ip access
Small cells everywhere

nanoLTE

High speed coverage
where it's needed most

nanoLTE AP Pre-Provisioning and Configuration

NANO_INST_43370 101_0.4

ip.accessLtd
Building 2020
Cambourne Business Park
Cambourne
Cambridgeshire
CB23 6DW
United Kingdom

Notices

The documentation and/or software may provide links to Web sites and access to content, products, and services from third parties. ip.access is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. ip.access is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. ip.access is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

ip.access Limited is a Private Limited Company Registered in England and Wales
Company No. 03400157

Registered Office:
Building 2020
Cambourne Business Park
Cambourne
CB23 6DW
UK
Tel: +44 (0) 1954 713 700
Fax: +44 (0) 1954 713 799

Further company information may be found at www.ipaccess.com.

Revision History

Version	Change Summary	Date	Author
101_0.1	First Draft for N4G_1.1	13 Oct 2015	AM4
101_0.2	Add miscellaneous parameter section to network-wide settings, move provisioning overview to a separate section	31 Mar 2016	AM4
101_0.3	Add AP Info template information and update references to other manuals	03 Jun 216	AM4
101_0.4	Add hardware capability equivalence statement for 248 and 278, update UL/DL bandwidth according to support by frequency band	19 Jul 2016	AM4

Table of Contents

1 Introduction

The ip.access nanoLTE AP is an indoor Access Point for Enterprise and SOHO applications.

Use the step-by-step procedures in this manual to pre-provision a new nanoLTE AP in the NOS so that the AP is ready to provide service after obtaining its configuration from the NOS.

This manual only describes how to use the NOS Client to pre-provision a nanoLTE AP in the NOS. This manual provides no information about site installation of AP hardware. For information about installing nanoLTE AP hardware on site, see [INST_43311].

1.1 Installation Tasks

To make a new nanoLTE AP ready to provide service, complete the following tasks:

- System preparation and AP pre-provisioning in the NOS, as described in this manual - see section 2 for an overview
- Site installation of the AP hardware - see [INST_43311] for nanoLTE AP hardware installation requirements and procedures

These tasks can be completed in any order. In most cases, however, the most practical approach is to pre-provision an AP in the NOS before final site installation.

1.1.1 First AP Startup

In summary, assuming that all preparation and installation tasks are complete, the first AP startup will take place as follows:

- The AP sets its date and time with NTP - this is mandatory for certificate validation
- The AP connects to the Redirector to obtain its unique OLM Package (see the assumptions in section Assumptions About the nanoLTE AP) - the AP also contacts a CRL as part of this procedure to validate the Redirector certificate
- The AP uses the DOCP parameters and certificate from the OLM Package (see section Network-Wide AP Commissioning Parameters for a summary of the DOCP parameters) to establish an IPsec tunnel with its serving SecGW - the AP also contacts a CRL as part of this procedure to validate the SecGW certificate
- The AP connects to its serving NOS via the SecGW and performs its first Inform() procedure to obtain the configuration that is pre-provisioned in the NOS - this may also trigger a software update from the NOS if the current AP software is older than the software version associated with the AP's assigned Product Class (see section Product Class and AP Software Version Objects)
- The AP uses the downloaded configuration to connect to the core network, bring up its cell and enter service

Hence this manual is about ensuring that the last two phases of this process take place successfully. See section Pre-Provisioning Overview for an overview of the activities and procedures in this manual.

Note: For a more detailed first startup sequence, in case the AP has difficulty connecting to its serving NOS, see [TRB_43005].

1.1.2 Assumptions About the nanoLTE AP

It is assumed that any secure nanoLTE AP (278 variants of the nanoLTE E40 AP) supplied to an operator has already been processed by the Redirection System. Hence the Redirector will already contain the unique OLM Package for the AP, ready for the AP to download on first startup or following a factory reset.

The OLM Package contains the parameters that an AP uses to connect to its serving IPsec Security Gateway and NOS. Collectively, these parameters are called the DOCP (Default Operator Connection Point). For a summary of these parameters, see section Network-Wide AP Commissioning Parameters. For more information on the Redirection System, see [GST_14700].

1.2 User Requirements

It is assumed that any readers that will use the NOS Client already know how to:

- Start the NOS Client
- Navigate the Explorer Pane to find an AP object

It is also assumed that the any readers that will use the NOS Client will have suitable user privileges for the NOS Client.

Refer to [OPM_14015] for information on using the NOS Client.

1.3 Hardware Equivalence for 248 and 278 Product Variants

The 248 and 278 product variants have an identical hardware build for each set of supported bands. Hence the hardware build is identical in each of these cases:

- 248J and 278J
- 248L and 278L
- 248M and 278M

The only difference between 248 and 278 variants is that internal fuses within the processor are configured on the 278 variants in order to store unique security information, allowing the product to boot up securely.

Note: To implement the added security, the software/firmware has been adjusted for the 278 variants. Product operation and in particular the RF operation of this variant is not altered in any way. The RF Technology (LTE), frequencies and power level are identical between both variants.

In respect of the 248M and 278M variants of the nanoLTE E40 AP, ip.access has reviewed the Software Changes section of the FCC Permissive Changes Document dated 16th Oct 2015. It has been determined that the difference between these two product models can be classed as a permissive change.

Note: In general, it is expected that this manual will primarily be used for pre-provisioning the 278 variants of the nanoLTE AP, which obtain their connection parameters via the Redirector (see section 1.1.2). The 248 variants of the nanoLTE AP must be provisioned with the parameters that allow them to connect to the NOS in a different way, as described in *NANO_INST_43005 nanoLTE AP Quick Start Guide* (as applicable to the 248 variants only). There are no further references to this provisioning method in this manual.

1.4 Related Information

[GST_14415]	NOS Bulk Provisioning Feature (NANO_GST_14415)
[GST_14700]	Redirection System Overview (NANO_GST_14700)
[GST_41050]	nanoLTE System Planning (NANO_GST_41050)
[GST_43415]	nanoLTE Network Listen (NANO_GST_43415)
[INST_14300]	NOS Configuration (NANO_INST_14300)
[INST_43311]	nanoLTE AP Hardware Installation (NANO_INST_43311)
[INST_43375]	nanoLTE AP Long Range Extension Setup (NANO_INST_43375)
[INST_43380]	nanoLTE AP Templates for Provisioning (NANO_INST_43380)
[OPM_14005]	NOS Server Operations (NANO_OPM_14005)
[OPM_14015]	NOS Client Operations (NANO_OPM_14015)
[OPM_43005]	nanoLTE AP Operations (NANO_OPM_43005)
[REF_11105]	System Glossary (NANO_REF_11105)
[REF_43005]	nanoLTE AP Open Source Software (NANO_REF_43005)
[REF_43150]	nanoLTE AP Data Model CM Reference (NANO_REF_43150)
[REF_14490]	NOS Northbound SOAP/XML API Reference (NANO_REF_14490)
[TRB_43005]	nanoLTE AP Troubleshooting Manual (NANO_TRB_43005)
[21.905]	Vocabulary for 3GPP Specifications (3GPP 3G TR 21.905)

1.5 Licenses and Copyright Notices

Portions of the AP are constructed from third-party software and open source code and ip.access Ltd gratefully acknowledges the contributions that these libraries, technologies and components have made to the product. Each of these is supplied under the terms of a license agreement and these are either reproduced or referenced in [REF_43005], in line with the stipulations of their authors.

1.6 Terminology

Common System terminology is defined in [REF_11105].

For additional terminology, see [21.905].

2 *Pre-Provisioning Overview*

The objective of the procedures in this manual is to provide a nanoLTE AP with a working configuration, stored in the NOS. That is, to pre-provision the AP in the NOS so that the AP can download the configuration from the NOS and successfully start to provide service.

The topics in this section are:

- *2.1 End-to-End Provisioning Summary*
- *2.2 Planning - Determine and Plan Network Policies and AP Parameters*
- *2.3 Preparation - General System Preparation and Templates*
- *2.4 Pre-Provisioning nanoLTE APs in the NOS*
- *2.5 Post-Installation Checks*

2.1 End-to-End Provisioning Summary

Pre-provisioning the nanoLTE APs in the NOS requires the following activity phases:

- Planning:
  - Determine and plan network policies
  - Plan for the parameter settings that are unique for each AP
- System preparation:
  - General system preparation
  - Create nanoLTE AP templates based on policies and system preparation
- **Pre-provisioning nanoLTE APs in the NOS**
- Post-installation checks

The tasks leading up to nanoLTE AP pre-provisioning ensure that all network-wide choices and policy decisions have been made and all system preparation is complete prior to pre-provisioning any APs. Hence the pre-provisioning procedure itself, which is required per AP, should be straightforward.

2.2 Planning - Determine and Plan Network Policies and AP Parameters

In this phase, determine and plan network policies that affect shared parameter settings and AP management settings in the NOS. This may also affect core network configuration but core network configuration aspects are outside the scope of this manual.

This should be a one-off activity for new deployments only. However, it may be useful to revisit the policies from time to time.

The relevant sections of this manual are:

- *3 Capturing Network Policies and AP Modes*
  See this section for general network policies, including AP naming policies in the NOS and different levels of planning for AP parameter scope (network wide, groups of APs by use case, etc.).

- *4 AP-Unique Parameters*
  See this section for information about the AP parameters that must be unique to each AP.
- *8 How to Implement Policies*
  Also see this section for supplemental information on implementing AP parameter usage according to different policies. For example, see section 8.3 for information about determining an appropriate Periodic Inform Interval across the nanoLTE System.

2.3 Preparation - General System Preparation and Templates

In the context of this manual, this mainly means preparing the NOS so that it is ready for nanoLTE AP pre-provisioning. However, as per the assumptions in section 5.1, it is assumed that the NOS has been installed correctly and that the required NOS services are operational and that any other required configuration is complete.

The relevant sections of this manual are:

- *5 System Preparation for nanoLTE AP Provisioning*
  Follow the procedures in this section to prepare the NOS for nanoLTE AP pre-provisioning, including: creating MME objects, placing AP software on the NOS server, creating AP SW Version and Product Class objects, ensuring the LTE APs object is present, checking the configuration of the APs object, optionally creating AP Group objects and optionally preparing Neighbour Cell objects.
- *6 Template Preparation*
  Use this section as a template strategy guide. The procedures to create templates are in [INST_43380]. As a minimum, create the Mandatory Settings Template that contains CQI to DSCP mappings and AP temperature settings.

In parallel to this, it is further assumed that the preparation of external systems (outside the NOS) is complete:

- NTP servers are operational
- The required IPsec SecGW is operational and ready to establish IPsec tunnels with the APs
- The core network is ready for S1AP connections from nanoLTE APs
- All other supplemental network systems are ready, including but not limited to: firewall configuration, network switching, DNS and gateways

The correct preparation of these external systems is outside the scope of this manual.

2.4 Pre-Provisioning nanoLTE APs in the NOS

Use any of the following methods for pre-provisioning a nanoLTE AP in the NOS:

- Use the Create Site Wizard in the NOS Client
- Use the SOAP/XML interface
- Use the Bulk Provisioning interface

The planning and preparation phases leading up to pre-provisioning are common to all these AP pre-provisioning methods.

2.4.1 Create Site Wizard

See *7 AP Provisioning* for full details on using the Create Site Wizard in the NOS Client to pre-provision an AP in the NOS.

2.4.2 SOAP/XML Interface

The SOAP/XML interface provided by the NOS offers is suitable for pre-provisioning APs from external provisioning systems, typically with some automation for creating the SOAP/XML provisioning requests.

Further information about using SOAP/XML is outside the scope of this manual.

For information about the SOAP/XML interface provided by the NOS, including the IRP for nanoLTE AP provisioning, see [REF_14490].

2.4.3 Bulk Provisioning Interface

The Bulk Provisioning interface provided by the NOS is also suitable for pre-provisioning APs from external provisioning systems. Typically this depends on some automation for creating the XML batch files that create the AP Info and AP objects that comprise each AP site definition. The AP Info and AP object details for a new AP site must both be in the same XML file, but each XML batch file can also define multiple sites (hence "bulk provisioning").

The XML batch file uses the same format as the Load/Save Attributes function, but should not include any read-only attributes or parameters.

Further information about using Bulk Provisioning is outside the scope of this manual.

For information about the Bulk Provisioning interface provided by the NOS, see [GST_14415] and [OPM_14015].

2.5 Post-Installation Checks

See *9 Installation Checks* for basic checks to verify that the AP is successfully pre-provisioned. The activities in this section assume that the AP has now been powered up and connected to the backhaul.

If an AP has difficulty connecting to the NOS, see [TRB_43005] for troubleshooting information.

3 *Capturing Network Policies and AP Modes*

This section summarises the considerations that affect AP provisioning policies. This is inclusive of all parameters from the data fill in the CIQ that are applicable to nanoLTE AP provisioning.

The topics in this section are:

- *3.1 Parameter Categories*
- *3.2 Customer Policies*
- *3.3 AP Naming Policies and Management Identities*
- *3.4 Network-Wide AP Commissioning Parameters*
- *3.5 Network-Wide AP Provisioning Parameters*
- *3.6 Parameters Shared by a Group of APs*
- *3.7 "Per AP" Parameters*
- *3.8 Other AP Parameters*

3.1 Parameter Categories

3.1.1 Mandatory Network-Wide Parameters

Many of these parameters have no default value, but are common across the whole network. They are typically identities representing the network and its common resources (e.g. NTP Servers). When pre-provisioning APs in the NOS, use templates to consistently apply these parameters to all APs. For example:

- PLMN ID (MCC + MNC) - usually the same across the whole network

3.1.2 Network-Wide Policy Parameters

These are parameters that have a sensible default value, but the default may not match an operator's preferred policy. Once selected, the value is common across the network. When pre-provisioning APs in the NOS, use templates to consistently apply these parameter changes to all APs. For example:

- Management traffic DSCP marking

3.1.3 Shared Parameters

These are parameters that may have no sensible default value, but the same value is shared by many or all APs. When pre-provisioning APs in the NOS, use templates to consistently apply these parameters to all APs. For example:

- PLMN IDs to scan with Network Listen

3.1.4 Deployment Mode Parameters

These parameters reflect different AP use cases or modes of operation. These use-cases are captured in a specific collection of parameters and associated values. After initial provisioning in the NOS, apply suitable deployment mode templates to the required APs to modify their configuration from the baseline. For example:

- AP group - typically for regionalising AP management

3.1.5 Mandatory AP Unique Parameters

Some parameters must be unique per AP, such as identities and descriptions. Most are assigned during pre-provisioning but some parameters must be applied after an AP is provisioned. For example:

- Cell Identity - assigned during pre-provisioning
- Location (latitude, longitude and radius of uncertainty) - assigned during pre-provisioning
- Static neighbour list - assigned after an AP is provisioned (usually with the Static Neighbour List wizard)

3.2 Customer Policies

Considerations that will affect parameter settings for AP provisioning include:

- AP Naming policies and Identities
    - Decide on site naming and cell ID policies and associated file-naming policies for uploads
    - These are configured into “central” NOS parameters and per-AP parameters
- AP scenarios, operation and associated parameters
    - Identify key use cases
    - Define associated policies/settings, for example:
        - Management interaction (inform interval, upload frequency)
        - Power limits
        - Synchronisation sources

As part of the Network Design, the above considerations should have been used when capturing information in the CIQ (Customer Information Questionnaire). The CIQ is a data fill that must be completed before beginning a new deployment. A brief overview of the CIQ parameter groupings follows with the subsequent sub-sections containing detailed parameter lists.

Note: It is assumed that the CIQ has already been completed and that all the required parameter values are now known. This discussion is about how to use the parameters. Also, the parameter groups affect template construction, as in section 6 and [INST_43380].

Network-wide AP commissioning parameters, as delivered to all APs in the DOCP (Default Operator Connection Point) set of parameters:

- NTP server address
- IPsec configuration
- CRL Mirror address
- NOS address

Mandatory Network-wide identities and network resources, to be set via a network-wide global template, including:

- The Operator’s identities MCC/MNC
- Timezone
- Addresses of shared network resources (NTP Servers, IPSec GW, traffic Selectors, PM Upload Servers, Mirror CRL Server)
- Some RAN details to be aligned with existing operator policy

Parameters shared by groups of APs, to be set by use case templates:

- TAC
- Macro cell Tx threshold

Per AP parameters, such as:

- An RF Resource "pool", which may be separate from the macro network, from which individual AP settings are chosen

The sub-sections covering the CIQ groups above are followed by further sub-sections about other parameter considerations for AP provisioning, such as AP groups.

3.3 AP Naming Policies and Management Identities

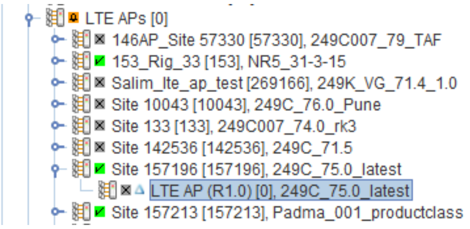
It is important to have a clear policy on how APs are named for management purposes, as this affects not only the display in the NOS Client, but also the names and contents of Performance Management counter files and the contents of the SNMP Traps sent on the NOS Northbound interface.

3.3.1 Site ID and Site Name Display in the NOS Client

The Site ID is a numeric identifier for the AP and the Site Name is a textual name. When using the NOS Create Site Wizard the NOS automatically generates a Site Name of "Site <Site ID>", but this can be changed by the user if desired. The Site ID must be unique. The NOS enforces uniqueness of the numeric Site ID, but not the Site Name.

- It is recommended that the AP Serial Number is NOT used as a basis for the Site ID as this could result in confusion if the AP is subsequently swapped. For example, due to a failure.
- Site ID could be associated with the AP's on-air Cell-ID, provided the customer is confident the Cell-ID will not be changed for any reason.

Each AP Info object is labelled with the Site Name, Site ID in square brackets and the currently provisioned Product Class in the NOS Client:



```
LTE APs [0]
  146AP_Site 57330 [57330], 249C007_79_TAF
  153_Rig_33 [153], NR5_31-3-15
  Salim_lte_ap_test [269166], 249K_VG_71.4_1.0
  Site 10043 [10043], 249C_76.0_Pune
  Site 133 [133], 249C007_74.0_rk3
  Site 142536 [142536], 249C_71.5
  Site 157196 [157196], 249C_75.0_latest
    LTE AP (R1.0) [0], 249C_75.0_latest
  Site 157213 [157213], Padma_001_productclass
```

Note: The Site ID is taken from the AP Info object's Object Instance ID. In most cases, the NOS automatically assigns an Object Instance ID to new objects. However, in the case of APs, this is configurable to allow the use of a meaningful numeric identifier.

Each AP object is labelled with its object name, the instance ID (always [0]) and the currently provisioned Product Class. The object name is assigned automatically, and is the display name of the current class of the AP object. Hence this changes automatically when an AP is upgraded to a different Product Class that is associated with a different AP class.

3.3.2 PM Filenames and Identities in PM Files

While 3GPP defines structures for filenames and file contents, it is not prescriptive on exactly how the associated identifiers are used.

PM File Names

The LTE AP PM file names have the following format:

```
<Type><Startdate>.<Starttime>-<Enddate>.<Endtime>-<jobId>_<UniqueId
>
```

The jobId is based on an AP parameter of the same name which defaults to blank, but its use in the filename can also be modified by two NOS policy parameters, which can be applied separately or in unison.

- To ensure the filename is unique it is suggested that a NOS option (“Append Equipment ID to Job ID”) is enabled to append the Equipment ID (which includes the Serial Number) to the Job ID. This option is enabled by default.
- The NOS can also be configured to auto-generate a Job ID from the concatenation of the AP’s Group ID and Provisioned Product Class parameters (via the “Generate AP Job ID” attribute). “Group” is a flexible concept that can be used to associate a set of APs, for example identifying APs within a geographic region. The Provisioned Product Class is typically used to represent an AP “type” e.g. E40, but can also be used to identify the use case of the AP, e.g. “E40 SoHo”. So having policies for these parameters can help in grouping PM files.

The UniqueId is set to the AP’s Object Name. If the operator has a rigorous naming policy this can be used to create unique filenames to the operator’s preferred policy.

In this case the (“Append Equipment ID to Job ID” option would not be necessary. Alternatively, the Object Name can be left at its default (“LTE_AP” for an AP) if the preference is to use other identities.

Example list of parameter values and resulting PM file name:

- generateJobId = TRUE
- appendEquipmentId = TRUE
- Group name (from the objectName of the associated Group) = “NewJersey”
- provisionedProductClass = “E40”
- objectName = “LTE AP”
- EquipmentId = 000295-0000011115

Example resulting PM Filename, with automatically generated date and time stamp:

```
C20130806.1700+0000-20080807.0500+0000-NewJersey_E40_000295-0000011
115_LTE_AP
```

Identities in PM File Headers

While the filename can be configured to provide a unique name related to the AP, the PM File header also includes identity information:

- DN Prefix – user-configurable text. By appropriate configuration this can be combined with the Local DN to generate a full DN
- Local DN - this attribute is set based on the class type and the object instance ID of the AP object. This is typically “AP#0”.
- User label – set to the AP’s Object Name (the same parameter used for unique-id in the filename)
- Job ID – the same parameter as the Job ID in the file name, subject to the same NOS policy parameters.

Example PM File header:

```
<?xml version="1.0" encoding="UTF-8"?>

<mc:measCollecFile
xmlns:mc="http://www.3gpp.org/ftp/specs/archive/32_series/32.435#me
asCollec" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.3gpp.org/ftp/specs/archive/32_series
/32.435#measCollec pm_report.xsd">

    <mc:fileHeader fileFormatVersion="32.435 V7.0"
vendorName="ip.access"
dnPrefix="ROOT#1;APS#0;LTE_APs#6;LTE_AP_INFO#793">

        <mc:fileSender localDn="LTE_AP_#0" elementType="LTE AP"/>

        <mc:measCollec beginTime="2000-03-01T14:00:00+02:00"/>

    </mc:fileHeader>

    <mc:measData>
```

Example Policies for PM Related Identities

Policies depend how the receiving PM system wishes to identify the AP. For example:

- the filename may suffice and there are no specific requirements for the header
- the Job ID in the filename and header (including equipment ID) uniquely identifies the AP
- the operator has a rigorous policy for Object name that can be used by the PM system
- The DN Prefix is configured so that when concatenated with the Local DN, it produces the full DN (Distinguished Name) of the AP object as used in the NOS (see example in PM Header above).

3.3.3 FM Northbound - AP Information in SNMP Traps

By default the SNMP Traps sent on the NOS Northbound interface include the Managed Object Class and Managed Object Instance. The Object Instance is the full Distinguished Name (DN), which provides a unique identifier for the source.

However, the operator may prefer to use another identifier. In this case the Northbound SNMP Service on the NOS can be configured to emit additional fields according to the source object class. So for example, the Site ID and/or Site Name could be added to the Traps associated with an AP by configuring the “Alarm Watch List” attribute.

3.3.4 Parameters for AP Naming

Use the following attributes in the APs object to automatically configure the X_000295_JobId parameter for all APs:

MIB/Data Model Name	Description	Comment
Generate AP Job ID (generateJobId) (APs object, jobIdConstructionPackage)	Setting this attribute to TRUE causes the NOS to generate the value of an AP's X_000295_JobId parameter from the Associated Group and Provisioned Product Class attributes of the AP Info object.	See the Associated Group attribute held in the AP Info object in the NOS.
Append Equipment ID to Job ID (appendEquipmentId) (APs object, jobIdConstructionPackage)	If set to TRUE, the AP's [equipmentId] is appended to the AP [jobId] regardless of the setting of the [generateJobId] attribute value.	An automatic method for ensuring AP-unique PM filenames.

For a list of attributes and parameters used for naming and identification of individual APs, see section 4.1.

3.4 Network-Wide AP Commissioning Parameters

The AP needs the following parameters to reach the NOS so that the AP can be provisioned:

Parameter	Description	Comment
Device.Time.X_000295_DefaultNTPServer	Default NTP Server address	Supplied to each AP in the DOCP.
Device.IPsec.X_000295_DefaultIPsecEnable	IPsec Enable	Supplied to each AP in the DOCP.
Device.IPsec.X_000295_DefaultRemoteTrafficSelectors	AP Tunnel IP Address Pool (IPSec traffic selectors)	Supplied to each AP in the DOCP.
Device.Services.FAPService.{i}.FAPControl.LTE.Gateway.X_000295_DefaultSecGWServer	Default Security Gateway address	Supplied to each AP in the DOCP.
Device.Security.X_000295_DefaultCRLServerBaseUrl	Primary Mirror CRL Server Base URL	Supplied to each AP in the DOCP.
Device.ManagementServer.X_000295_DefaultMgmtServerURL	Management Server (NOS) URL	Supplied to each AP in the DOCP.

These read-only parameters are supplied to each AP in the DOCP, and are included in the CIQ for reference. The AP has read-write equivalents of these parameters. In most scenarios, set most the read-write equivalents to the same values as those supplied in the DOCP.

The DOCP parameters must be agreed with ip.access in advance of placing any orders for APs. A set of DOCP parameters is given a unique ID, the DOCP_Id, The DOCP_Id must be specified at the time of ordering nanoLTE APs, so that the AP Equipment IDs (EIDs) can be linked to the DOCP_Id, which in turn ensures that the AP is provided with the correct DOCP parameters by the Redirector. For more information about how this is used by the Redirection System to aid AP deployment, see [GST_14700].

3.5 Network-Wide AP Provisioning Parameters

In most deployments, all these parameters will be the same for all APs. There are some exceptions which may apply instead to groups of APs, where noted.

It is recommended to set these parameters with a network-wide Global Template, as in [INST_43380].

3.5.1 PLMNId and Timezone

Parameter	Description	Comment
Device.Services.FAPService.{i}.CellConfig.LTE.EPC.PLMNList.{i}.PLMNID	One or more PLMN IDs (MCC + MNC) available to the operator.	Own PLMN that is usually common across the network.
Device.Services.FAPService.{i}.REM.LTE.X_000295_PLMNListToSyncWith	Either blank or a list of one or more PLMN IDs that APs can use for frequency synchronisation.	It is expected that this will be the same for all APs. If the list is empty, APs will use cells with any PLMN ID for frequency synchronisation. If this is not desired, ensure this list is populated with at least one PLMN ID.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.NeighborList.LTECell.{i}.PLMNID	Neighbour PLMNs in the static neighbour list.	Use the Neighbour Cell Wizard to update the static neighbour cell list after an AP has completed pre-provisioning.
Device.Services.FAPService.{i}.REM.LTE.REMBandList	Scan Bands for Network Listen.	If the list is empty, APs will scan all bands supported by the hardware. If, all APs should scan the same set of bands during Network Listen, add the required bands to this list.
Device.Time.LocalTimeZone	The AP's Local time zone. An operator may not always set to the time zone where the AP is installed. May for example prefer to baseline to UTC or a NOC time zone (if in a different time zone).	Set this globally with a template if all APs are in the same time zone. Alternatively, set this per group of APs according to region, typically with a regional policy template.

3.5.2 Security Resources

Parameter	Description	Comment
Device.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer1	secGwServer1. The first SecGW that a nanoLTE AP attempts to establish a connection with.	This should be the same Security Gateway as the default Security Gateway address supplied in the DOCP.
Device.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer2	secGwServer2. The second SecGW that a nanoLTE AP attempts to establish a connection with.	Not needed in most cases, but it depends on the deployment.
Device.Services.FAPService.{i}.FAPControl.LTE.Gateway.SecGWServer3	secGwServer3. The third SecGW that a nanoLTE AP attempts to establish a connection with.	Not needed in most cases, but it depends on the deployment.
Device.IPsec.X_000295_ConfiguredRemoteTrafficSelectors	Configured Remote end Traffic Selectors	When using an ACME SecGW, this must be left at default. Configure this when using other SecGW types.
Device.Security.X_000295_CRLServerBaseUrl	CRL server Base URL. If Mirror CRL Server is reached via Tunnel, CRLServerBaseUrl should be set by the NOS after connection. If the Mirror CRL Server address is Public, this CRLServerBaseUrl should be part of AP commissioning data (that is, the DOCP).	Should be the same for all APs. This may be the same as the CRL Mirror server in the DOCP.

3.5.3 NTP Servers

These are the operator’s own NTP servers, which should be the same for all APs. Hence it is recommended to set these with a template associated with the Product Class, as in [INST_43380].

Parameter	Description	Comment
Device.Time.NTPServer1	Public NTP Server address 1. Public IP address or FQDN (the FQDN must resolve to a single address).	Should be the same for all APs.
Device.Time.NTPServer2	Public NTP Server address 2.	Should be the same for all APs.
Device.Time.NTPServer3	Public NTP Server address 3.	Should be the same for all APs.
Device.Time.NTPServer4	Public NTP Server address 4.	Should be the same for all APs.

3.5.4 Management Servers

Parameter	Description	Comment
Device.ManagementServer.URL	Management Server Address. A URL specifying the NOS address for TR-069 management connections. That is, for APs to connect to the TR-069 AP Service, which allows the NOS to act as an ACS.	Usually there is a single ACS (NOS) per network. This is the same for all APs connecting to the same NOS.
Device.FAP.X_000295_DiagMgmt.DiagReporting.{i}.	A list of diagnostic report conditions, each with a Diagnostic Server URL. The URL specifies only the destination file location, and does not indicate in any way the name or location of the local file to be uploaded. The full URL is formed from this attribute combined with the filename of the Diagnostic Report. If the URL ends with a "/" character, the AP constructs the filename. If the URL does not end with a trailing "/" character, the last part after the last "/" is assumed to be the filename and AP uses the specified filename. The AP always generates a file of type tar.gz, regardless of the filename specified in this URL.	It is recommended to configure at least one item in the list with the Report On Crash condition and the correct URL. When using the same URL for multiple APs, ensure the trailing "/" character is included. If this is not done, the same file will be overwritten each time an AP uploads a diagnostics file.
Device.FAP.PerfMgmt.Config.{i}.Enable	Performance reporting enabled. Defaults to False.	Configure this globally if it needs to be True for all APs.
Device.FAP.PerfMgmt.Config.{i}.URL	PM Server URL. That is, the URL for the AP to use for PM report file upl.oads.	Typically the same for all APs as there is usually a single PM upload server per network (typically the NOS). It is recommended to configure this in a template, even if PM reporting is not globally enabled, to ensure every AP has the correct URL when it is needed.
Device.FAP.PerfMgmt.Config.{i}.PeriodicUploadInterval	Periodic PM upload interval. in seconds. The default is 86400 (1 day).	Typically can be set to 1 hour for most enterprise deployments.

3.5.5 Network Wide Policies

Parameter	Description	Comment
Device.Services.FAPService.{i}.CellConfig.LTE.EPC.AllowedCipheringAlgorithmList	A list of allowed Ciphering Algorithms. By default, all are allowed: EEA0, 128-EEA1 and 128-EEA2. EEA0 means no ciphering.	Remove unwanted items according to the network policy. This can be done with a global template.
Device.Services.FAPService.{i}.CellConfig.LTE.EPC.AllowedIntegrityProtectionAlgorithmList	A list of allowed Integrity Algorithms. By default, all are allowed: 128-EIA1, 128-EIA2.	Remove unwanted items according to the network policy. This can be done with a global template.

3.5.6 MME

Parameter	Description	Comment
Device.Services.FAPService.{i}.FAPControl.LTE.Gateway.S1SigLinkServerList	Femto LTE AP S1 Interface end points.	May be set in a global template if all APs will use the same MME or set of MMEs. For regional use cases, this is a likely candidate for any regional templates.

3.5.7 Miscellaneous Parameters

Include these parameters in the Global Template so that all new APs are given the recommended values shown in the following table:

Parameter	Description	Recommended Value	Comment
FAPService.{i}.CellConfig.LTE.RAN.PHY.ULPowerControl.X_000295_AccumulationEnabled	This parameter controls whether accumulation is enabled or disabled for PUSCH power control.	False (Default is True)	Setting this to False limits the range of variation in power of UEs using PUSCH. This provides greater RL stability when there are multiple UEs connected to a nanoLTE AP, compared to setting the parameter to True. **Note:** Optionally, this parameter can be set to True for testing with a single UE.

Parameter	Description	Recommended Value	Comment
FAPService.{i}.CellConfig.LTE.RAN.RRCTimers.X_000295_TRRCReestablishment	When a nanoLTE AP detects a local RL failure it waits for the UE to send RRCReestablishmentRequest. This parameter defines how long the AP waits for a UE to send this message.	10000 (Default is 3000)	Increase the time to allow UEs more time to reconnect.

3.6 Parameters Shared by a Group of APs

These parameters can be set with a use case Group Template, as in [INST_43380].

Parameter	Description	Comment
Device.Services.FAPService.{i}.CellConfig.LTE.EPC.TAC	TAC.	This depends on the policy for Tracking Area Code for nanoLTE APs.
Device.Time.X_000295_NTPFrequencyDisciplineEnabled	NTP frequency discipline enabled. Defaults to False.	Not currently supported.
Device.Services.FAPService.{i}.AccessMgmt.LTE.AccessMode	Access Mode. Defaults to Open.	Only Open access is currently supported.
Device.Services.FAPService.{i}.Capabilities.LTE.DuplexMode	Duplexing Mode. Defaults to FDD.	Only FDD is supported.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.PHY.PUSCH.Enable64QAM	Enable 64 QAM. Defaults to False.	No support for 64QAM for PUSCH (i.e UL).
Device.Services.FAPService.{i}.REM.LTE.X_000295_MacroCellTxThreshold	Macro Cell Tx Threshold. The minimum value of Reference signal power, transmitted in SIB2 required for an LTE cell to be considered as a macro cell. Cells with reference signal power values below this level are considered femto cells and are excluded from frequency synchronisation. This is an integer value: 0-1100 representing (-60 to +50 dBm) in steps of 0.1 dBm. The default is 100, which equates to -50dBm.	If any APs will not use the default, typically configure this on a use case basis in an appropriate use case template.

3.7 "Per AP" Parameters

All these parameters should be considered on a per AP basis. After analysis, some parameters might be applicable to AP use cases, in which case include them in appropriate use case Group Templates.

Parameter	Description	Comment
Device.Services.FAPService.{i}.AccessMgmt.LTE.HNBName	eNodeB Name; as displayed by UEs camped on the cell or when performing a manual search for cells on a UE. The default is "ip.access".	It is recommended to ensure this is set, typically on a per AP basis. However, this depends on network policy. For example, there may be a policy where APs with the same use case should have the same HNBName.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.PhyCellID	Physical Cell ID.	This must not clash with neighbouring LTE cells.
Device.Services.FAPService.{i}.CellConfig.LTE.EPC.EAID	Emergency area ID. Tells the AP which emergency area it belongs to for PWS messages.	Depends on geographical location (refer to the nanoLTE AP Release Note to see if this is supported in N4G_1.1).
Device.FAP.GPS.X_000295_LCSLatitude, Device.FAP.GPS.X_000295_LCSLongitude	AP Location - GPS coordinates.	Unique per AP. This must be configured for enterprise APs to ensure the Neighbour Cell Wizard can identify appropriate neighbour cell candidates by location.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.ReferenceSignalPower	The downlink Reference Signal Power in dBm; defaults to -18. The range is -60 to 50. The linear average (in W) of all resource elements that carry cell-specific reference signals within the operating bandwidth.	Only change this if the default value is not correct for the AP's deployment scenario. It may be desirable to have some options for different planned use-cases.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.X_000295_ExternalPAGain	External PA Gain. Required for the LRE feature only. The AP must be connected to an external PA to boosts its Tx power for extended cell radius.	Do not change this if an AP will not use LRE. If the same LRE configuration is used by multiple APs, consider a separate LRE use case template.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.PHY.PRACH.RootSequenceIndex	The root Sequence Index that derives the 64 preamble sequences to be used for RACH.	Should be different from neighbour cells to prevent RACH collisions.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.EARFCNUL	Uplink EARFCN. This can be a comma separated list of candidate UL frequencies. However, as the nanoLTE AP does not yet support self configuration, only the first entry will be used.	Typically selected per AP, from a pool set aside for small cell usage.

Parameter	Description	Comment
Device.Services.FAPService.{i}.CellConfig.DownlinkEARFCNLTE.RAN.RF.EARFCNDL	DownLink EARFCN. This can be a comma separated list of candidate UL frequencies. However, as the nanoLTE AP does not yet support self configuration, only the first entry will be used.	Typically selected per AP, from a pool set aside for small cell usage.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.FreqBandIndicator	Band indicator - the frequency band the AP uses.	Typically selected per AP, but could be in a use case template if multiple APs with the same use case are on the same band.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.DLBandwidth	Downlink Bandwidth in resource blocks; defaults to 50 (10MHz). This can be a comma separated list of candidate UL bandwidths. However, as the nanoLTE AP does not yet support self configuration, only the first entry will be used. Modifying the value of this parameter triggers an AP re-boot on termination of the TR-069 session.	Typically selected per AP according to location dependent requirements, but could be in a use case template. Set to one of the following values, according to the required bandwidth: • 25 (for 5MHz) • 50 (for 10MHz) • 75 (for 15MHz) • 100 (for 20MHz) As per the 3GPP standards, the following bands only support 5MHz or 10MHz bandwidths: • Band 8 • Band 13 • Band 17 All other bands currently available from nanoLTE APs can support 5/10/15/20MHz operation. **Note:** If an invalid band and bandwidth combination (as per the 3GPP standards) is chosen for an AP, the AP will be unable to enter service.

Parameter	Description	Comment
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.ULBandwidth	Uplink Bandwidth in resource blocks; defaults to 50 (10MHz). This can be a comma separated list of candidate UL bandwidths. However, as the nanoLTE AP does not yet support self configuration, only the first entry will be used. Modifying the value of this parameter triggers an AP re-boot on termination of the TR-069 session.	Typically selected per AP according to location dependent requirements, but could be in a use case template. Set to one of the following values, according to the required bandwidth: • 25 (for 5MHz) • 50 (for 10MHz) • 75 (for 15MHz) • 100 (for 20MHz) As per the 3GPP standards, the following bands only support 5MHz or 10MHz bandwidths: • Band 8 • Band 13 • Band 17 All other bands currently available from nanoLTE APs can support 5/10/15/20MHz operation. **Note:** If an invalid band and bandwidth combination (as per the 3GPP standards) is chosen for an AP, the AP will be unable to enter service.

3.8 Other AP Parameters

3.8.1 LTE REM Configuration (Network Listen)

Parameters for Network Listen (NWL) scans of LTE neighbour cells. If all nanoLTE APs should have the same NWL configuration, include these parameters in the network-wide Global Template.

Note: "Radio Environment Measurement" (REM) is the LTE standards terminology for Network Listen (NWL).

MIB/Data Model Name	Description	Comment
FAPService.{i}.REM.LTE.InServiceHandling	AP REM behaviour with respect to ongoing active connections. The default is Immediate.	Immediate causes the AP to start the REM, regardless of active connections. Optionally set this to Delayed, which waits until no CS bearers or PS bearers of streaming or higher QoS class are assigned.

MIB/Data Model Name	Description	Comment
FAPService.{i}.REM.LTE.ScanOnBoot	Enables or disables Radio Environment Measurement during the FAP start up. This is False by default.	False is the recommended setting for enterprise APs.
FAPService.{i}.REM.LTE.ScanPeriodically	Enable Periodic Radio Environment Measurement on LTE EUTRAN bands.	Defaults to True for periodic scans. Change this to False if periodic scans are not required.
FAPService.{i}.REM.LTE.PeriodicInterval	When parameter ScanPeriodically is true, this value indicates the interval in seconds which REM is performed while the AP service is enabled.	Example value: 31536000 (one year)
FAPService.{i}.REM.LTE.PeriodicTime	An absolute time reference in UTC to determine when the AP will initiate the periodic REM. Each REM MUST occur at (or as soon as possible after) this reference time plus or minus an integer multiple of the parameter PeriodicInterval.	Example value: 0001-01-01T00:00:002
FAPService.{i}.REM.LTE.REMPLMNList	Comma-separated list. Each item is a PLMN ID to measure. PLMN ID consists of Mobile Country Code (MCC) and Mobile Network Code (MNC). If empty, then no specific PLMN ID is provided, meaning that the AP scans all available PLMN IDs.	PLMNs scanned by Network Listen. Likely to be a network-wide base set. It is recommended to set this with a template, as in [INST_43380].
FAPService.{i}.REM.LTE.REMBandList.	Comma-separated list. Each item is an LTE Band to measure. If empty then no specific LTE band is provided, meaning that the AP scans all available bands. The order of the band indicator has no significance.	Leave empty to scan all bands (within hardware capability). If bands are specified on a network-wide basis, set this with a template, as in [INST_43380].
FAPService.{i}.REM.EUTRACarrierARFCNDLList	Comma-separated list. Each entry is a EUTRA ARFCN in the DL direction to measure. If empty, then no specific EUTRA ARFCN is provided, meaning that the AP is required to scan all ARFCNs that it is aware of.	Leave empty to scan all EARFCNs. However, it is recommended to specify frequencies to scan, as this will reduce scan time. If DL ARFCNs are specified on a network-wide basis, set this with a template, as in [INST_43380].

3.8.2 3G REM Configuration (Network Listen)

Parameters for Network Listen (NWL) scans of 3G neighbour cells. If all nanoLTE APs should have the same NWL configuration, include these parameters in the network-wide Global Template.

Note: “Radio Environment Measurement” (REM) is the LTE standards terminology for Network Listen (NWL).

MIB/Data Model Name	Description	Comment
FAPService.{i}.REM.UMTS.WCDMA.InServiceHandling	AP REM behaviour with respect to ongoing active connections. The default is Immediate.	Immediate causes the AP to start the REM, regardless of active connections. Optionally set this to Delayed, which waits until no CS bearers or PS bearers of streaming or higher QoS class are assigned.
FAPService.{i}.REM.UMTS.WCDMA.ScanPeriodically	Enable Periodic Radio Environment Measurement on 3G bands.	Defaults to True for periodic scans. Change this to False if periodic scans of 3G neighbours are not required.
FAPService.{i}.REM.UMTS.WCDMA.PeriodicInterval	When parameter ScanPeriodically is true, this value indicates the interval in seconds which REM is performed while the AP service is enabled.	Example value: 31536000 (one year)
FAPService.{i}.REM.UMTS.WCDMA.PeriodicTime	An absolute time reference in UTC to determine when the AP will initiate the periodic REM. Each REM MUST occur at (or as soon as possible after) this reference time plus or minus an integer multiple of the parameter PeriodicInterval.	Example value: 0001-01-01T00:00:002
FAPService.{i}.REM.UMTS.WCDMA.REMPLMNList	Comma-separated list. Each item is a PLMN ID to measure. PLMN ID consists of Mobile Country Code (MCC) and Mobile Network Code (MNC). If empty, then no specific PLMN ID is provided, meaning that the AP is required to scan all available PLMN IDs.	PLMNs scanned by Network Listen. Likely to be a network-wide base set. It is recommended to set this with a template, as in [INST_43380].
FAPService.{i}.REM.UMTS.WCDMA.REMBandList.	Comma-separated list. Each item is a 3G Band to measure. If empty then no specific 3G band is provided, meaning that the AP scans all available bands. The order of the band indicator has no significance.	If bands are specified on a network-wide basis, set this with a template, as in [INST_43380].

MIB/Data Model Name	Description	Comment
FAPService.{i}.REM.UMTS.WCDMA.UARFCNDLList	Comma-separated list. Each entry is a 3G UARFCN in the DL direction to measure. If empty, then no specific 3G ARFCN is provided, meaning that the AP scans all ARFCNs that it is aware of.	Leave empty to scan all UARFCNs. However, it is recommended to specify frequencies to scan, as this will reduce scan time. If DL ARFCNs are specified on a network-wide basis, set this with a template, as in [INST_43380].

3.8.3 Additional Management Server Parameters

MIB/Data Model Name	Description	Comment
Device.FAP.PerfMgmt.Config.{i}.PeriodicUploadTime	An absolute time reference in UTC to determine when the AP will initiate the periodic PM file upload. Each file upload MUST occur at this reference time plus or minus an integer multiple of the parameter PeriodicUploadInterval. The actual value of PeriodicUploadTime can be arbitrarily far into the past or future. For example, if parameter PeriodicUploadInterval is 86400 (a day) and if PeriodicUploadTime is set to UTC midnight on some day (in the past, present, or future) then periodic file uploads will occur every day at UTC midnight. The Unknown Time value indicates that no particular time reference is specified.	Note the default is the "Unknown Time", resulting in a random upload time. For hourly reporting, this may be a good choice, spreading AP uploads across the interval. For daily reporting, this could mean up to a day's delay in reports being available, so it may be preferred to apply a set of different values across groups of APs to spread the load but ensure reports are available. For example, within 2 hours after midnight. The recommended value is: 0001-01-01T00:00:00Z (default)

3.8.4 AP Groups

MIB/Data Model Name	Description	Comment
Associated Group (associatedGroup) - set in the AP's parent AP Info object	Refers to the group object (if any) representing the group to which the AP belongs.	If used, the group name becomes part of the file name for file uploads, which allows grouping (for example) of PM files. This is optional. An optional management policy allows this to determine which APs a NOS Client user can manage. In this case, the AP Groups are typically organised on a regional basis. If AP groups are used, assign an AP to a group after site creation.

4 AP-Unique Parameters

The previous section deals with all of those parameters that are in some way shared and, thus, may be used to populate one or more templates. There remains a small set of parameters that must be uniquely configured on a per-AP basis.

The topics in this section are:

- *4.1 Parameters for AP Identification*
- *4.2 Network Names*
- *4.3 AP Location*

4.1 Parameters for AP Identification

Align the attributes and parameters in the following table with the naming policy. See section 3.3 for advice on the AP naming policy.

MIB/Data Model Name	Description	Comment
AP info->objectInstanceId	The numeric instance identifier of the AP Info object, displayed as part of the “Site ID” in the NOS Client.	Specified during AP pre-provisioning
AP Info->objectname	Textual ID for AP, displayed as the Site Name in the NOS Client.	The NOS Create Site Wizard automatically sets this as “Site <Site ID>”.
equipmentIdentity	The unique EID of an AP, composed of the OUI and the serial number.	Used by the NOS to identify an AP when it connects.
Device.DeviceInfo.X_000295_ObjectName	The user-defined name string associated with a managed object. The value of this parameter is used to populate the UniqueId field of PM report file names and the UserLabel field of the PM file contents. Up to 50 characters excluding the following: hash, semi-colon, equals and comma.	Optionally use this to provide a structured, unique name. However, this relies on rigorous application of this policy. It is recommended that an equipment ID suffix is used ensure uniqueness
Device.FAP.PerfMgmt.Config.{i}.X_000295_JobId	An identifier used to reference the measurements. This may optionally be set by the management system. If this has been set (i.e. is not an empty string) then this identifier is included in all PM reports and becomes part of the filename of the PM report. The value in Job ID must not be set via management system client unless the values of [generateJobId] and [appendEquipmentId] are set to FALSE. If the values of [generateJobId] and [appendEquipmentId] are set to TRUE, Job ID is automatically constructed and set by the management system.	If the recommended auto-naming policy is in use, there is no need to specify a value for this parameter. That is, only configure this manually if the automatic naming policies in the jobIdConstructionPackage in the APs object are disabled.

MIB/Data Model Name	Description	Comment
Device.Services.FAPService.{i}.DNPrefix	This attribute defines the DN (Distinguished Name) prefix that is included in PM reports generated by the AP in order to uniquely identify the object generating the report. Hence this allows generation of the full Distinguished Name of the reporting AP, which only knows the local part.	This is configured automatically during provisioning to ensure that PM reports delivered to the NOS are associated with the AP. This can be changed afterwards if an alternative policy is required for PM reporting.

4.2 Network Names

MIB/Data Model Name	Description	Comment
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.Common.CellIdentity	Cell Identity. This is a concatenation of the 12-bit RNC-ID and 16-bit on-air Cell ID	
Device.Services.FAPService.{i}.CellConfig.LTE.EPC.TAC	Tracking Area Code (TAC).	This identifies the tracking area that the nanoLTE AP belongs to.
Device.Services.FAPService.{i}.CellConfig.LTE.RAN.RF.PhyCellID	A physical cell ID in the range 0 to 503. This can be a comma separated list of candidate physical cell IDs. However, as the nanoLTE AP does not yet support self configuration, only the first entry will be used. Modifying the value of this parameter triggers an AP re-boot on termination of the TR-069 session.	Physical Cell ID that determines the PSS (Primary Synchronisation Signal) and SSS (Secondary Synchronisation Signal) used by the cell. This must be different from any of the nanoLTE AP's neighbour cells.

4.3 AP Location

MIB/Data Model Name	Description	Comment
LTEApInfo-> LTEAPInfoPackage> provisionedLatitude	Defines the AP's expected Latitude. The value of this attribute is specified at site creation time and may only be updated by a Change Location action.	Required for static neighbour planning.
LTEApInfo-> LTEAPInfoPackage> provisionedLongitude	Defines the AP's expected Longitude. The value of this attribute is specified at site creation time and may only be updated by a Change Location action.	Required for static neighbour planning.
LTEApInfo-> LTEAPInfoPackage> provisionedRadiusOfUncertainty	Defines the radius of uncertainty associated with the AP's provisioned location. The value of this attribute is specified at site creation time and may only be updated by a Change Location action.	Required for static neighbour planning.

5 System Preparation for nanoLTE AP Provisioning

This section describes how to setup MME Pools, AP SW Version and AP Product Class objects, ready for use during AP provisioning. Also ensure that, if used, any ACME Security Gateway objects are correctly configured. For a new system installation, also ensure that the LTE APs object exists, as all nanoLTE APs must be provisioned under this object.

Note: It is also recommended to setup templates to speed up provisioning, as covered in section 6 and detailed in [INST_43380].

The topics in this section are:

5.1 Assumptions About the NOS

This manual is about nanoLTE AP configuration, not NOS configuration. Hence, it is assumed that the NOS is already working and that the NOS itself and its services have been correctly setup in readiness for AP provisioning. This includes:

- Service configuration for AP connections:
  - TR-069 AP Service
  - Software Download Service
  - Performance Management File Service
  - Diagnostics File Service
  - Certificate Validation Service (if this NOS service is not used, an equivalent CRL Mirror server must be available)
- Creating Security Gateway objects
- Creating NTP Server objects

The NOS configuration manual [INST_14300] provides the information required for these aspects of NOS configuration.

All aspects of NOS-oriented configuration that are specific to AP provisioning are covered in the sections that follow.

5.2 MME Pools

There must be at least one MME Pool with at least one MME. If they have not yet been created, create them before using the LTE AP Create Site Wizard.

5.2.1 Create an MME Pool

1) Right-click the **Root > MME Pools** object and select **Create > Child Object**, then click **Next** twice to get to the Set Mandatory Attributes page.

2) Optionally change the **Object Name** to allow easy identification of the MME Pool referenced by this MME Pool object.

3) Select the **MME Pool Package** and enter the **MME Group Id**.

4) Drill down into the **PLMN Id List** and add at least one PLMN Id (MMC and MNC are entered separately).

5) Drill down into the **TACList** and add at least one TAC.

   Note: Additional PLMN IDs and TACs can be added to the MME Pool at any time after the object is created.

6) Click **Finish**.

7) Create additional MME Pool objects as needed.

5.2.2 Create an MME

1) Right-click an **MME Pool** and select **Create > Child Object**, then click **Next** twice to get to the Set Mandatory Attributes page.

2) Optionally change the **Object Name** to allow easy identification of the MME referenced by this MME object.

3) Select the **MME Package**.

4) Enter the **MME Code** used by the MME.

5) Enter the **MME Address** (IP address or FQDN) that APs must use to connect to this MME.

6) Click **Finish**.

7) If required, add more MMEs to the MME Pool.

5.3 Product Class and AP Software Version Objects

To assist with provisioning and software updates for APs, the NOS has Product Class and AP Software Version objects.

A Product Class defines an AP product in terms of an AP object class and an associated AP Software Version object. The associated AP Software Version object sets the minimum software version for any AP assigned to that Product Class. If an AP assigned to the Product Class has an older software version, it is upgraded automatically when it next connects to the NOS. Also, to make AP provisioning more efficient, associate up to 10 AP templates with a Product Class and the templates will be applied automatically when creating a new AP site.

As Product Classes can reflect AP use cases along with corresponding AP templates, also review the template information in section 6 as part of the decision making process for creating Product Classes.

An AP Software Version object defines the software version and references an SDP file on the NOS server running the Software Download Service. A Product Class refers to an AP Software Version, so at least one AP Software Version object must be created before any Product Classes.

As an LTE AP must be assigned to a Product Class, there must be at least one Product Class and at least one AP Software Version object defined before using the Create Site wizard to provision an AP.

5.3.1 About AP Software Versions

This section explains AP software versions, and how this is reflected in the .sdp file name and in the software version information shown in the NOS Client.

AP Software Version

Here is an example of an AP software version, as shown in a nanoLTE AP Release Note:

- 1.1.0_LTE_137.0

This is structured as follows:

- <APRel>_LTE_<Version>

Where:

<APRel>	This is the overall AP system release, which currently will be 1.0.0.
LTE	Indicates it is a nanoLTE AP software release.
<Version>	The software version. This is a sequential number generated automatically. A higher number indicates a later (newer) software version.

AP Software File Name

Here is an example of an AP software file name:

- 279K007_137.0_signed.sdp

This is structured as follows:

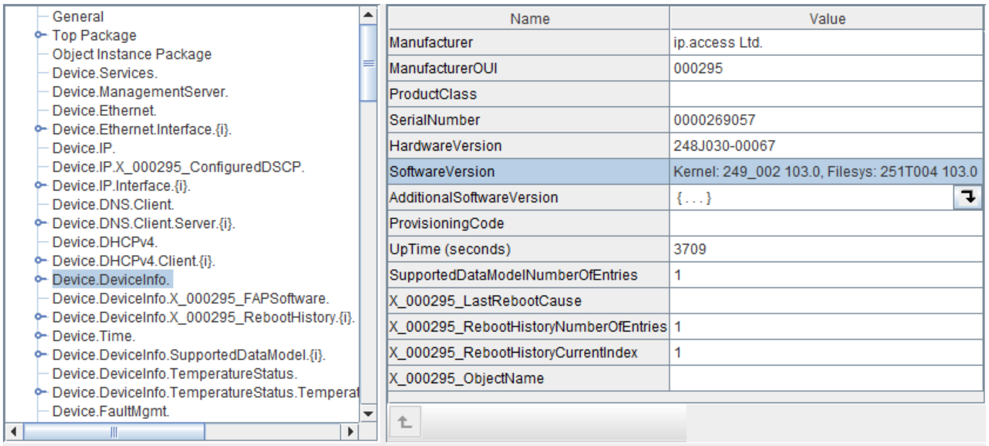
- <SWC><Var><PKG>_<Version>.sdp

The file name contains the following information:

<SWC>	The software code that corresponds to the target hardware platform, which will be one of: • 251 for the nanoLTE E40 AP (hardware code 248) • 279 for the nanoLTE E40 AP with secure boot enabled (hardware code 278) **Note:** The hardware code appears on the information label on each nanoLTE AP.
<Var>	The software variant, which will be: • T for lab test builds (251 software only) • K for secure boot builds (279 software only)
<PKG>	This is 007 for all .sdp files, to indicate that an AP software file is a complete AP software image. That is, it includes the three following items: • 001 - Boot loader • 002 - Kernel • 004 - Filesys The "007" comes from adding up the numbers of these three items. These are always delivered as a complete 007 set, but are shown separately in the NOS Client (see below).
<Version>	The software version, such as "123.0_signed".
.sdp	The file extension, which is always .sdp.

AP Software Version in the NOS Client

In the NOS Client, select an **AP** object then select **Device.DeviceInfo**. in the **Navigation pane**:


General
Top Package
Object Instance Package
Device.Services.
Device.ManagementServer.
Device.Ethernet.
Device.Ethernet.Interface.{i}.
Device.IP.
Device.IP.X_000295_ConfiguredDSCP.
Device.IP.Interface.{i}.
Device.DNS.Client.
Device.DNS.Client.Server.{i}.
Device.DHCPv4.
Device.DHCPv4.Client.{i}.
Device.DeviceInfo.
Device.DeviceInfo.X_000295_FAPSoftware.
Device.DeviceInfo.X_000295_RebootHistory.{i}.
Device.Time.
Device.DeviceInfo.SupportedDataModel.{i}.
Device.DeviceInfo.TemperatureStatus.
Device.DeviceInfo.TemperatureStatus.Temperat
Device.FaultMgmt.

Name	Value
Manufacturer	ip.access Ltd.
ManufacturerOUI	000295
ProductClass	
SerialNumber	0000269057
HardwareVersion	248J030-00067
SoftwareVersion	Kernel: 249_002 103.0, Filesys: 251T004 103.0
AdditionalSoftwareVersion	{...}
ProvisioningCode	
UpTime (seconds)	3709
SupportedDataModelNumberOfEntries	1
X_000295_LastRebootCause	
X_000295_RebootHistoryNumberOfEntries	1
X_000295_RebootHistoryCurrentIndex	1
X_000295_ObjectName	

This package shows all the available software version information. The parameter of interest the SoftwareVersion. Here is an example value for a lab test build:

- Kernel: 279_002 123.0, Filesys: 279K004 123.0

The Filesys part of the SoftwareVersion shows version of software that is loaded and running on the AP. This relates to the overall software version.

Note: The Kernel version can be ignored for the purposes of determining the software version on the AP.

5.4 Copy AP Software onto the NOS Server

This procedure needs to be executed once for each AP software file that is required for the APs:

1) Use a graphical SCP client (such as WinSCP) to log in as user oamnorth on the NOS server hosting the Software Download Service.

   Alternatively, login directly to the NOS as oamnorth and use the **`scp`** command to pull the file into the directory.

2) Copy the required AP software files into this directory:

   ```
   /var/lib/ipaccess/data/oamfiles/download/sw/install
   ```

   The software files are named as follows:

AP Software with Code Signing: Variants and Filenames

AP	AP Product and S/W Variant	Software Filename
nanoLTE E40 AP (278 variant)	279K	279K007_<ver>.sdp

   Where <ver> is the version, such as "123.0_signed".

   Note: See the corresponding release note for the relevant software version and file names.

3) Wait five minutes for the .sdp files to be validated and copied to:

   ```
   /var/lib/ipaccess/data/oamfs-web/download/sw
   ```

   The .sdp files are now available for download to nanoLTE APs.

5.5 Create an AP SW Version Object

This is only required if there is no suitable AP SW Version object.

1) Under the NOS object, right-click the **AP SW Versions** object and select **Create > Child Object**.

2) Only one type of AP SW Version object can be created, so click **Next**.

   Note: If a Template has been created for any AP SW Version object, a Template Selection screen will appear. If it is not necessary to use a template, click Next without selecting any template names.

3) In the Configure AP Software Version page, set the attributes values as follows:

   - Object Name: A name that identifies this software version.
   - SW Version: The formal software version as provided in the Release Notes for that AP software release. For example: *123.0_signed*.
   - Software Product Number and Variant: This is a three digit code followed by the letter K, so this will be one of:

AP Type	**Enter Value**
nanoLTE E40 AP (278 hardware)	279K

   - Software Image Download URL: The URL an AP can use to locate the SDP file on the NOS server running the Software Download Service. The SDP file name must match the specified software version and AP variant. Enter a URL of the form:
     `http://<server>/download/sw/<file>`
     Where: <server> is the IP address or FQDN of the NOS server hosting the Software Download Service, and <file> is the relevant .sdp file name. The file name must contain the SW Version and Software Product Number and Variant. This is validated by the wizard.

4) Click **Next**. The wizard will validate the entries, then close and the new AP SW Version object is added.

5.6 Create an AP Product Class

This is only required if there is no suitable Product Class.

1) Under the NOS object, right-click the **Product Classes** object and select **Create > Child Object**.

2) Only one type of Product Class object can be created, so click Next.

   Note: If a Template has been created for any Product Class object, a Template Selection screen will appear. If it is not necessary to use a template, click Next without selecting any template names.

3) In the Configure Product Class page, set the attributes values as follows:

   - Class Type:
     Select **AP_TR069**.
   - Associated Object Class:
     This will also set Target Object Class. This must match the version of software (.sdp file) in the associated AP SW Version object. For N4G_1.1 releases, select the Associated Object Class according to the software version as follows:

AP Software Version	Associated Object Class
122.0 or later	lte11Tr069_004

   Note: Details of the Data Model for the AP Class can be found in the version of [REF_43150] included in the corresponding system release.

   - Object Name:
     Enter a useful name to identify this object class. This can be any text, but should reflect the usage of this Product Class.
   - AP Software Version:
     Select the name of the required **AP SW Version** object, as created previously.

   Note: Only set the Associated Object Class to the class noted above as other classes will not match any AP software in N4G_1.1 System Releases.

4) Click **Finish**. The wizard will close and the new Product Class object is added. This can now be referenced when using the Create Site wizard to pre-provision an AP.

5) Create additional Product Classes as determined by nanoLTE AP hardware variants and/or use cases.

6) If templates have already been created, associate one or more AP templates with the Product Class. To do this, go to its Product Class Package, drill down to the AP Template Object List, click the **+** button to add a new instance, then click the Select button to choose a template to associate.

   Note: A template used by a Product Class must not have any AP specific parameters as this will cause attempts to use the Product Class to fail. See section 6.5 for more information.

5.7 Check the LTE APs Object

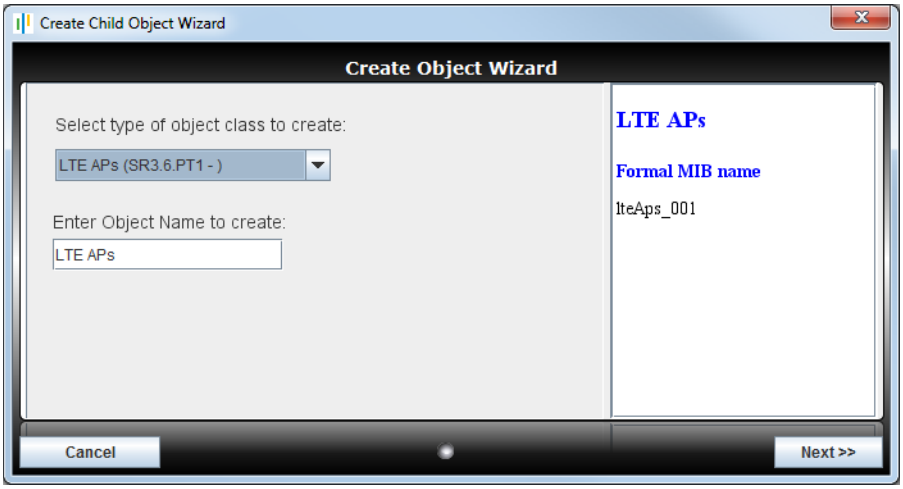
Only one LTE APs object is required, which must be created before provisioning the first nanoLTE AP. For a new system installation, verify that this object exists and, if needed, create the object.

5.7.1 Verify the LTE APs Object Exists

1) To check if the LTE APs object already exists, look for it under the **Root > APs** object. If it is present, no further action is required in this respect.

2) If the LTE APs object does not yet exist, right-click the **APs** object and select **Create > Child Object**.

3) In the wizard, select the **LTE APs** object in the drop-down list:



Create Child Object Wizard

Create Object Wizard

Select type of object class to create: LTE APs (SR3.6.PT1 -)

Enter Object Name to create: LTE APs

LTE APs

Formal MIB name

lteAps_001

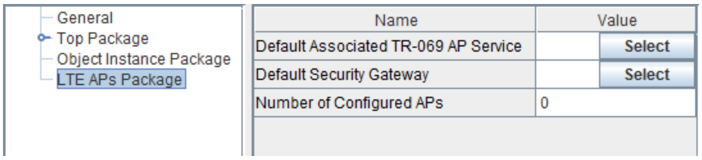
Note: Do not change the Object Name. It is recommended to leave this object with the default name of "LTE APs".

4) Click **Next>>** twice, then click **Finish** (that is, there is no need to make any other edits in the Create Child Object Wizard). The new LTE APs object will appear below the APs object.

5.7.2 Configure the LTE APs Object

1) Select the **LTE APs** object, then select its **LTE APs Package**:

2) Inspect the Default Associate TR-069 AP Service and Default Security Gateway attributes to see if they are blank or not. For example:

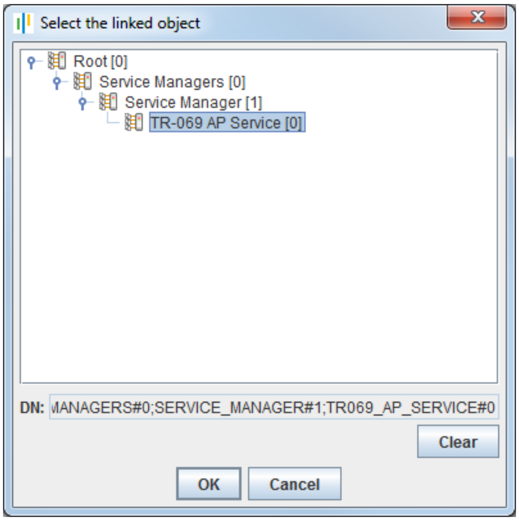


Name	Value
Default Associated TR-069 AP Service	Select
Default Security Gateway	Select
Number of Configured APs	0

As can be seen in this case, the new object is not yet associated with a TR-069 AP Service or a default Security Gateway. If they are not blank, no further action is required for configuring the LTE AP object, so skip to the next section.

3) Click the **Select** button for Default Associated TR-069 AP Service.

4) In the Select the linked object box, drill down to the TR-069 AP Service and select it:

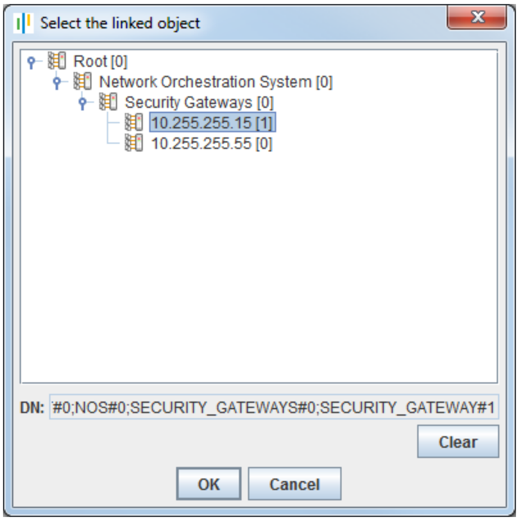


DN: MANAGERS#0;SERVICE_MANAGER#1;TR069_AP_SERVICE#0

5) Click **OK** and the Value for Default Associated TR-069 AP Service will show the DN (Distinguished Name) of the TR-069 AP Service.

6) Click the **Select** button for Default Security Gateway.

7) In the **Select the linked** object box, drill down to the required Security Gateway and select it:



DN: #0;NOS#0;SECURITY_GATEWAYS#0;SECURITY_GATEWAY#1

8) Click **OK** and the Value for Default Security Gateway will show the DN (Distinguished Name) of the chosen security gateway.

9) Click **Apply** to save the changes. Configuration of the LTE APs object is now complete.

5.8 Check the APs Object

Ensure the APs object is configured according to the required naming policy. See section 3.3 for information about naming policies.

5.8.1 Automate the Job IDs

This is only necessary if changes are required to the way that Job IDs are automatically generated for APs. By default, Generate AP Job ID is false (unchecked) and Append Equipment ID to Job ID is true (checked).

1) Select the **Root > APs** object.

2) Select the **Job ID Construction Package**.

3) Verify that the **Generate AP Job ID** and **Append Equipment ID to Job ID** attributes are set correctly.

4) Click **Apply** to save any changes.

5.8.2 Check if AP Management by Group is Enabled

By default, all nanoLTE APs can be managed by NOS Client users. If preferred, manage APs according to AP Group membership, and use this check to verify that this policy has been enabled.

Note: If the NOS also manages nano3G APs, any changes to this policy will affect the nano3G APs as well.

1) In the **Root > APs** object, select the **User AP Groups Filter Package**.

2) If AP management by AP Group is required, verify that **Filter By User AP Groups** is checked.

3) If it is not checked, but it should be, a NOS Client user with user management rights must change this via the Manage Users screen. See [OPM_14015] for details.

5.9 Create AP Groups

This is optional.

Create AP Groups if the groups must be used for one or both of the following purposes:

- AP management by Group - if this is enabled, it is recommended to associate an AP Info object template with each Product Class (see [INST_43380]) to ensure all APs will be pre-provisioned with a Group
- Group identity in uploaded PM file names

5.9.1 Create a Group

1) In the NOS Client, select the **Root > Network Orchestration System > Groups** object. Any existing Group objects are shown in the Workspace pane, or expand the Groups object to list them in the Explorer pane.

2) Right-click the Groups object and select **Create > Create Group**.

3) Enter a **Group ID** of up to 16 characters.

   Spaces are not allowed so it is recommended to use underscore (_) characters instead of spaces. This is enforced to avoid spaces in the file names of PM files uploaded by APs.

4) Repeat as needed according to the Group IDs required by the network policy.

5.10 Neighbour Cell Objects

Optionally create Neighbour Cell Objects now, so that they are ready to assign to APs as neighbours via the Neighbour Cell Wizard. This can be done if an AP’s planned location is known.

See [OPM_43005] for full information on creating neighbour cell objects.

6 *Template Preparation*

Before starting AP Provisioning, create at least one AP Product Class for each AP type and create a set of templates. For templates that will always be used for every AP, associate those templates with the Product Classes, or with the Product Classes where they are applicable. If there are different use-cases for the same Product Class that need different templates then they should not be associated.

This section assumes that all system preparation activities in section 5 are complete prior to creating any AP templates.

The topics in this section are:

- *6.1 Template Strategy*
- *6.2 Network Global Template*
- *6.3 AP Mode and Regional Templates*
- *6.4 AP Info Object Templates*
- *6.5 Associating Templates with Product Classes*

6.1 Template Strategy

There is a balance here regarding whether the number of Product Classes should be kept small, e.g. one per physical AP type (E40), or whether the primary use cases could be represented as Product Classes (E40 enterprise, E40 SOHO). As an initial starting point, create a "Global Template" of network-wide parameter settings that captures the all settings used by all APs.

Most deployments will need a minimum of one Product Class per physical AP type, each of which includes all global templates.

A minimum set of templates will be the templates for mandatory and global settings, plus one "Group Template" per use case. A more complex network, for example with multiple Security Gateways and/or regional RF policy, may need to move some parameters from the global template into separate Regional Templates.

Hence, the typical types of templates to create are:

- Mandatory Settings Template - a global template that must be applied to all nanoLTE APs, regardless of deployment strategy - hence this is associated with every Product Class for nanoLTE APs
- Global Template for all nanoLTE APs - a baseline global template, containing network-wide settings that are applicable to all Product Classes and use cases for nanoLTE APs
- Use case Group Templates for groups of APs, such as:
  - "AP mode" templates for different AP deployment scenarios
  - Regional templates - where APs need to be deployed in different regions that have different parameter requirements
- AP Info templates, typically for assigning a AP to a Group for management by Group and/or PM report file naming

6.2 Network Global Template

Use the network Global Template to configure shared aspects of AP operation. As a minimum, there should be one template for mandatory settings and one global template for baseline AP configuration.

The mandatory settings template includes:

- QCI to DSCP mapping
- AP Temperature limits

The baseline Global Template includes:

- Core network connection defaults (assumes APs connecting to the same NOS will use the same set of core network entities)
- Time related defaults (NTP servers and time zone)
- REM (Network Listen) defaults (recommended if APs will use the same REM settings as a baseline)
- NOS connections (recommended to ensure all APs connecting to the same NOS are consistently configured for connecting to NOS services)

Also refer to section 3 for considerations that will affect the content of these templates.

Note: When using the Create Site Wizard, the Security Gateway Address and Management Server Address (NOS address) are auto-assigned so they do not need to be in a template. It may still be useful to specify them so that they are explicitly captured.

6.3 AP Mode and Regional Templates

If there are multiple AP use cases for APs connecting to the same NOS, create one or more use case templates that reflect the different modes and/or regional templates that reflect local policies.

These can either be applied to APs as an overlay after initial pre-provisioning, or automatically by associating the templates with Product Classes that reflect the AP use cases or deployment regions.

6.4 AP Info Object Templates

The main reason for associating an AP Info template with a Product Class is to automatically associate the APs in that Product Class with a Group. There are two reasons for associating APs with Groups:

- PM report identification:
  Use the Group name to identify groups of APs for PM reporting purposes, where the Group name is used in the names of PM files that APs upload.
  To enable this, the Generate AP Job ID attribute in the APs object must be set to True (checked).
- AP management by Group:
  This overrides the default mechanism of using the AP Collection objects to provide AP management permissions to users. In this scenario, assigning APs to Groups is effectively mandatory as any APs that are not in a Group will not be available to any normal NOS Client users. Hence the most effective way to ensure Group membership for all APs is to also organise the Product Classes by Group and associate each Product Class with an AP Info template that points to the correct Group for that Product Class.
  To enable AP management by Group, ensure the Enable Search Filter By User AP Groups option is checked in the Manage Users dialogue box in the NOS Client.

Once the first AP Info template exists, optionally copy it to create additional templates for each AP Group.

6.5 Associating Templates with Product Classes

Templates may be associated with a Product Class, and this is recommended for:

- Speeding up AP pre-provisioning
- Ensuring consistent and error free configuration of APs
- Applying planned values for new parameters where an upgrade requires a new Product Class, instead of staying with default values for any new parameters

In most cases it should only be necessary to associate two or three templates with each Product Class, but it is possible to associate up to 10 templates with each Product Class.

A template used for a Product Class should only provide the default and/or specific values that are applicable to all APs of that Product Class. To ensure this, it is strongly recommended to create templates for Product Classes either from scratch (as in [INST_43380]) or by copying a prior template that is known to work for a Product Class. To copy an existing template, use **Create > Duplicate** then use **Morph Template** to change the target object version.

ALERT: Do not create a template for a Product Class from an existing AP object. This will avoid accidentally including any AP-specific parameters in the template that will cause usage of the associated Product Class to fail during site creation and upgrades.

Information on creating Product Classes is in the section 5.

6.6 Create the AP Templates

If templates have not yet been created, create them now and associate them with the Product Classes created during system preparation (section 5.6).

See [INST_43380] for information on creating different types of templates.

7 AP Provisioning

Ensure the System Preparation activities in section 5 and Template Preparation in section 6 are complete before using the Create Site Wizard to provision an AP.

The procedures in this section assume that the AP will connect to the NOS after the procedures are complete. That is, the AP is not powered up and connected to the backhaul until the NOS is ready for the AP.

The topics in this section are:

- *7.1 About the Create Site Wizard*
- *7.2 Pre-Provisioning a nanoLTE AP*
- *7.3 Use the Create Site Wizard to Pre-Provision a New AP*
- *7.4 Apply Templates and Configuration Files to the AP*
- *7.5 Update the Individual AP Parameters*
- *7.6 Assign Planned (Static) Neighbours*

7.1 About the Create Site Wizard

Use the Create Site Wizard for nanoLTE AP Provisioning, but simplify the path through it as much as possible by means of appropriate template application.

For a basic system the sequence through the Wizard should be:

- Select Product Class, which can reference one or more global templates
- Optionally select an appropriate AP policy template
- Enter the AP-unique parameters
- Enter the AP’s geographical location
- Select the NTP servers for the AP
- Configure some remaining mandatory parameters

After completing the Create Site Wizard, then:

- Optionally apply one or more templates, typically an appropriate AP policy template
- Optionally load one or more XML configuration files to apply parameter settings to the AP object
- Manually configure any remaining parameters that are individual to each AP, or that do not fit into an AP policy

7.2 Pre-Provisioning a nanoLTE AP

The nanoLTE AP must be pre-provisioned on the NOS Server before it can be brought into service. It is recommended to do this in advance of physical site installation. An AP is pre-provisioned using the Create Site Wizard in the NOS Client.

The user account used for these activities in the NOS Client must have Full Access rights to the LTE APs object.

Note: It is assumed that a new AP already has an OLM Package waiting for it in the Redirector, so that when the AP is started up for the first time it can obtain the information it needs to connect to its serving NOS. Each AP must be able to connect to the Redirector via the Internet so that it can retrieve its unique OLM Package from the Redirector. See [GST_14700] for more information on the requirements for this.

7.2.1 Pre-Provisioning Parameters

For information about the pre-provisioning parameters refer to section 3 and section 4.

7.2.2 Pre-Provisioning Methods

Pre-provision a nanoLTE AP in the NOS using one of the following methods:

- Use the Create Site Wizard from the right-click menu on the LTE APs object. This is the method described in this manual. See section 7.3.
- Use the SOAP/XML interface to submit an LTE AP provisioning request to the NOS. This method is not described in this manual. However, the requirements and preparation are the same. That is, there must be an appropriate Product Class and associated AP SW Version object. Also, it is strongly recommended to associate templates with a Product Class used for SOAP/XML provisioning requests, as this minimises the parameter load in the SOAP/XML request. For information about the SOAP/XML interface provided by the NOS, including the IRP for nanoLTE AP provisioning, see [REF_14490].

Note: Do not use the Create Auto-Allocated TR-069 Site Wizard on the Actions menu for the APs object. This is not applicable to nanoLTE APs.

7.3 Use the Create Site Wizard to Pre-Provision a New AP

Use the Create Site Wizard in the NOS Client to create a site (AP Info) object and child AP object for an AP. The physical AP will be matched to the AP object according to its serial number. The configuration data for the AP object is stored on the AP's serving NOS Server. When a commissioned AP starts up, it connects to the serving NOS Server and downloads the configuration. This approach means that the AP's configuration can be entered and changed on the NOS Server in advance of physically installing an AP on site.

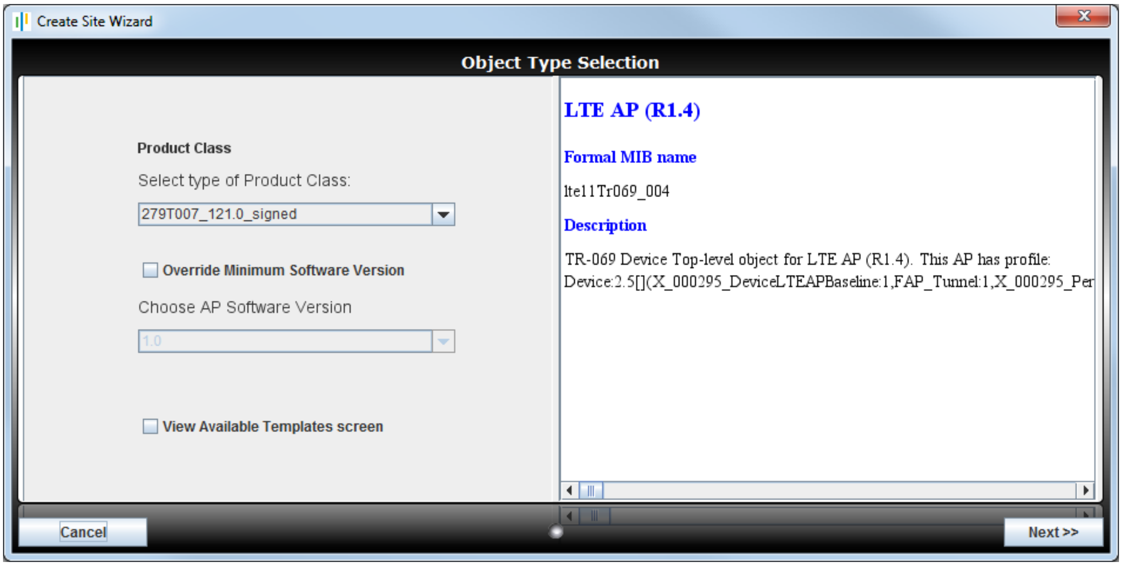
7.3.1 Start the Create Site Wizard

1) Login to the NOS Client with a user ID that has Full Access rights to the LTE APs object.

2) Select the **LTE APs** object. That is:

```
Root > APs > LTE APs
```

3) Right-click the **LTE APs** object and, from the menu, select **Create > Create LTE AP Site**. The first page of the Create Site Wizard will appear:



Product Class

Select type of Product Class: 279T007_121.0_signed

□ Override Minimum Software Version

Choose AP Software Version: 1.0

□ View Available Templates screen

LTE AP (R1.4)

Formal MIB name

lte11Tr069_004

Description

TR-069 Device Top-level object for LTE AP (R1.4). This AP has profile: Device:2.5[](X_000295_DeviceLTEAPBaseline:1,FAP_Tunnel:1,X_000295_Per

4) Use the **Product Class** drop-down list to select the required LTE AP Product Class. The object class used by the Product Class is shown on the right.

Note: If the Product Class has any associated templates, these will be used for configuring the corresponding AP parameters.

Note: It is not recommended to use the Override Minimum Software Version option. The Product Class should already be associated with the required software version. However, if this is used, the nanoLTE AP object class used to build the chosen software must match the object class used by the Product Class.

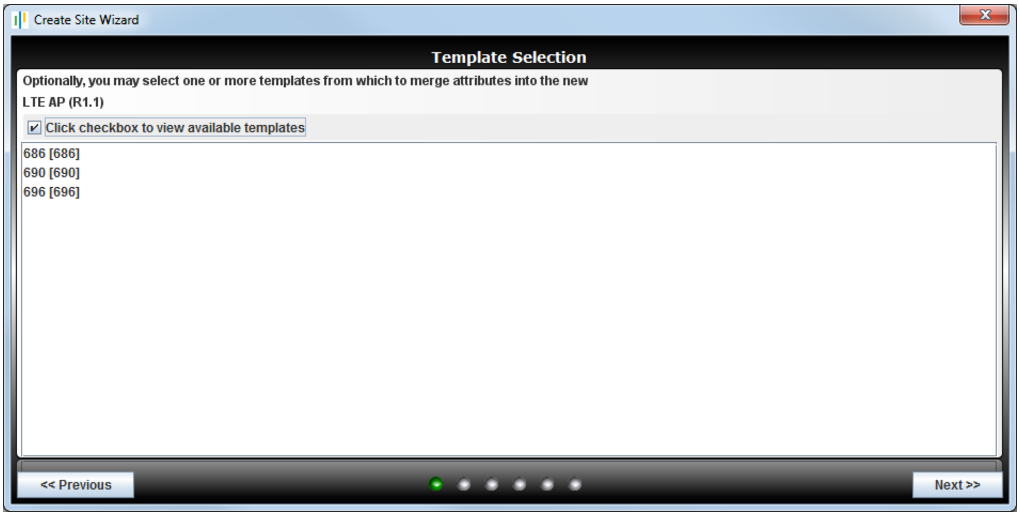
5) If there is a requirement to apply a specific that embodies, for example, a regional policy or AP operational use case, ensure **View Available Templates** is checked.

6) Click **Next**.

7.3.2 Select an AP Template

This is optional as, instead, it is recommended to automatically apply templates by associating them with the Product Class. However, this page can be used to apply one template that embodies, for example, a regional policy or AP operational use case. Alternatively, any number of templates can be applied to the AP on completion of the Create Site Wizard.

7) If **View Available Templates** was checked on the first page of the wizard, the Template Selection page will appear:



Optionally, you may select one or more templates from which to merge attributes into the new LTE AP (R1.1)

☑ Click checkbox to view available templates

686 [686]
690 [690]
696 [696]

Use this page to load a template for the AP. Typically the template can contain a reference configuration for the AP according to the AP's intended location and/or usage.

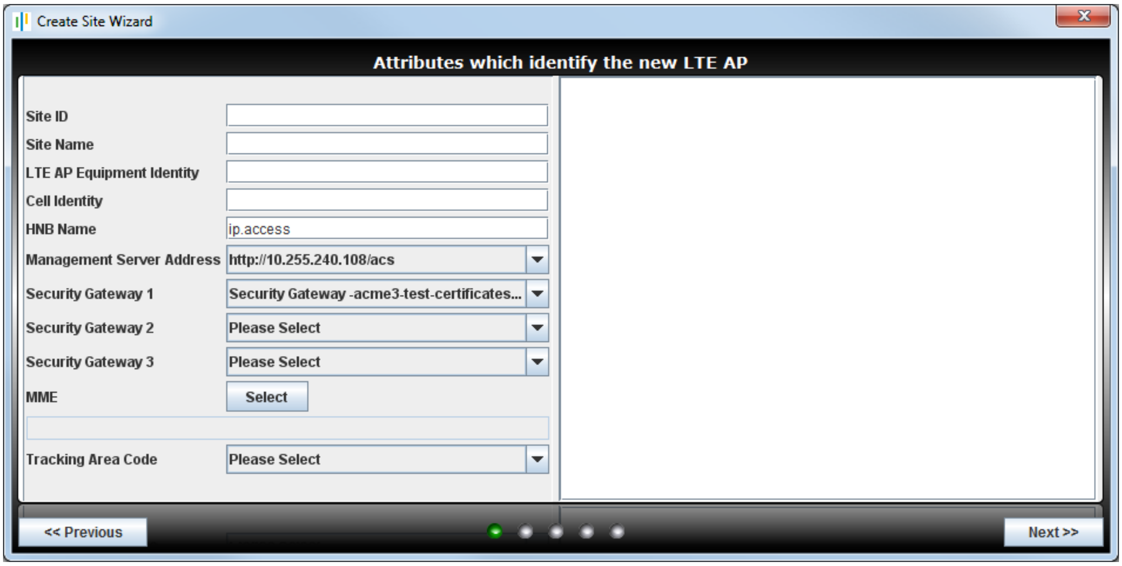
For information on setting up templates for AP provisioning, see [INST_43380].

8) Click the required template in the list, then click **Next>>**.

Note: If a template is not required after all, click **<<Previous**, uncheck **View Available Templates** then click **Next>>** again.

7.3.3 Enter AP Identification Details

9) The page for specifying AP identification details will appear:



Attributes which identify the new LTE AP

Site ID	
Site Name	
LTE AP Equipment Identity	
Cell Identity	
HNB Name	ip.access
Management Server Address	http://10.255.240.108/acs
Security Gateway 1	Security Gateway -acme3-test-certificates...
Security Gateway 2	Please Select
Security Gateway 3	Please Select
MME	Select
Tracking Area Code	Please Select

Notice that the Management Server Address and Security Gateway are set automatically according to the TR-069 object selected for invoking the wizard. The Management Server Address may not be changed.

10) Click in the **Site ID** box and type a numeric ID. This must be unique. As the ID number is entered, the Site Name is set automatically.

Note: Do not use the AP's serial number for the Site ID. An AP can be physically replaced at a site, in which case the site configuration will stay the same, but the AP's serial number will be updated.

11) If required, click in the **Site Name** box and type any text to replace the default Site Name. Enter text that will help identify this site.

12) Click in the **LTE AP Equipment Identity** box and enter the serial number for the AP. This must be an exact match for the AP's serial number. If this does not match, the NOS Server will not allow the AP to connect.

13) If Security Gateway 1 is not correct for this AP, click the drop-down list and choose a different Security Gateway from the available ACME SecGWs defined under Root > Southbound SNMP Interfaces and/or the generic gateways defined under Root > NOS > Security Gateways.

14) Optionally specify Security Gateway 2 and/or Security Gateway 3.

15) If the MME has not been filled from a template or it is not correct for this AP, click the MME **Select** button, choose one or more MMEs from the Edit Target Objects List dialogue, then click **OK**.

Note: Multiple MMEs can be selected by checking the MME Pools object , any combination of MME Pool objects or any selection of individual MME objects.

16) Choose the required **Tracking Area Code** from the drop-down list.

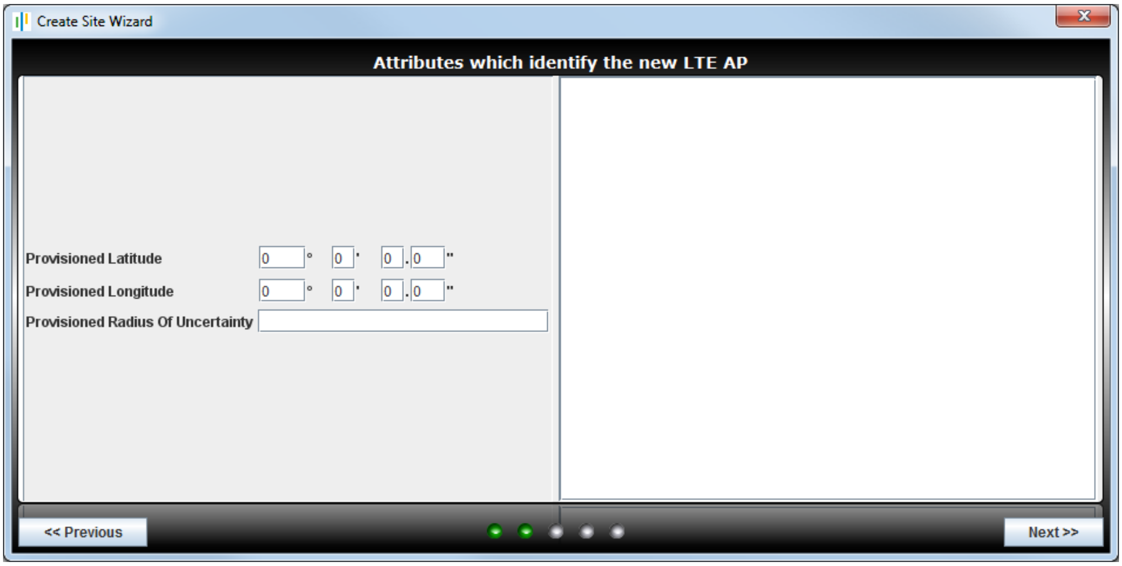
17) Click **Next>>**.

- If there are any errors on this page, the error will be displayed and the wizard will stay on the AP identity details page. For example, the identification details are checked to ensure there are no duplication conflicts with existing APs. Edit the required field(s) to correct the errors then click **Next** again.
- The wizard will go to the next page if there are no errors.

7.3.4 Set the AP Location

This is required by the Static Neighbour List Wizard, to determine candidate neighbours that are near the AP's location.

18) To provide the location of the configured AP, enter the Latitude, Longitude and Radius of Uncertainty in the appropriate fields. If the deployment location



Provisioned Latitude 0 ° 0 ' 0 . 0 "

Provisioned Longitude 0 ° 0 ' 0 . 0 "

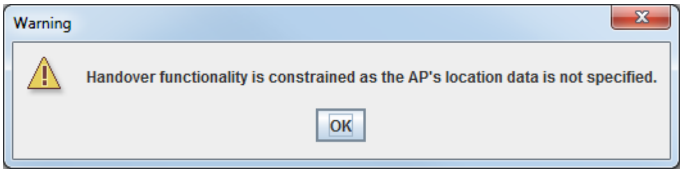
Provisioned Radius Of Uncertainty

If the AP's deployment location is not currently know, leave these fields blank. Alternatively, if the approximate destination location is known, enter a suitable approximation for the coordinates and a larger Radius of Uncertainty.

Note: This sets the location in both the AP object (in Device.FAP.GPS.) and its parent AP Info object (in LTE AP Info Package).

19) Click **Next>>**.

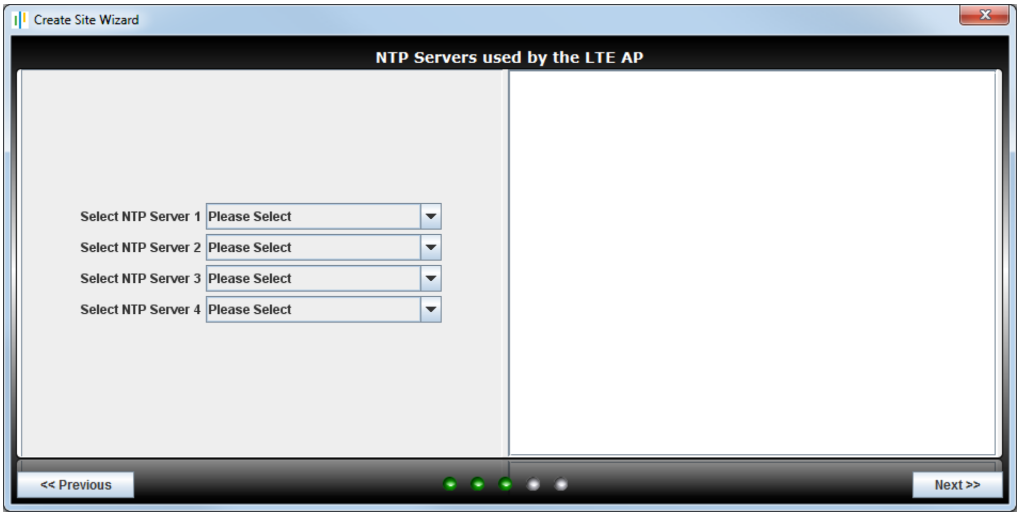
20) If the location is not specified, a warning message will appear. Click **OK** to clear the message:



Handover functionality is constrained as the AP's location data is not specified.

7.3.5 Select NTP Servers

21) The page for selecting NTP servers will appear:



Create Site Wizard

NTP Servers used by the LTE AP

Select NTP Server 1: Please Select

Select NTP Server 2: Please Select

Select NTP Server 3: Please Select

Select NTP Server 4: Please Select

All four NTP server addresses must be selected, as required by the AP's NTP algorithm for setting its time and date.

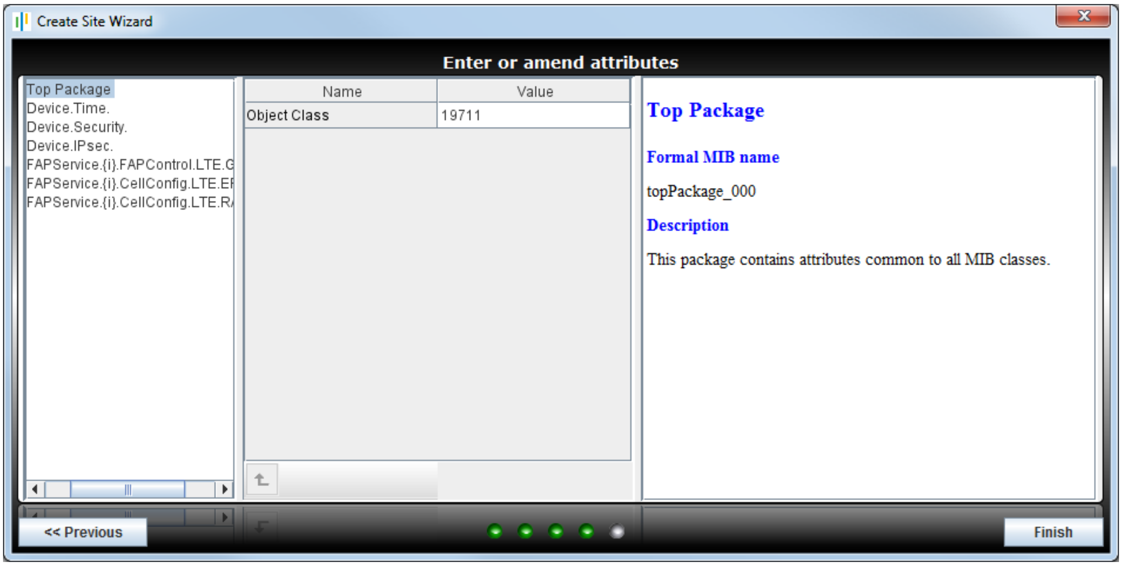
The NTP servers may have been automatically selected from either a template associated with the Product Class or a template selected in the Template page of the wizard. Any changes on this page of the wizard will override settings from a template.

22) Click the drop-down lists to choose the four NTP server addresses for the AP. The the available Meinberg NTP Servers are defined under Root > Southbound SNMP Interfaces and/or any generic NTP Servers are defined under Root > NOS > NTP Servers.

23) Click **Next>>**.

7.3.6 Amend the Mandatory AP Parameters

24) The final page of the wizard has a selection of mandatory attributes:


Create Site Wizard
Enter or amend attributes
Top Package
Device.Time.
Device.Security.
Device.IPsec.
FAPService.{i}.FAPControl.LTE.G
FAPService.{i}.CellConfig.LTE.EF
FAPService.{i}.CellConfig.LTE.R/
<< Previous
Finish

Name	Value
Object Class	19711

Top Package

Formal MIB name

topPackage_000

Description

This package contains attributes common to all MIB classes.

Use this page to check the parameters that are not configured in the previous pages of the wizard. Also, if these parameters have been set by a template as recommended, ensure that the parameters are set are correct for this AP.

25) Select **Device.Security.** on the left. If **X_000295_CRLServerBaseUrl** is not set from a template, enter the correct URL now.

26) Select **Device.IPsec.** on the left. This is enabled by default. If IPsec is not required, uncheck the **Enable** check box.

27) Select **FAPService.{i}.CellConfig.LTE.RAN.RF.** on the left.

28) Ensure that **FreqBandIndicator** is set to the band of operation required for this AP.

29) Ensure that **PhyCellID** is set to a value that does not clash with any neighbour cells.

Note: If the AP's deployment location, and hence its neighbour cells, are not yet known, this can be left at any value until the AP is deployed.

30) Drill down into the **DLBandwidth** parameter and ensure it is set to the correct value in resource blocks, which is one of:

Required Bandwidth	Enter Value in Resource Blocks
5MHz	25
10MHz	50 (default value)
15MHz	75
20MHz	100

31) Click **Finish**.

The site (AP Info object) and the AP object will be added under the LTE APs object and can now be selected for further actions.

Note: Any AP filter results in the NOS Client are cleared so that the new AP Info and AP object can be seen.

7.4 Apply Templates and Configuration Files to the AP

This is optional. This could be done if, for example:

- No templates were used as the basis for the AP's initial configuration
- One or more additional templates are required to apply a policy overlay on top of any templates associated with the Product Class, such as AP use cases or regional policies
- One or more files containing additional configuration must be loaded with Load Attributes From File

7.4.1 Apply an AP Template to the AP

This procedure assumes that this is a one-time operation that should take place immediately.

For general information about templates, including re-applying templates with scheduling, see [OPM_14015].

1) If the AP is not currently visible, use AP filtering to make the required AP visible in the object tree in the Explorer Pane.

   Note: For details on using AP filtering, see [OPM_43005].

2) Select the required **Template Definition** object under **Root > Network Orchestration System > Templates**.

3) Right-click the **Template Definition** object and select **Apply Template**.

4) Select the **Template Operation Package**.

5) Click the **Edit** button for **Target Objects**.

6) Expand the object tree in the **Edit Target Object List** screen until the required **AP object** is shown, then click the **check box** next to the AP object.

7) Click **OK** to close the Edit Target Object List screen.

8) Click **OK** to apply the template. The AP configuration held in the NOS database is updated. The AP will pick up the updated configuration when it connects to the NOS for the first time.

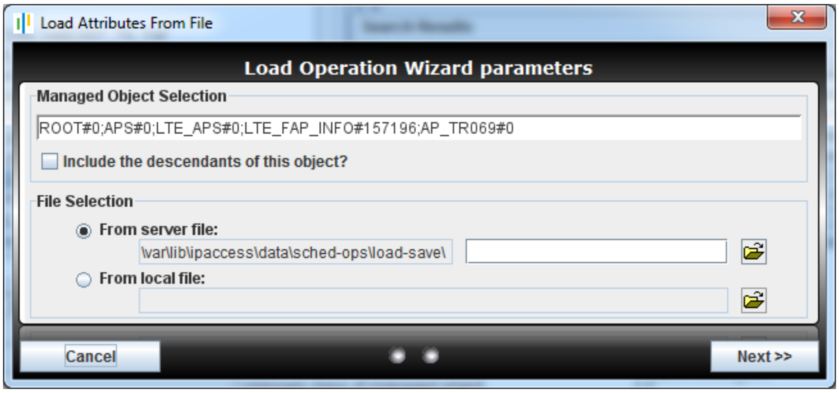
7.4.2 Load a Configuration File for the AP

For information on preparing a configuration file for an AP, see [OPM_43005].

1) If the AP is not currently visible, use AP filtering to make the required AP visible in the object tree in the Explorer Pane.

   Note: For details on using AP filtering, see [OPM_43005].

2) To start the NOS Load Attributes Wizard, right-click on the AP object in the NOS Client and then select **Load Attributes From File**. The Load Attributes From File Wizard shows the chosen AP object:



Load Attributes From File

Load Operation Wizard parameters

Managed Object Selection

ROOT#0;APS#0;LTE_APS#0;LTE_FAP_INFO#157196;AP_TR069#0

□ Include the descendants of this object?

File Selection

● From server file: \var\lib\ipaccess\data\sched-ops\load-save\

○ From local file:

3) Choose **From server file** or **From local file**, according to the location of the required configuration file.

4) Click the Browse button then use the file browser to select the edited configuration file.

5) Click the **Load** or **Open**, according to which file browser is in use, and the file name is shown in the Load Attributes wizard. Click **Next>>**.

6) By default the operation is scheduled for Now, so click **Finish** to load and apply the configuration settings. The AP configuration held in the NOS database is updated. The AP will pick up the updated configuration when it connects to the NOS for the first time.

7) Repeat as needed, if there are multiple configuration files.

7.5 Update the Individual AP Parameters

These are AP object parameters and AP Info object attributes that are either unique per AP or must be selected on a per AP basis (for example, the Physical Cell ID may not be unique, but it depends on the AP's location).

Either update the AP with these settings immediately after completing any other provisioning activities, or apply them once the AP is installed on site and is able to connect to the NOS.

Note: Some of the parameters reviewed in this section are configured in the Create Site Wizard or by applying a template withing the wizard or after completing the wizard. However, it is useful to review these parameters in case any required changes on a per-AP basis were missed during the previous configuration phases.

7.5.1 AP Group

The AP Group is part of the AP Info object's configuration.

Configuring an AP with a Group is optional, depending on whether or not AP Groups are needed.

If AP Group identities correspond to Product Classes, the recommended method for configuring the Group is to associate an AP Info object template with the Product Class. This will set the Group automatically when creating the site.

Alternatively, either set the Group manually with the procedure below or create an AP Info template apply it to the corresponding AP Info objects after provisioning multiple APs. To apply a template after provisioning, use the Apply Templates action on the AP search/filter panel after selecting the required APs - see [OPM_43005] for more details on using this action.

Note: If AP management by Group is already enabled (the Enable Search Filter By User AP Groups option is checked in the Manage Users dialogue box) then only NOS Client users with the Manage Users role will be able to use the search/filter panel to find any APs that are not already in a Group. Hence, only those users can subsequently assign APs to the correct Group either manual or with a template. Once APs are in a Group, any users assigned to manage the AP Group will be able to find and manage the APs in the NOS Client.

1) If the AP is not currently visible, use AP filtering to make the required AP visible in the object tree in the Explorer Pane.

   Note: For details on using AP filtering, see [OPM_43005].

2) Select the **AP Info** object for the required AP.

3) Select the **AP Group Membership Package**.

4) Click the **Select** button for the **Associated Group**.

5) Expand the object tree until the **Groups** are shown.

6) Click the name of the required **Group**, then click **OK**.

7) Click **Apply** to save the changes to the AP Info object.

7.5.2 RF Parameters

1) Select the **AP** object.

2) Select **FAPService.{i}.CellConfig.LTE.RAN.RF.**.

3) Ensure the following parameters are set correctly for this AP:
   - EARFCNDL
   - EARFCNUL
   - FreqBandIndicator
   - DLBandwidth
   - ULBandwidth
   - ReferenceSignalPower
   - PhyCellID
   - X_000295_PHICHResource

4) Click **Commit to DB** to save the parameters in the NOS database. The AP will pick up the updated configuration when it connects to the NOS for the first time.

7.5.3 Other Mandatory Parameters

5) Select the **Device.Time.** package and ensure the **LocalTimeZone** is set correctly.

6) Select **Device.Services.FAPService.{i}.CellConfig.LTE.RAN.PHY.PRACH**. and ensure **RootSequenceIndex** is set correctly. This needs to be different from neighbour cells to prevent RACH collisions.

7) Select **Device.Services.FAPService.{i}. CellConfig.LTE.EPC.** and ensure **TAC** is set correctly.

7.5.4 Other Parameters

8) Select **Device.Services.FAPService.{i}.REM.LTE.** and ensure **X_000295_MacroCellTxThreshold** is set correctly.

9) Select **Device.Services.FAPService.{i}.AccessMgmt.LTE.** and ensure **HNBName** is set correctly.

10) Select **Device.Services.FAPService.{i}.CellConfig.LTE.EPC.** and ensure that the **AllowedCipheringAlgorithmList** and **AllowedIntegrityProtectionAlgorithmList** are correct. That is, delete any unwanted items from each list - there must be at least one item in each list.

    Note: These parameters are not "per AP" parameters, but they must be checked per AP if the network policy is to remove any entries from these lists. This is because unwanted entries in these lists cannot be removed with a template.

7.5.5 Save any Parameter Updates

11) If any parameter values have changed, click **Commit to DB**. The AP configuration held in the NOS database is updated. The AP will pick up the updated configuration when it connects to the NOS for the first time.

7.6 Assign Planned (Static) Neighbours

Configure an enterprise nanoLTE E40 AP with planned "static" neighbours by using the Neighbour List Wizard. Do this when the AP’s deployment location is known. After the AP is installed on site, optionally use information gathered with Network Listen to determine and/or confirm the best LTE neighbours for an AP.

The static neighbour list must be populated so that the AP can successfully handover and reselect to neighbouring cells. Neighbour cells must also be provisioned so that nanoLTE APs can use them for CS Fallback (CSFB).

It is expected that this is an ongoing operations activity, which can be revisited at any time. Hence see [OPM_43005] for full information on creating neighbour cell objects (candidates for AP neighbours) and using the Neighbour Cell Wizard to assign neighbours to an AP. Also see [OPM_43005] for information about using Network Listen to detect neighbouring LTE cells.

8 *How to Implement Policies*

The sections above describe a suggested set of mandatory parameters and templates to be considered for AP provisioning. There are other patterns of behaviour that could usefully be defined in templates for application to selected APs, but these are not usually fundamental to deployment in the way the parameter groups above are.

The groups below could be created as separate overlay templates, or some elements could be added to the Network Wide or AP Mode template if deemed important for a particular deployment design.

The parameters below are all defined in the TR-069 AP CM Data Model Reference Manual [REF_43150], with further information available in other manuals.

Note: For information on configuring the optional Long Range Extension (LRE) feature, see [INST_43375].

The topics in this section are:

- *8.1 Access Control*
- *8.2 Optional Network Listen Policies*
- *8.3 Periodic Inform Interval*
- *8.4 PM Reporting*
- *8.5 DSCP Marking on the Backhaul*
- *8.6 Diagnostics Settings*
- *8.7 Mobility Parameter Optimisation*

8.1 Access Control

The nanoLTE AP only uses Open Access.

8.2 Optional Network Listen Policies

Use Network Listen (NWL) to detect an AP's neighbour lists and calibrate its master frequency to the surrounding macro network. Use these policies to determine Network Listen operates. It is recommended to embody these policies in a template, as in [INST_43380].

For more information about Network Listen see [GST_43415].

8.2.1 Configure Network Listen Schedule

For example, to configure a weekly update in quiet hours:

- Set Device.Services.FAPService.{i}.REM.LTE.ScanPeriodically to True.
- Set Device.Services.FAPService.{i}.REM.LTE. PeriodicInterval to 604800 (i.e. weekly scan is every 604800 seconds).
- Set Device.Services.FAPService.{i}.REM.LTE. PeriodicTime to 2015-01-25T02:00:00+05:00:00.(for example: the specified date is a Sunday, the most typical quiet day; 02:00:00 means Network Listen scanning begins after 2AM; +05:00:00 is timezone offset from UTC).

8.2.2 Configure Bands, PLMNs and EARFCNs to Scan

The LTE Bands, PLMNs and EARFCNs can be restricted for NWL scans. This may be useful for reducing the scan time in areas with macro cells run by several different operators.

To specify a list of Bands to scan, add the required Bands to:

- FAPService.{i}.REM.LTE.REMBandList

To specify a list of PLMNs to scan, add the PLMN IDs to:

- FAPService.{i}.REM.LTE.REMPLMNList

To specify a list of EARFCNs to scan, add the DL EARFCNs to:

- FAPService.{i}.REM.LTE.EUTRACarrierARFCNDLList

If a particular list is empty then the NWL scan is unrestricted in that respect.

8.2.3 Configure the Use of Network Listen for Frequency Synchronisation

Since the AP is doing Network Listen, also tune the AP oscillator against the macro so it remains in calibration indefinitely.

Specify the PLMN(s) to be used for frequency synchronisation by configuring the following:

- Device.Services.FAPService.{i}.REM.LTE.X_000295_PLMNListToSyncWith

Note: Cells will only be detected from the specified list of Scan Bands.

8.3 Periodic Inform Interval

The following tables summarise the recommended minimum and recommended values for setting the Periodic Inform Interval for Enterprise and SOHO APs. These values assume a population of consisting only of the specified AP type. If a mixed population is in use then calculate a pro-rata value.

These initial recommendations are based on typical estimated behaviour. As the network is deployed the aggregate inform rate should be monitored and the Periodic Inform Interval adjusted if needed to keep within NOS limits.

The default value for Device.ManagementServer.PeriodicInformInterval is 43200 seconds, which is 12 hours.

When using a network-wide Periodic Inform Interval that is different to the default, use a template associated with the Product Class to apply this to all APs during pre-provisioning.

8.3.1 Enterprise nanoLTE APs

APs in the Network	Minimum Inform Interval	Recommended Inform Interval
<=5,000	15 mins	30 mins
5 - 10,000	30 mins	60 mins
10 - 15,000	1 hour	2 hours

8.3.2 SOHO nanoLTE APs

APs in the Network	Minimum Inform Interval	Recommended Inform Interval
<=5,000	30 mins	60 mins
5 - 15,000	1 hour	2 hours
15 - 30,000	3 hours	6 hours
25 - 50,000	6 hours	12 hours (default)

8.4 PM Reporting

PM reporting is enabled by default, with a default upload interval of 86400 seconds (daily) at a random time selected by the AP (thus avoiding peaks in server load/bandwidth).

It is recommended to embody these policies in a template, as in [INST_43380].

A destination for PM report uploads must be entered in:

- Device.FAP.PerfMgmt.Config.{i}.URL

Adjust the upload interval in:

- Device.FAP.PerfMgmt.Config.{i}.PeriodicUploadInterval

Configure the reporting time in:

- Device.FAP.PerfMgmt.Config.{i}.PeriodicUploadTime.

If a reporting time is configured then also consider the following parameter:

- Device.Services.FAPService.{i}.REM.LTE.X_000295_RandomisationPeriod

This adds some randomisation to the exact upload time to spread server load/bandwidth. The randomisation period can be adjusted, if required.

8.5 DSCP Marking on the Backhaul

If the default backhaul DSCP values do not match the network policy, configure the following AP parameters to change their settings:

- Device.IP.X_000295_ConfiguredDSCP.NTPDSCP
- Device.IP.X_000295_ConfiguredDSCP.ManagementDSCP

The following parameters under Device.IP.X_000295_ConfiguredDSCP are not supported by the nanoLTE AP, as the QCI configuration (which maps QCI levels to DSCP values) is used instead:

- Device.IP.X_000295_ConfiguredDSCP.PSTrafficDSCP
- Device.IP.X_000295_ConfiguredDSCP.SignallingDSCP

Note: QCI mapping to DSCP values must be configured with the mandatory template, which must be associated with every nanoLTE AP Product Class. See [INST_43380] for details.

8.6 Diagnostics Settings

8.6.1 Diagnostics Reporting

Including parameters from the list below in one or more Templates allows useful collections of diagnostics setting to be turned on or off!.

- Device.FAP.X_000295_DiagMgmt.DiagReporting.{i}
  Each item in this list has a ReportOn condition and a URL for uploading a diagnostics file
- Device.FAP.X_000295_DiagMgmt.PeriodicUploadInterval

To allow post-analysis of AP software issues it is recommended that “Report on Crash” is configured in ReportOn. To allow post-analysis connection problems, use “Report on Lost IPSec” and “Report on Lost Gateway Connection”. The URL is specified separately for each condition, but can be the same URL in all cases.

Periodic Upload is enabled by configuring “Report on Periodic Timeout” in ReportOn with an associated interval in PeriodicUploadInterval. Only use this for a small number of APs for special monitoring purposes.

8.6.2 Diagnostics Tuning

Diagnostics tuning is configured in Device.FAP.X_000295_DiagMgmt.DiagTuning.{i}., which is a list that can contain the following parameters in each item:

- Device.FAP.X_000295_DiagMgmt.DiagTuning.{i}.TuningName
- Device.FAP.X_000295_DiagMgmt.DiagTuning.{i}.TuningValue

The DiagTuning parameters TuningName/TuningValue should only be used on a per AP basis under the guidance of ip.access.

8.7 Mobility Parameter Optimisation

The sections below list the parameter groups used for tuning of handover and reselection behaviour.

Contact ip.access Professional Services for further guidance.

8.7.1 Handover Control

Use the parameters in the following "packages" to control handover behaviour:

- FAPService.{i}.CellConfig.LTE.RAN.Mobility.ConnMode.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.ConnMode.EUTRA.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.ConnMode.Irat.

For descriptions and default values for each parameter within each "package", see [REF_43150].

8.7.2 Standard Reselection (Idle Mode Mobility)

Use the parameters in the following "packages" to control reselection behaviour:

- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.Common.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IntraFreq.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.InterFreq.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.InterFreq.Carrier.{i}.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IRAT.UTRA.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IRAT.UTRA.UTRANFDDFreq.{i}.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IRAT.GERAN.
- FAPService.{i}.CellConfig.LTE.RAN.Mobility.IdleMode.IRAT.GERAN.GERANFreqGroup.{i}.

For descriptions and default values for each parameter within each "package", see [REF_43150].

9 *Installation Checks*

All the activities in this section are managed from the NOS Client.

Use the procedures in this section to ensure the AP is correctly configured. For troubleshooting information, see [TRB_43005].

The activities in this section assume that the AP has now been powered up and connected to the backhaul.

The topics in this section are:

- *9.1 Check and Upgrade the nanoLTE AP Software Image*
- *9.2 Configuration Audit*
- *9.3 Ensure the AP is in Service*

9.1 Check and Upgrade the nanoLTE AP Software Image

This is a useful check to ensure that the AP has the required software version, even if the AP software was recently updated during commissioning or provisioning.

Note: The download of any required software is automated in the NOS for TR-069 by specifying the correct Product Class during Site creation.

9.1.1 Check the Current Software Image Version

1) Login to the NOS Client with a user name (and password) that has Full Access rights for changing the AP's configuration.

2) Use AP filtering to make the required AP visible in the object tree in the **Explorer Pane**.

   Note: For details on using AP filtering, see [OPM_43005].

3) Either select the AP's parent AP Info object in the search results, or find the required AP within the LTE APs area.

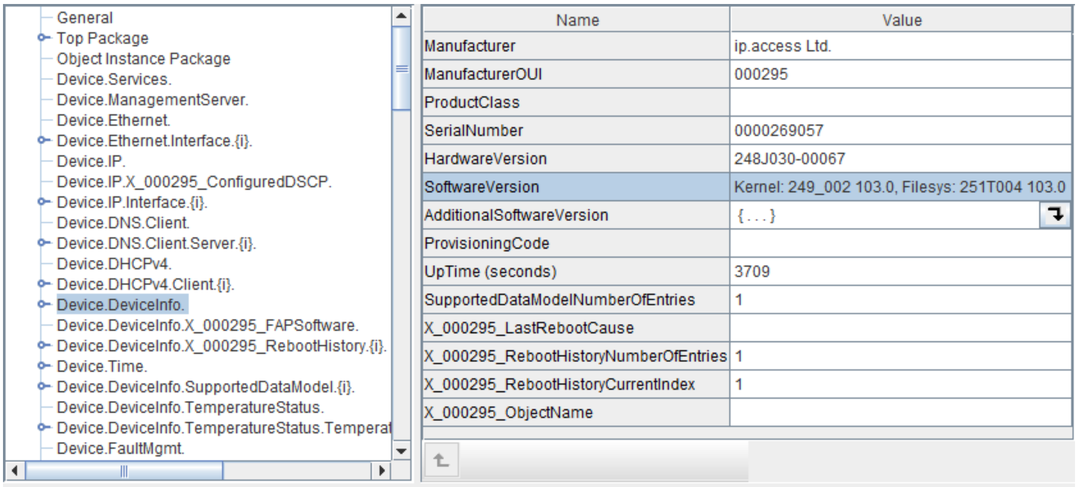
   For example, drill down to the AP like this:

   Root > APs > LTE APs > AP Info > AP

   Note: For full information on using the NOS Client, see [OPM_14015].

4) In the Navigation pane, browse to **Device.DeviceInfo.**.

5) Check the values of the **SW Version** attribute:


General
Top Package
Object Instance Package
Device.Services.
Device.ManagementServer.
Device.Ethernet.
Device.Ethernet.Interface.{i}.
Device.IP.
Device.IP.X_000295_ConfiguredDSCP.
Device.IP.Interface.{i}.
Device.DNS.Client.
Device.DNS.Client.Server.{i}.
Device.DHCPv4.
Device.DHCPv4.Client.{i}.
Device.DeviceInfo.
Device.DeviceInfo.X_000295_FAPSoftware.
Device.DeviceInfo.X_000295_RebootHistory.{i}.
Device.Time.
Device.DeviceInfo.SupportedDataModel.{i}.
Device.DeviceInfo.TemperatureStatus.
Device.DeviceInfo.TemperatureStatus.Temperat
Device.FaultMgmt.

Name	Value
Manufacturer	ip.access Ltd.
ManufacturerOUI	000295
ProductClass	
SerialNumber	0000269057
HardwareVersion	248J030-00067
SoftwareVersion	Kernel: 249_002 103.0, Filesys: 251T004 103.0
AdditionalSoftwareVersion	{...}
ProvisioningCode	
UpTime (seconds)	3709
SupportedDataModelNumberOfEntries	1
X_000295_LastRebootCause	
X_000295_RebootHistoryNumberOfEntries	1
X_000295_RebootHistoryCurrentIndex	1
X_000295_ObjectName	

6) If the AP does not have the latest software image, download it to the AP from the NOS Server according to the instructions in section 9.1.2.

9.1.2 Download the Latest Software Image from the NOS Server to the AP

For instructions about how the software images (SDP files) are uploaded to the NOS Server, see section 5.4.

1) Select **Device.DeviceInfo.** for the AP object and verify that the Filesys version reported by the **Software Version** matches the SDP file that was downloaded.

2) Select the AP's parent **AP Info** object.

3) Click the **Select** button for the **Associated Provisioned SW Version** attribute.

4) Find the new AP SW Version object in the list and click **OK**.

5) Click **Apply** to save the changes.

6) Right-click the AP Info object and select **Actions > Connect Now**. The AP will be updated to the new software version immediately.

9.2 Configuration Audit

9.2.1 Final Attribute Changes and Checks

1) Login to the NOS Client with a user name that has Full Access to the required AP.

2) Use AP filtering to make the required AP visible in the object tree in the Explorer Pane.

   Note: For details on using AP filtering, see [OPM_43005].

3) Check any AP-specific configuration changes that may not have already been applied by the Create Site Wizard or loading configuration files. In particular, ensure the static neighbour lists are correctly configured. See [OPM_43005] for information on neighbour list configuration.

4) Spot check any or all of the following packages to verify the parameters are set to the correct values:

   - Device.Services.FAPService{i}.CellConfig.LTE.RAN.RF
   - Device.Services.FAPService.{i}.CellConfig.LTE.EPC

9.2.2 Network Listen and Frequency Correction

1) If not already logged in, login to the NOS Client with a user name that has Full Access to the required AP.

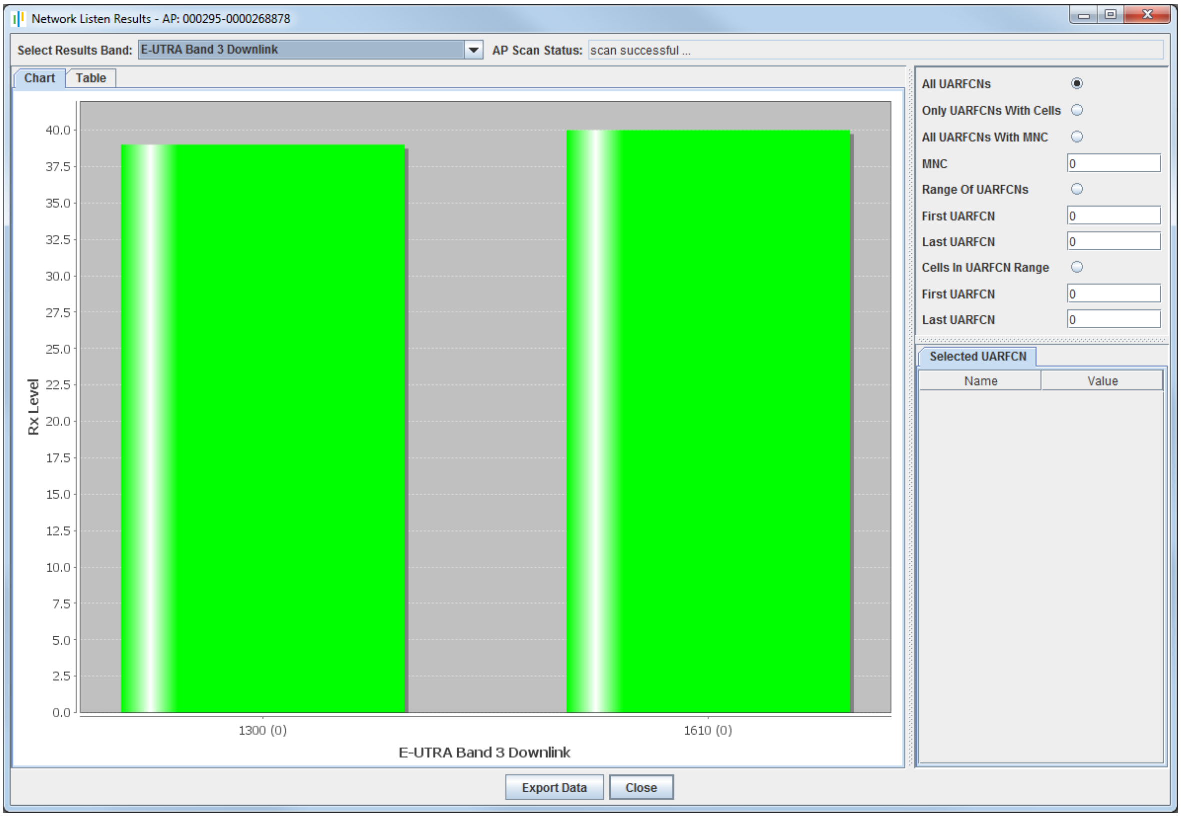
2) Use AP filtering to make the required AP visible in the object tree in the Explorer Pane.

   Note: For details on using AP filtering, see [OPM_43005].

3) Select the AP object and select the Device.DeviceInfo. package and check that the UpTime parameter is greater than 1200 (which is 20 minutes) before continuing. This ensures the frequency crystal has had some time to warm up and achieve a degree of thermal stability prior to checking if it needs any frequency correction.

4) To execute a Network Listen scan, right-click the AP Site (AP Info) object, then select **Action > Perform NWL Scan**.

5) When the scan is complete, view the results to verify there is some radio activity. This assumes that the AP is in a location where it can detect neighbouring LTE cells.


Network Listen Results - AP: 000295-0000268878

Select Results Band: E-UTRA Band 3 Downlink

AP Scan Status: scan successful ...

All UARFCNs ●
Only UARFCNs With Cells ○
All UARFCNs With MNC ○
MNC 0
Range Of UARFCNs ○
First UARFCN 0
Last UARFCN 0
Cells In UARFCN Range ○
First UARFCN 0
Last UARFCN 0

Selected UARFCN

Name	Value

9.3 Ensure the AP is in Service

Once the AP has the latest software image, any additional configuration is complete and any frequency correction has been applied, it is ready for service.

These steps ensure that all configuration changes are correctly applied to the nanoLTE AP.

1) Right-click the AP’s parent AP Info object and select **Actions > Lock AP**.

2) Right-click the AP’s parent AP Info object and select **Actions > Unlock AP**.

3) If the installation engineer is still on site, the engineer should make test calls to verify the AP is providing service.