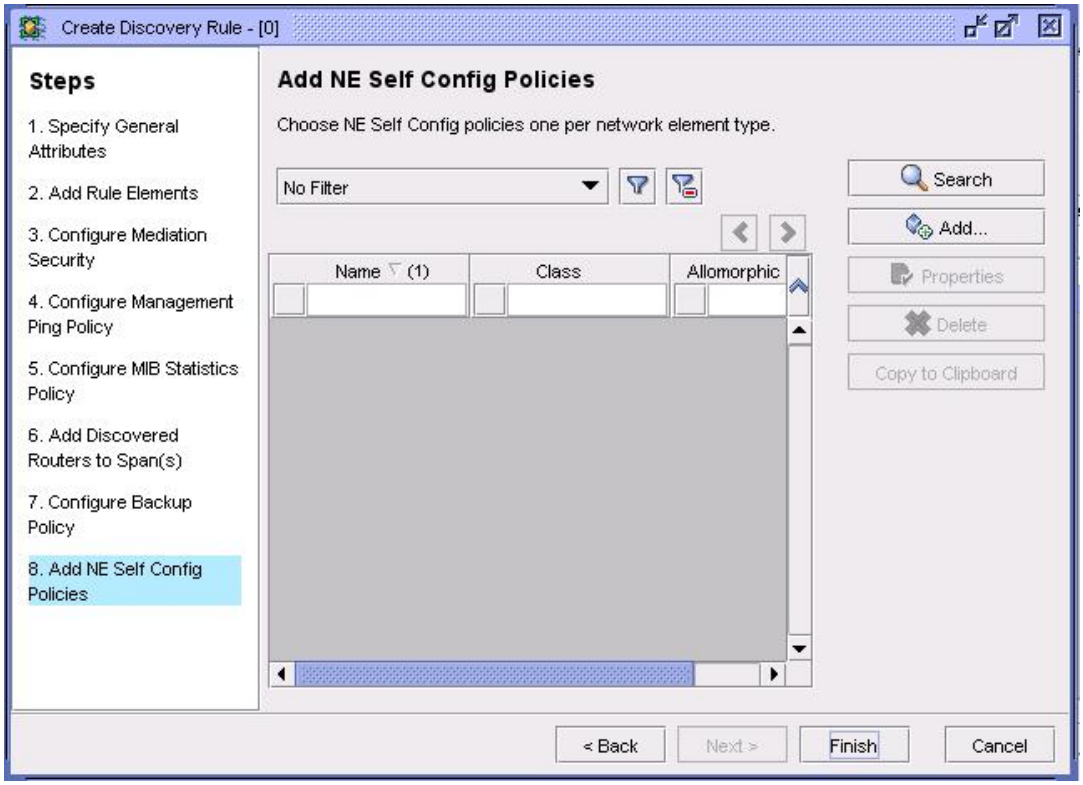
9. Configure Mediation Security step:
   - Click on the Select button for the Read Access Mediation Policy and select the dedicated mediation policy that was created previously for eNodeB management.
   - Click on the OK button.
   - Do the same for "Write Access Mediation Policy" and "Trap Access Mediation Policy"
   - Click on the Next button.



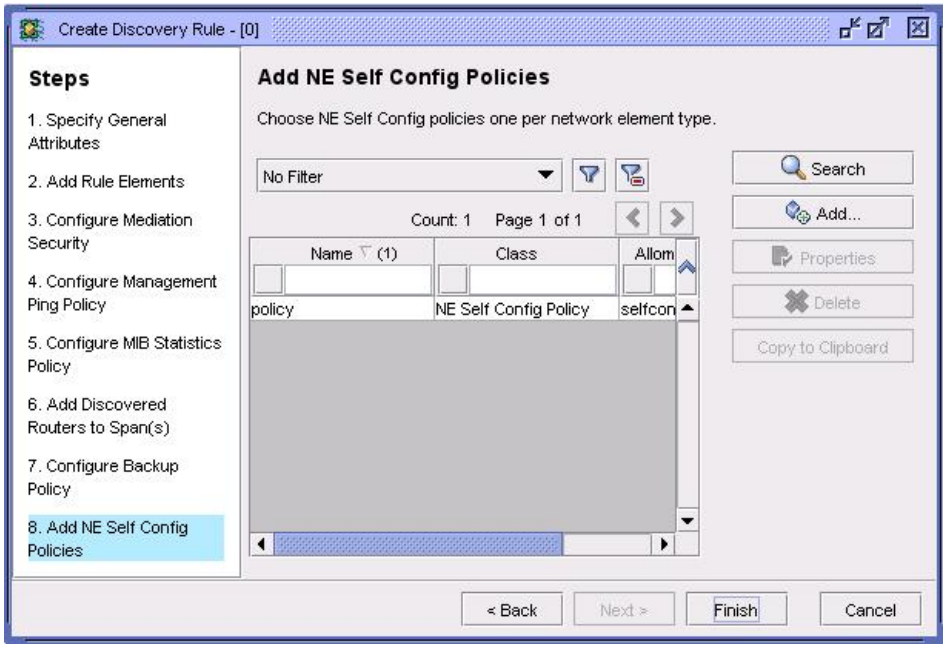
10. Configure Management Ping Policy: Skip this step by clicking on the Next button.
11. Configure MIB Statistic Policy: Skip this step by clicking on the Next button.

12. Add Discovered Routers to Span(s): Skip this step by clicking on the Next button.
13. Configure Backup Policies step:
    - Click on the Select button.
    - Choose the RAN Based Default Policy from the list and click on the OK button.
    - Click on the Next button.

14. Add NE Self Config Policies step:
    - Click on the Add button.
    - Click on the Search button.



- Choose the previously created self configuration policy from the list and click on the OK button.
- Click on the Finish button.



15. In the Discovery Manager form, click on the Apply button and confirm by clicking on the Yes button.
16. Click on the Resync Status tab in order to follow the device discovery.

NOTE: eNodeB resynchronization takes up to 7 minutes to complete.

17. When the eNodeB(s) display a status of Full Resync Done, you can UNLOCK the eNodeBs.

Note: The discovered NEs will move to the dedicated Network group.

4.10. ALARM MANAGEMENT

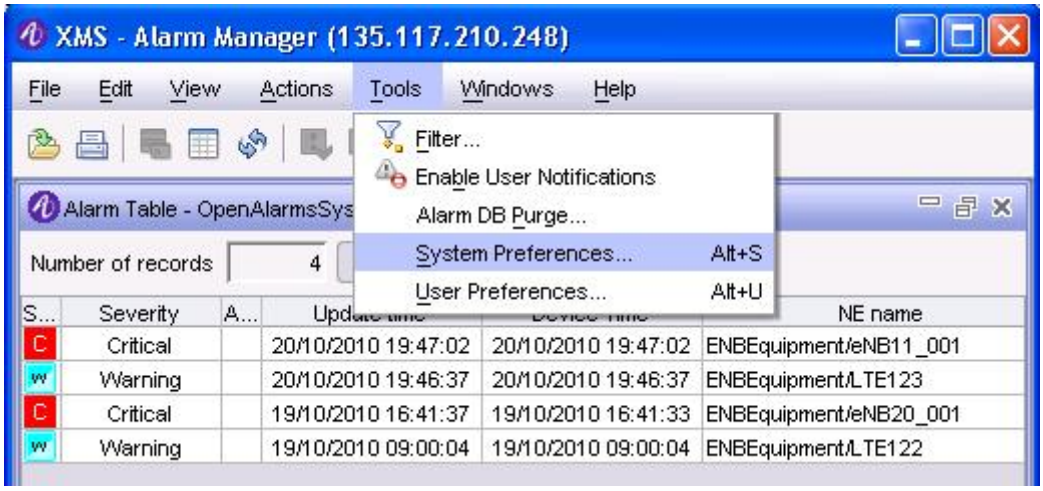
This section describes XMS alarm user preferences.

Note that historical alarms are not migrated.

4.10.1 Get XMS Information

1. In XMS WiBox (as the administrator user), click on the Fault Mangement icon.

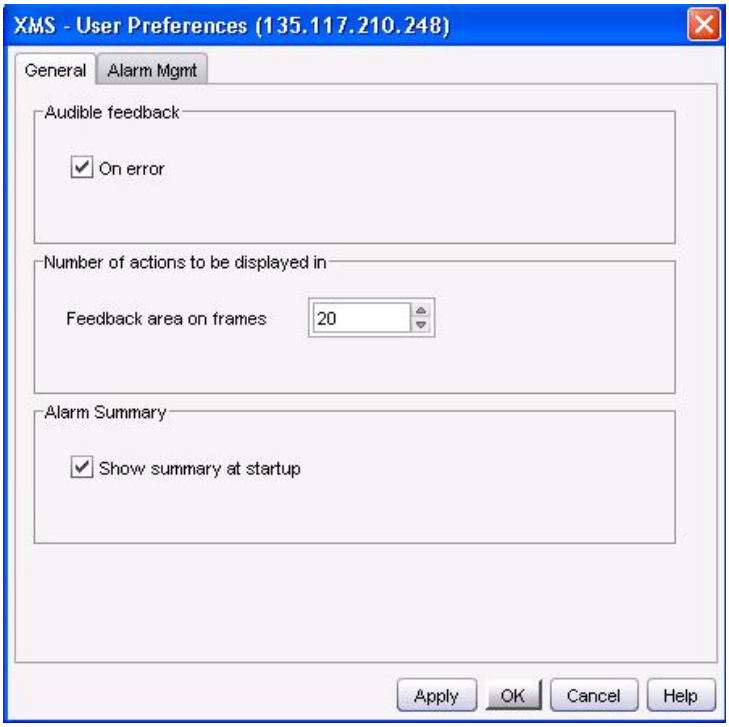
2. The XMS – Alarm Manager window opens.



3. Choose Tools → System Preferences from the main menu.

Make a note of the settings and save the preferences carefully.

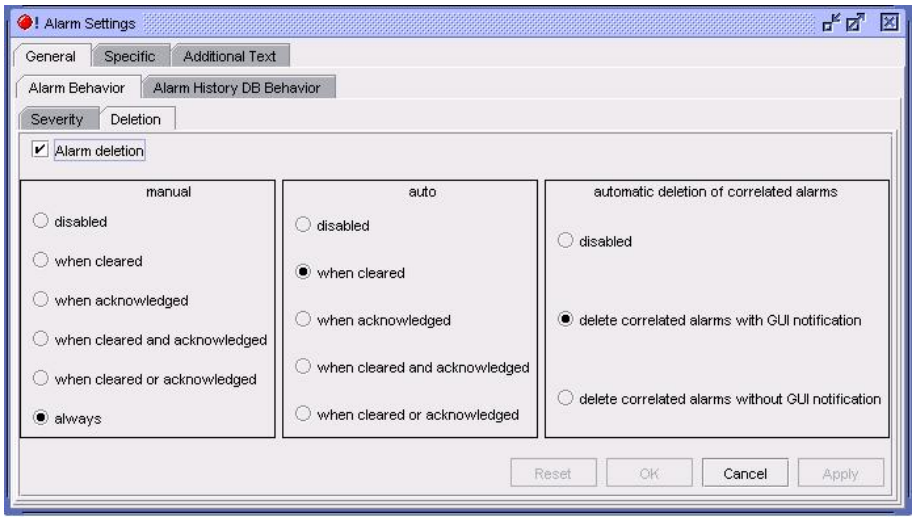
4. Choose Tools → User Preferences from the main menu.



Make a note of the settings and save the preferences in the General and Alarm Mgmt tabs carefully.

4.10.2 Configure 5620 SAM Alarm Management

1. In the 5620 SAM client (as the admin user), choose Administration → Alarm Settings from the main menu
2. Configure the alarm settings, as required.



3. Click on the OK or Apply button when finished.

4.11. PERFORMANCE MANAGEMENT MIGRATION

4.11.1 Action on XMS Server

In order to retrieve granularity period, perform the following steps on the XMS server:

1. On XMS Wibox, click on 'Wicl Console' icon
2. When wicl prompt displayed, enter the following command on the eNodeB (enter the command on all eNodeBs if you are migrating an eNB cluster):

ENBEquipment <eNodeB Name> obs 0 dis

Note: "0" is zero in the above command.

The following is displayed:

```
availabilityStatus          UNSET
operationalState            UNSET
pmcGranularityPeriod        15minutes
```

4.11.2 Configuration on 5620 SAM Server

Please refer to the [A3] document.

Do not forget to perform the steps in section 4.12.2 Stop connection between NPO and XMS server of this document if you are using an NPO server.

4.12. EXPORT NETWORK ELEMENTS

This section describes automatic NE export.

On XMS server:

If you want to export the XMS crontab entries to the 5620 SAM server, you must remove following line previously:

15 2 * * * /opt/oam/shell/wlm/wlm_cli.sh -export > /dev/null 2>&1

On 5620 SAM server, follow the procedures in section 6.3 Configuration snapshots of the [A3] document to create a configuration snapshot.

4.13. NPO DATA SOURCE MANAGEMENT

This section describes how to switch the current NPO data source from the XMS server to the 5620 SAM server. You must undeclare XMS as the OMC data source and declare the 5620 SAM as the OMC data source.

4.13.1 Undeclare the XMS server

Please refer to chapter 7 of the [A4] document in order to undeclare the datasource for parameters (PARAM) and QoS (QOS) on the XMS server.

4.13.2 Declare the 5620 SAM server

Please refer to chapter 7 of the [A4] document in order to declare the 5620 SAM server as the data source for parameters (PARAM) and QoS (QOS).

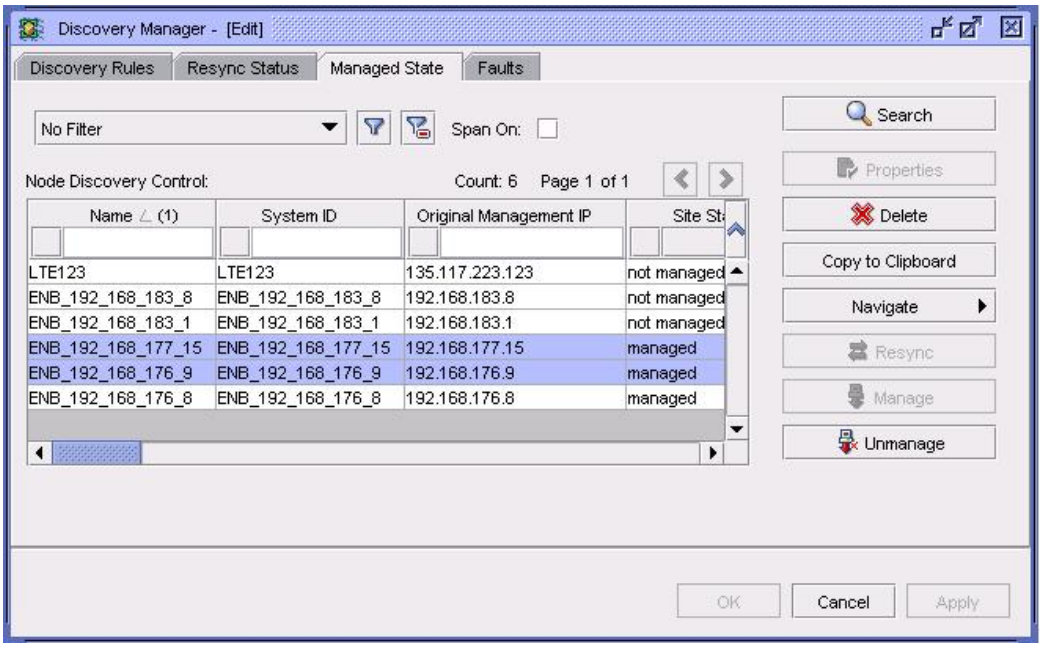
In order to be able to use the NPO on the 5620 SAM server, Performance Management must be correctly configured on the 5620 SAM server.

4.14. REVERSE PROCEDURE

This section describes how to unmanage the eNodeB(s) in the 5620 SAM server and manage them with the XMS server.

4.14.1 Unmanage eNodeB(s) in 5620 SAM

1. Log in to the 5620 SAM client as the admin user.
2. Choose Administration → Discovery Manager from the main menu.
2. Click on the Managed State tab.
3. Select all eNodeB(s) that are to be unmanaged in the 5620 SAM server. You can multi-select by holding down the CTRL key and clicking on multiple eNodeBs.
4. Lock the OAM link.
5. Click on the Unmanage button.
6. Wait until the Site State status displays "not managed."
7. Click on the Delete button.
8. You can also remove the dedicated rule in the Discovery Rules tab.



9. Close the 5620 SAM client.
10. Log on to the 5620 SAM server as the root user and enter the following commands to stop the server application.

    NOTE: only perform this step if the 5620 SAM is not being used to manage network elements

    # /etc/rc3.d/S975620SAMServerWrapper stop

    # su – samadmin

```
-bash-3.00$ /opt/5620sam/server/nms/bin/nmsserver.bash  stop
-bash-3.00$ exit
```

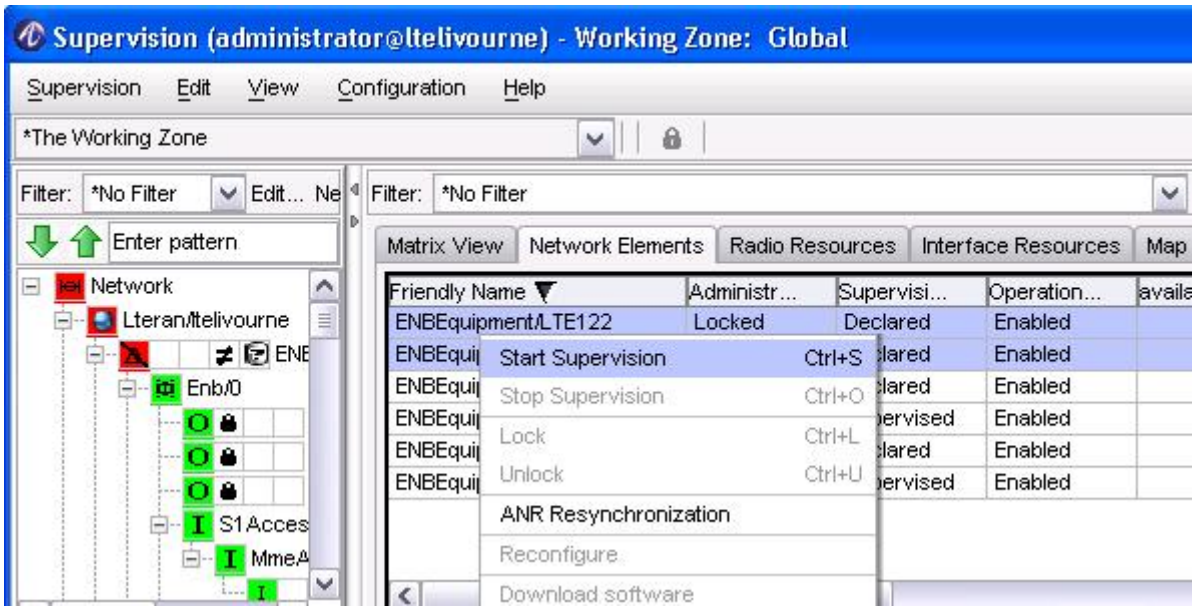
4.14.2 Start eNodeB Supervision from XMS

1. Log on XMS server as the oamops user and enter the following command to restart the XMS applications:

   ```
   (oamops) % /opt/oam/exe/pmgt/svcadm.x enable /application/xms/xms
   ```

2. Wait until the XMS server starts. This will take several minutes.
3. Open the XMS Wibox, as described in the XMS User Guide (http://<IP address of XMS server>:8080).
4. Log in to the XMS Wibox as the administrator user.
5. Click on the Supervision icon.

6. In the Supervision – Working Zone: Global window, select all of the eNodeB(s) that were previously unmanaged on the 5620 SAM server. Right-click on the eNodeB(s) and choose Start supervision from the contextual menu. You can now unlock the eNodeB(s).



7. Check in XMS that your eNodeB(s) are correctly supervised.

5. LIST OF KNOWN PROBLEMS

Please refer to 5620 SAM RLN for more information about 5620 SAM issues that have not been fixed in current software load.