nano3G AP Installation Manual

N3G_INST_300 292_1.0

ip.access Ltd
Building 2020
Cambourne Business Park
Cambourne
Cambridgeshire CB23 6DW
United Kingdom
www.ipaccess.com

Notices

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
292_0.1	Draft for N3G_2.92 and S16 information	22 Aug 2012	CFB
292_0.2	Updated with S16 information	14 Sep 2012	CFB
292_1.0	Released for N3G_2.92	18 Sep 2012	CFB

Table of Contents

1 Introduction

The ip.access nano3G AP is an indoor Access Point for enterprise applications.

This manual provides all the necessary information required to install an ip.access nano3G AP. The manual provides step-by-step instructions for hardware installation and configuration steps required to bring a nano3G AP into service.

The AP can be configured with a static IP address or it can obtain an IP address dynamically via DHCP. The AP-NOS Server and AP-AC connections can be configured to be secure (via IPSec and a security gateway) or unsecured.

1.1 Overview

This manual is organised as follows:

- This introduction
- An overview of AP installation, including installation requirements for all AP variants and specific requirements for each AP model
- AP pre-provisioning in the NOS Server using the NOS Client
- AP configuration file preparation - this is supplementary information for pre-provisioning
- Commissioning an AP for connection to its serving NOS Server
- AP hardware installation
- Optional activities to finalize installation
- Installation troubleshooting
- Regulatory warnings and safety information

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_415] for information on using the NOS Client.

1.3 Related Information

[INST_440]	nano3G NOS Server Installation Manual (N3G_INST_430)
[OPM_300]	nano3G AP Operations Manual (N3G_OPM_300)
[OPM_415]	NOS Client Operations Manual (N3G_OPM_415)
[OPM_440]	NOS Server Operations Manual (N3G_OPM_440)
[REF_105]	nano3G System Glossary (N3G_REF_105)
[REF_110]	nano3G System Configuration Management (CM) MIB Reference Manual (N3G_REF_110)
[REF_300]	nano3G AP License and Copyright Reference (N3G_REF_300)
[TRB_300]	nano3G AP Troubleshooting Manual (N3G_TRB_300)
[21.905]	Vocabulary for 3GPP Specifications (3GPP 3G TR 21.905)

1.4 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_300], in line with the stipulations of their authors.

1.5 Terminology

Common nano3G System terminology is defined in [REF_105].

For additional 3G terminology, see [21.905].

2 Installation Overview and Requirements

2.1 Installation Tasks

There are three tasks that must be completed to install a nano3G AP and make it ready to provide service:

- Pre-Provisioning
- Commissioning
- Site installation

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

2.1.1 Pre-Provisioning

Pre-provisioning means to provide configuration details for a nano3G AP prior to site installation. As an AP's configuration is stored on its serving NOS Server, an AP can be pre-provisioned at any time. This offers maximum flexibility for pre-provisioning an AP as far or as little ahead of site installation as is needed. Pre-provision a nano3G AP with the information it needs to allow it to provide service, such as a serving AC address, neighbour lists, operating frequency and network identity details.

It is recommended to perform at least some pre-provisioning for an AP before on site installation. As a minimum, use the Create Site Wizard in the NOS Client to create a site and AP object on the serving NOS Server that will contain the AP's configuration. If an AP attempts to connect to its serving NOS Server, but the NOS Server has not yet been provisioned with site details for the AP, the NOS Server will raise alarms about attempts to connect by an unknown AP.

For more information about AP pre-provisioning, see *3 Pre-Provisioning a nano3G AP*.

2.1.2 Commissioning

Use the nano3G AP's built-in configuration web page to configure the AP with the settings it needs to establish a connection with its serving NOS Server.

This is done using a commissioning terminal, either before sending the AP out for installation or on site using a suitably prepared laptop.

Pre-Commissioning

This is recommended for residential deployment. The benefits of commissioning an AP before on site installation are:

- The site installation engineer does not need a commissioning laptop.
- This also means that the site installation engineer does not need to know the user name and password for the AP commissioning web page.
- If the AP has been properly pre-provisioned, the AP is effectively plug-and-play.
- This also means that a nano3G S8 AP or nano3G S16 AP could be installed by an end customer, without help from a site installation engineer. The customer simply needs to provide suitable network and power connections.

Note: For residential deployments, commissioning should have already been done at the factory or by the supplier. If in doubt, contact the supplier for confirmation.

On-Site Commissioning

The benefits of using a laptop for commissioning an AP on site are:

- If there is a commissioning error, this can be corrected immediately without needing to return the AP
- If an AP has been in storage for some time, the required software build and/or ATAS package can be installed on the AP on site, without needing to return the AP to base

2.1.3 On Site Installation

Physical installation of a nano3G AP at its operating site, including providing the AP with power and a suitable network connection that provides a backhaul path to the NOS Server and AC.

If a nano3G AP has been enabled for service prior to the site visit, the installation engineer can make test calls immediately.

Note: For some deployment scenarios, APs may be setup by end users. Generally, this may be the case for plug and play residential deployments, where the end user has some easy to follow setup instructions.

Note: Due to the physical installation requirements of a nano3G E8 AP or E16 AP, which **must** be securely wall mounted in a location with adequate ventilation, it is recommended that an E8 AP or E16 AP is installed by a suitably qualified site installation engineer.

2.2 Requirements for All nano3G APs

This applies to all nano3G APs.

2.2.1 General Requirements

Requirements for Commissioning

- A commissioning terminal, which can be either a desktop computer or a laptop, with:
  - OS: Windows XP or later
  - Web browser: Microsoft Internet Explorer 7 or later
  - JavaScript enabled in the web browser
- A short Ethernet cable for connecting the commissioning terminal to the AP
- A temporary means to provide power to the AP while it is connected to the commissioning terminal

Site Installation Requirements

All nano3G AP models have the following general requirements for installation:

- A permanent means to provide power to the AP once it is connected to the backhaul
- An Ethernet connection to the backhaul via CAT5 Ethernet cabling
- Access to a DNS service on the backhaul to resolve symbolic addresses
- Access to NTP services on the backhaul to set the correct time and date each time the AP starts up
- Access to a DHCP service on the backhaul to allow dynamic IP address configuration
- If IPsec will be used to secure the interface across the backhaul, access to the relevant Security Gateway that terminates the IPsec tunnel
- If a firewall is in place on the network an AP will use for backhaul, this must be configured to allow traffic to and from the AP - see the port usage section below

Port Usage

All connections are outgoing. That is, they are initiated from the AP. Port usage has some dependency on whether or not the AP is using IPsec.

With IPSec, the standard two ports are used:

Protocol	Destination Port	Use
udp	500	IPSec initial connection
udp	4500	IPSec operations

Without IPSec, the following ports are used:

Protocol	Destination Port	Use
sctp	29169	SCTP connection
udp	1024 to 1086	CS RTP to AC
udp	1025 to 1087	CS RTCP to AC
udp	1088 to 1150	CS Mux to AC
udp	2152	PS GTP to AC

These ports are used and allowed through the firewall where IPsec is used:

Protocol	Destination Port	Use
tcp	80	PM upload, software download, CRL download
tcp	443	PM upload, software download, CRL download
udp	53	DNS
udp	123	NTP

The following ports are allowed through the firewall independently of IPsec configuration. For example:

AP > Firewall > DHCP Server

Protocol	Destination Port	Use
udp	67	DHCP - not needed for static IP configuration
udp	68	DHCP - not needed for static IP configuration

2.2.2 nano3G AP Cooling

Special attention **must** be given to ensure a nano3G AP will meet its air cooling requirements in its installed location.

Take the following points into consideration for the physical location of an AP:

- All AP models **must** be installed so that they are upright, to ensure proper air will flow through the body of the AP to provide cooling.
- All AP models **must no**t be installed in enclosed spaces where air flow is restricted. This includes, but is not necessarily limited to:
  - Roof or ceiling spaces
  - Small cabinets
  - Tightly enclosed shelf spaces
- When free-standing the nano3G S8 AP, the stand supplied for this purpose **must** be used, and the AP must be upright, as noted above.

2.2.3 Information Required for Pre-Provisioning

This information will be used to configure an AP from the NOS Client. The parameters depend on the deployment scenarios:

- Parameters for Enterprise Deployments
- Parameters for Residential Deployments

Note: It is recommended to pre-provision an AP before taking it on site, so that the AP can download its configuration when it starts up on site.

OMC-R Client Login Details

User name and password for the NOS Client. To be able to configure an AP from the NOS Client, the user name must have Full Access to the NOS Server serving the AP and Full Access granted to its APs. See [OPM_415] for full details about user permissions.

2.2.4 Parameters for Enterprise Deployments

Minimum Configuration - Enterprise Deployments

The minimum set of configuration data for the AP is:

Parameter	Notes
HNB C-Id (hnbCId)	This is the unique ID of this AP on the serving nano3G AC. The term HNB is used in 3GPP in reference to small cells. The HNB C-Id is used in the Register Request message to uniquely identify the AP within the AC. The value is also combined with the RNC-ID to give the 28 bit UC-Id (also known as TR-196 CellID) that is used on-air in SIB3. Use the same value in the dummy cell.
RNC ID (mcIdentity)	RNC ID of the AC - this is selected by choosing the BSMIS object for the AP's site.
AC address (acAddressinUse)	IP Address or FQDN of the serving AC.
MCC (mcc)	Mobile Country Code.
MNC (mnc)	Mobile Network Code.
LAC (lac)	Location Area Code.
RAC (lac)	Routing Area Code.
SAI SAC (sac)	This is the SAI SAC (Service Access Code) which can be used by the billing system. If this is not used by the billing system, it is recommended to set this to 1.
SAI LAC (saiLac)	SAI Location Area Code which can be used by the billing system. This is a different value than the LAC set in the lacRacCandidateList for an individual AP. If this is not used by the billing system, it is recommended to set this to 1.
UARFCN within (rfParamsCandidateList)	The frequency on which the AP will operate. This should be determined by network planning.
Scrambling code within (rfParamsCandidateList)	The scrambling code assigned to the AP. This should be determined by network planning.
RSSI scan bands (rssiScanBands_002)	Specify which bands to scan with Network Listen, when performing RSSI detect and BCCH decode tests. Leave this empty to scan all bands supported by the AP hardware.
Lat, Long and LCS uncertainty (lcsLatitude), (lcsLongitude), (lcsUncertainty)	Latitude and longitude of the APs installation site, for RANAP location reporting

Other Attributes - Enterprise Deployments

The following table shows some other attributes to consider for initial AP configuration. Apart from the static neighbour lists, which are usually configured individually, any of these can be in a general template for all APs or can be set individually.

.

Parameter	Notes
Cell Parameter Selection Method (cellParameterSelectionMethod)	Determines whether values for cell parameters such as UARFCN, LAC, RAC, and CPICH TX Power are selected by Network Listen (NWL) or are configured via the management system. The default is configuration by the management system. In this case, cell parameters should be determined through planning, preferably informed by on site measurements. This is particularly appropriate for the enterprise APs, nano3G E8 APs and nano3G E16 APs and for nano3G S8 APs used in enterprise or SOHO environments.
Neighbour List Population (neighbourListPopulation)	This determines how the live neighbour list is populated. For enterprise and SOHO deployments, the recommended setting is STATIC_ONLY, which only uses neighbours entered in the static neighbour lists, as determined by network planning.
Static neighbour lists, GSM and UMTS (staticGsmNeighbourList), (staticUMTSNeighbourList_001)	These are complex attribute that specify GSM (2G) and UMTS (3G) neighbour candidates. It is recommended to enter these directly in the NOS Client. However, if a similar list has already been configured for a nearby AP, it may be advantageous to copy this attribute from a configuration file saved from the nearby AP, load this into the target AP and then make suitable adjustments from the NOS Client. See [OPM_300] for static neighbour list configuration **Note:** In the static neighbour list, the list must be ordered by **best first** to ensure optimal reselection and handover.
Neighbour PLMNs (neighbourPlmns)	If specified, this restricts the networks that neighbouring cells can belong to for populating the neighbour lists by specifying the MCC/MNC values.
PLMNs To Sync With (plmnsToSyncWith)	If specified, this restricts the networks that nearby cells can belong to for frequency synchronisation by specifying the MCC/MNC values.
PM Reporting URL (reportingUrl)	For reporting performance measurements to the PMS on the NOS.
Diagnostic Reporting URL (diagnosticReportingUrl)	Set the URL of the NOS Server diagnostics service. Replace oam.server with the IP address or FQDN of the server.
reportingUrl (reportingUrl)	Set the URL of the NOS Server measurement reporting service. Replace oam.server with the IP address or FQDN of the server.
localTimeZone (localTimeZone)	Set the timezone, in POSIX format, where the APs are located. This assumes that all APs on the same AC are in the same timezone, which is the most probable scenario. If APs are spread across several timezones, this can be an AP-specific setting.
psHandoverEnabled (psHandoverEnabled)	Whether or not PS RABs will handover between an AP and the macro network. This is disabled (false) by default.

Parameter	Notes
Oscillator Synchronisation Timeout (oscillatorSynchronisationTimeout)	The number of days an AP can go without resynchronisation before it raises the relevant alarm.
Closed Access vs Open Access	See section 2.2.6.
IuUP Initialisation (iuUpInitNoDataSupported)	If this attribute is set to TRUE (default value), the AP includes NO_DATA RFCs as appropriate in IuUP Initialisation frames.If this attribute is set to FALSE, the HNB omits any NO_DATA RFCs that would otherwise have been included.
Network Listen Scan Interval (applyFrequencyCorrection)	Set the interval for frequency corrections. Default is 28 days. For enterprise deployments use the OCXO option, this can be increased to any value.
Realm Id (realmId)	Allows a nano3G AP to include a configurable realm in the HNBAP Register Request message. This is only used by Iuh APs.

2.2.5 Parameters for Residential Deployments

Minimum Configuration - Residential Deployments

The minimum set of configuration data for the AP is:

Parameter	Notes
HNB C-Id (hnbCId)	This is the unique ID of this AP on the serving nano3G AC. The term HNB is used in 3GPP in reference to small cells. The HNB C-Id is used in the Register Request message to uniquely identify the AP within the AC. The value is also combined with the RNC-ID to give the 28 bit UC-Id (also known as TR-196 CellID) that is used on-air in SIB3. Use the same value in the dummy cell.
RNC ID (mcIdentity)	RNC ID of the AC - this is selected by choosing the BSMIS object for the AP's site.
AC address (acAddressinUse)	IP Address or FQDN of the serving AC.
MCC (mcc)	Mobile Country Code.
MNC (mnc)	Mobile Network Code.

Parameter	Notes
Cell Parameter Selection Method (cellParameterSelectionMethod)	Determines whether values for cell parameters such as UARFCN, LAC, RAC, and CPICH TX Power are selected by Network Listen (NWL) or are configured via the management system. The default is configuration by the management system. In this case, cell parameters should be determined through planning, preferably informed by on site measurements. This is particularly appropriate for the enterprise APs, nano3G E8 APs and nano3G E16 APs and for nano3G S8 APs used in enterprise environments. Configuration by NWL can be selected for APs that are deployed for plug-and-play installation by end users - typically only nano3G S8 APs. In this case, the AP configuration must include extended LAC/RAC and RF Parameter Candidate Lists. This is so that the AP can choose the best settings from the candidate lists according to its RF environment.
LAC (lac)	Location Area Code. For configuration by Network Listen (NWL), an AP needs a list of candidate LACs that can be chosen NWL. NWL will look for the least conflicting option.
RAC (rac)	Routing Area Code. For configuration by Network Listen (NWL), an AP needs a list of candidate RACs that can be chosen by NWL. NWL will look for the least conflicting option.
SAI SAC (sac)	This is the SAI SAC (Service Access Code) which can be used by the billing system. If this is not used by the billing system, it is recommended to set this to 1.
SAI LAC (saiLac)	SAI Location Area Code which can be used by the billing system. This is a different value than the LAC set in the lacRacCandidateList for an individual AP. If this is not used by the billing system, it is recommended to set this to 1.
UARFCN within (rfParamsCandidateList)	The frequency on which the AP will operate. For configuration by Network Listen (NWL), an AP needs a list of candidate UARFCNs that can be chosen by NWL.NWL will look for the least conflicting option.
Scrambling code within (rfParamsCandidateList)	The scrambling code assigned to the AP. For configuration by Network Listen (NWL), an AP needs a list of candidate Scrambling Codes that can be chosen by NWL.NWL will look for the least conflicting option.
RSSI scan bands (rssiScanBands_002)	Specify which bands to scan with Network Listen, when performing RSSI detect and BCCH decode tests. Leave this empty to scan all bands supported by the AP hardware.
Lat, Long and LCS uncertainty (lcsLatitude), (lcsLongitude), (lcsUncertainty)	Latitude and longitude of the APs installation site, for RANAP location reporting

Other Attributes - Residential Deployments

The following table shows some other attributes to consider for initial AP configuration. Apart from the static neighbour lists, which are usually configured individually, any of these can be in a general template for all APs or can be set individually.

Parameter	Notes
Neighbour List Population (neighbourListPopulation)	This determines how the live neighbour list is populated. For residential deployments, the recommended setting is MERGE_STSTIC_AND_DETECTED, so that neighbours can be determined by Network Listen as well as network planning.
Static neighbour lists, GSM and UMTS (staticGsmNeighbourList), (staticUMTSNeighbourList_001)	This is generally not needed for residential deployments. Where APs use Network Listen (NWL) to detect neighbours. However there may be some cases where it is necessary to configure some static neighbours. See [OPM_300] for static neighbour list configuration **Note:** In the static neighbour list, the list must be ordered by "best first" to ensure optimal reselection and handover.
Neighbour PLMNs (neighbourPlmns)	If specified, this restricts the networks that neighbouring cells can belong to for populating the neighbour lists by specifying the MCC/MNC values.
PLMNs To Sync With (plmnsToSyncWith)	If specified, this restricts the networks that nearby cells can belong to for frequency synchronisation by specifying the MCC/MNC values.
PM Reporting URL (reportingUrl)	For reporting performance measurements to the PMS on the NOS.
Diagnostic Reporting URL (diagnosticReportingUrl)	Set the URL of the NOS Server diagnostics service. Replace oam.server with the IP address or FQDN of the server.
reportingUrl (reportingUrl)	Set the URL of the NOS Server measurement reporting service. Replace oam.server with the IP address or FQDN of the server.
localTimeZone (localTimeZone)	Set the timezone, in POSIX format, where the APs are located. This assumes that all APs on the same AC are in the same timezone, which is the most probable scenario. If APs are spread across several timezones, this can be an AP-specific setting.
psHandoverEnabled (psHandoverEnabled)	This is disabled (false) by default. This is the normal setting for residential deployments.
Oscillator Synchronisation Timeout (oscillatorSynchronisationTimeout)	The number of days an AP can go without resynchronisation before it raises the relevant alarm.
Closed Access vs Open Access	See section 2.2.6.
Access Control List (accessControlList)	Entries in the Access Control List are only needed if an AP is configured for Closed Access. The Access Control List is a white list of IMSIs that are allowed to use the AP. Each entry in the Access Control List also has an option to allow hand-in from the macro network. A UE that is on the white list for multiple APs can only be Allowed to do this on one AP.

Parameter	Notes
IuUP Initialisation (iuUpInitNoDataSupported)	If this attribute is set to TRUE (default value), the AP includes NO_DATA RFCs as appropriate in IuUP Initialisation frames.If this attribute is set to FALSE, the HNB omits any NO_DATA RFCs that would otherwise have been included.
Network Listen Scan Interval (applyFrequencyCorrection)	Set the interval for frequency corrections. Default is 28 days. 1 day for VCTCXO. This is used for most residential deployments. Any time for OCXO.
Realm Id (realmId)	Allows a nano3G AP to include a configurable realm in the HNBAP Register Request message. This is only used by Iuh APs.

2.2.6 Access Control

The configurations for four common scenarios are described here:

- Full open access (Enterprise or Residential)
- Open access for Zonal AP (Enterprise only)
- Closed access with CSG parameter broadcast and Access Control via the AC, which uses the AAA service (Enterprise or Residential)
- Closed access using Legacy Mode, with Access Control via the AC, which uses the AAA service (Enterprise or Residential)

Note: In all cases, a UE that needs to make an emergency call can access an AP for that purpose.

Full Open Access

In this scenario, any UE on the operator's network can use the AP.

Use the following attribute settings:

Attribute	Setting	Notes
CSG Access Mode (csgAccessMode)	Open	This is the default for nano3G APs. No other settings are required.

Open Access with Zonal AP Functionality

In this scenario, any UE on the operator's network can use the AP. However, the AP will notify the AC when UEs camp onto the AP, so that UEs registered for location services can be identified and, if appropriate, trigger some action.

Zonal functionality requires the following attribute settings:

Attribute	Setting	Notes
Zonal AP (reservedBoolean2)	True	When set to True, this attribute causes the Iuh 3GAP to request the IMSI from the UEs when operating in Open Access Mode. This IMSI is then included in the HNBAP UE Registration and De-Registration Messages between the AP and AC.
CSG Access Mode (csgAccessMode)	Hybrid	Must be set to Hybrid as part of the mechanism that ensures the IMSI check takes place with the AC.
Non CSG UE Access Decision (nonCsgUeAccessDecision)	Query	Causes the AP to perform an IMSI challenge to provide the AC with the IMSI. The AC checks the IMSI with the AAA service in the NOS, which always succeeds for access. The AAA service uses this information to inform any registered Zonal presence application.
Access Decision Mode (accessDecisionMode)	CSG Lite	The AP transmits the CSGIndicator, CSGID, and HNBIdentifier (when available). This prevents foreign CSG-capable UEs from attempting to access the HNB. This setting does not invoke CSG based access control.
Closed Subscriber Group Identifier (csgId)	0 to 134217727	This is the Closed Subscriber Group Identity. This is broadcast in SIB3 when Access Decision Mode is set to CSG Lite. The UE may have a whitelist of CSGIDs, and may also permit manual selection of CSGIDs via the corresponding HNB Names.
HNB Name (hnbName)	Text	This is an optional name of up to 48 characters. It is only broadcast (in SIB20) if it has a value and when Access Decision Mode is set to CSG Lite. Together with the CSG ID, this can be used to identify a CSG cell to a UE user.

Information about zone configuration and implementation and setting up subscribed services for GSMA OneAPI is outside the scope of this manual. Refer to manuals covering the nano3G System NOS for further information.

2.2.7 Closed Access with CSG Parameter Broadcast

This is the recommended approach for Closed Access.

A Closed Subscriber Group (CSG) identifies a cell to a UE in order for the UE to determine whether or not it should attempt to use that cell according to a whitelist of CSG identifiers stored by the UE. This is a 3GPP Release 9 capability, and may or may not be used by Rel 9 UEs.

In this scenario, the AP transmits CSG information and as a result, CSG-aware Release 9 UEs that do not have the AP in their CSG whitelists will ignore the AP. However, this is not a full implementation of CSG-based access control.

Note: This assumes that the operator has mechanisms in place to update CSG-aware UEs that need to use the APs.

All other UEs will attempt to access the AP, but only UEs that are in the whitelist will be allowed access to the AP.

Use the following attribute settings:

Attribute	Setting	Notes
CSG Access Mode (csgAccessMode)	Hybrid	The AP also accepts UEs that do not implement CSG.
Access Decision Mode (accessDecisionMode)	CSG Lite	The AP transmits the CSGIndicator, CSGID, and HNBIdentifier (when available). This prevents foreign CSG-capable UEs from attempting to access the HNB. This setting does not invoke CSG based access control.
Non CSG UE Access Decision (nonCsgUeAccessDecision)	Query	Causes the AP to perform an IMSI challenge to provide the AC with the IMSI (or IMEI for emergency calls). The AC checks the IMSI with the AAA service in the NOS, which checks the IMSI whitelist configured for the AP to determine whether or not the AP is granted access.
Closed Subscriber Group Identifier (csgId)	0 to 134217727	This is the Closed Subscriber Group Identity. This is broadcast in SIB3 when Access Decision Mode is set to CSG Lite. The UE may have a whitelist of CSGIDs, and may also permit manual selection of CSGIDs via the corresponding HNB Names.
HNB Name (hnbName)	Text	This is an optional name of up to 48 characters. It is only broadcast (in SIB20) if it has a value and when Access Decision Mode is set to CSG Lite. Together with the CSG ID, this can be used to identify a CSG cell to a UE user.
Access Control List (accessControlList)	List of IMSIs and corresponding phone numbers	This is provisioned against an AP but used by the AAA service in the NOS.

2.2.8 Closed Access in Legacy Mode

In this scenario, the AP does not transmit any CSG parameters. Access control is performed for all UEs.

Use the following attribute settings:

Attribute	Setting	Notes
Access Decision Mode (accessDecisionMode)	Legacy Mode	Instructs the AP to function in a mode that does not transmit any CSG parameters.
Non CSG UE Access Decision (nonCsgUeAccessDecision)	Query	Causes the AP to perform an IMSI challenge to provide the AC with the IMSI (or IMEI for emergency calls). The AC checks the IMSI with the AAA service in the NOS, which checks the IMSI whitelist configured for the AP to determine whether or not the AP is granted access.
Access Control List (accessControlList)	List of IMSIs and corresponding phone numbers	This is provisioned against an AP but used by the AAA service in the NOS.

2.2.9 Pre-Prepared Configurations - Optional

The options described here can be used independently or in any combination.

Use an Existing AP

The Create Site Wizard, which is used for the initial pre-provisioning of an AP, allows selection of an existing AP as the basis for configuring the new AP. This is a one-time option that is only available in the Create Site Wizard.

Configuration Files

An initial configuration file can be used to rapidly configure the AP via the NOS Create Site Wizard. This is can be an alternative or in addition to using settings from an existing AP or using a template. Additional configuration files can be loaded against the AP object after it has been created by the Create Site Wizard. If they will be used, the location of any configuration files must be known.

Configuration files are described in section 4.

AP Templates

As with configuration files, an initial AP template can be used to rapidly configure the AP via the NOS Create Site Wizard. This can be an alternative to or in addition to using settings from an existing AP or using a configuration file. Additional templates can be applied against the AP object after it has been created by the Create Site Wizard.

For information on working with templates, see [OPM_415].

2.2.10 Information Required for Commissioning

All nano3G AP models require the configuration details listed in this section. Use this information to commission an AP from the commissioning terminal, so that the AP can subsequently connect to its serving NOS Server.

It is possible to commission an AP before taking it on site.

Note: For residential deployments, commissioning should have already been done at the factory or by the supplier. If in doubt, contact the supplier for confirmation.

For connecting to the AP from the commissioning terminal:

- User name and password for the AP web server - if necessary, contact customer support at ip.access for the current user name and password

For commissioning the AP:

- IP Address or FQDN of the serving NOS Server
- IP Address or FQDN of an NTP server
- DHCP or static IP
- If static IP is required:
  - IP address for the AP
  - Netmask
  - IP Address or FQDN of the default gateway
  - IP Address or FQDN of the Primary DNS
- IPSec is optional, but if IPSec is required:
  - IP Address or FQDN of the IPsec Security Gateway
  - IP Address or FQDN of a CRL server
  - Optionally, Traffic Selector information (IP address and subnet mask)
    A traffic selector defines a range of IP addresses that are sent through the IPSec tunnel. This allows an extra degree of control over the traffic that is passed down the IPSec tunnel. Normally, the security gateway controls this range and no other configuration is needed.

2.2.11 Other Items for Commissioning

The items in this section can only be used if the commissioning terminal is running a web server that provides a path to any ip.access AP software download packages. That is, the required .sdp files must be present on the commissioning terminal.

Setting up a web server for this purpose on the commissioning terminal is outside the scope of this manual.

Software Image

If there is a requirement to update the AP's software during commissioning, the relevant .sdp file must be present on the commissioning terminal.

ATAS File

If there is a requirement to update the trust anchors in the AP during commissioning, the relevant .sdp file containing the ATAS package must be present on the commissioning terminal, ready to be downloaded to the AP. The ATAS package contains augmenting trust anchors which allow an AP to trust specific security gateways.

This will be necessary where the security gateway certificates are not supplied by ip.access Limited, to ensure the ATAS package is correct for the security gateway terminating IPsec.

The .sdp file containing the ATAS package must be created for the specific security gateways used in each implementation of the nano3G System. This must be done in consultancy with ip.access Limited prior to system deployment.

2.3 nano3G S8 AP Site Requirements

In addition to the site requirements for all APs, each S8 AP will require:

- Power supplied in one of the following ways, according to the accessory unit(s) supplied with the S8 AP:
  - From the mains adaptor unit, which requires a suitable mains power supply point near the AP that is within reach of the adaptor's cabling

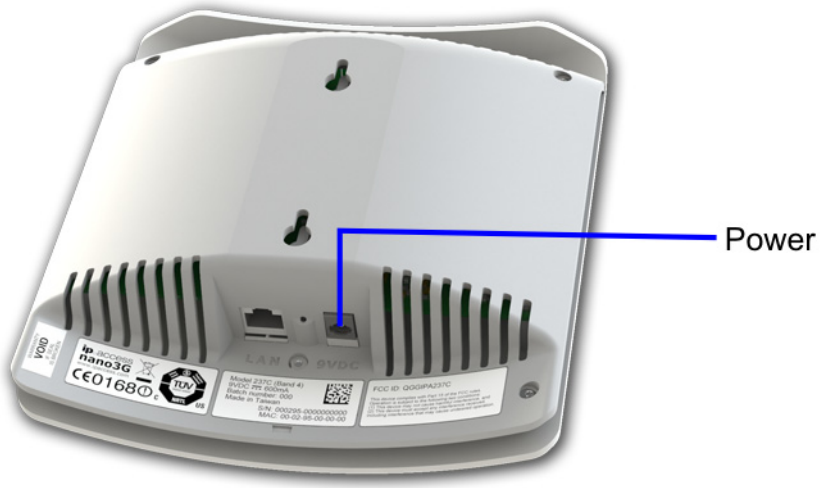
  or

  - From the supplied POE splitter, which requires a Power over Ethernet connection to the splitter
- A site for the AP:
  - Wall mount location

  or

  - Stable surface for free standing installation

2.3.1 nano3G S8 AP Power Requirements



Maximum expected power consumption:

- 8 Watts (Rated 9VDC 890mA)

The nano3G S8 AP supports the following power and Ethernet cabling options:

- Direct power from the power adapter
- Power over Ethernet from the POE injector, via the POE splitter
- Power over Ethernet from a POE switch, via the POE splitter

A POE cable must not be inserted directly into the AP.

The power adapter, as well as the POE inserter and splitter supplied by ip.access comply with LPS requirements in accordance with IEC/EN 60950-1.

Power Adapter

A suitable mains power supply point into which the power adapter for the AP can be plugged.

Only use the power adapter available from ip.access to power the AP:

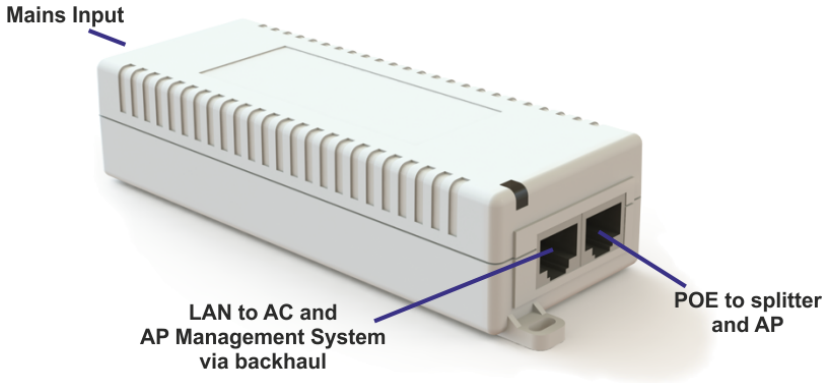
ip.access part number	PSA15R-090PV-R
Input	100-240V ~ 50/60Hz 0.5A
Output	+9VDC 1.67A

Power over Ethernet

POE requires the use of a power inserter and a splitter. The power inserter is positioned close to the backhaul network connection and mains supply, while the splitter is positioned close to the AP.

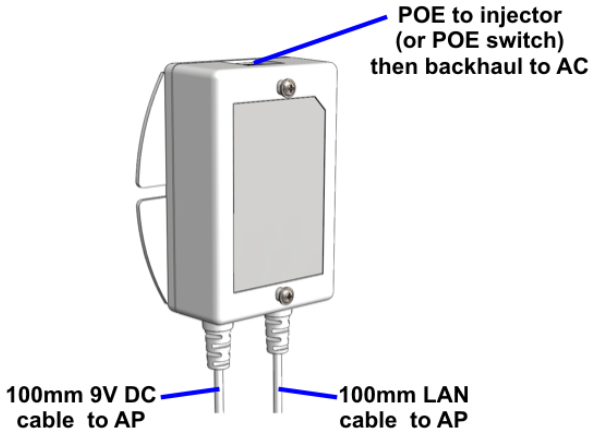
This is the POE inserter supplied by ip.access:

ip.access part number	236
Input	100/240V ~ 60/50Hz 0.5A
Output	48VDC 0.35A



Only use the POE splitter available from ip.access:

ip.access part number	222A
Input	48VDC 0.35A
Output	9VDC 1.33A



2.3.2 nano3G S8 AP Physical Requirements

A nano3G S8 AP may be installed in one of the following ways (see section 6.2.4):

- Free-standing on a flat stable surface.
- Attached to a wall or partition using two screws that engage in keyhole slots in the rear surface of the AP.
- Attached to a POE splitter using the two screws that engage in keyhole slots in the rear surface of the AP. The POE splitter in turn attaches to a wall or partition using two screws.

The unit **must** be vertical to ensure that air can circulate freely around it.

It is recommended to install the AP with its front surface facing the area requiring cellular coverage, unobstructed by walls or partitions that may cause significant RF attenuation.

Dimensions and weight	Height	176mm (without stand) 193mm (with stand)
	Width	170mm
	Depth	51mm
	Approximate Weight	0.42 kg (AP only)
Environmental	Cooling	Vents on the back at top and bottom
	Operating Temperature	0°C to 40°C
	Operating Humidity	10 to 70% non-condensing

2.3.3 nano3G S8 AP IP Bandwidth Requirements

At maximum capacity, a nano3G S8 AP will require:

- Downlink: 17Mbps
- Uplink: 1.8Mbps

This will deliver up to 8 voice calls and HSDPA services up to 14.4 Mbps.

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8 N User Configuration.

2.3.4 nano3G S8 AP Sundry Installation Equipment

To mount the POE splitter or the nano3G S8 AP onto the wall:

- 2 self tapping pan head screws, size No. 6 (approx 3.5mm (0.14in) in diameter)
- Wall plugs if required
- Suitable drills and screwdriver

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8 N User Configuration.

2.4 nano3G S16 AP Site Requirements

In addition to the site requirements for all APs, each S16 AP will require:

- Power supplied in one of the following ways, according to the accessory unit(s) supplied with the S16 AP:
  - From the mains adaptor unit, which requires a suitable mains power supply point near the AP that is within reach of the adaptor's cabling

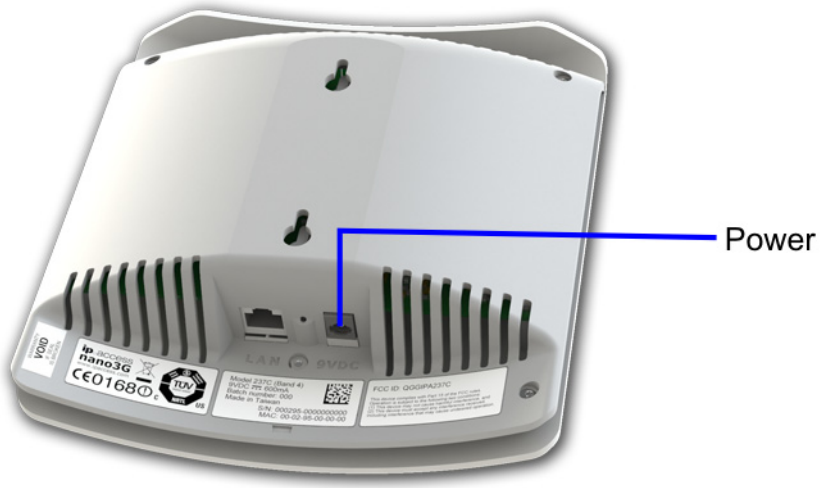
  or

  - From the supplied POE splitter, which requires a Power over Ethernet connection to the splitter
- A site for the AP:
  - Wall mount location

  or

  - Stable surface for free standing installation

2.4.1 nano3G S8 AP Power Requirements



Maximum expected power consumption:

- 8 Watts (Rated 9VDC 890mA)

The nano3G S8 AP supports the following power and Ethernet cabling options:

- Direct power from the power adapter
- Power over Ethernet from the POE injector, via the POE splitter
- Power over Ethernet from a POE switch, via the POE splitter

A POE cable must not be inserted directly into the AP.

The power adapter, as well as the POE inserter and splitter supplied by ip.access comply with LPS requirements in accordance with IEC/EN 60950-1.

Power Adapter

A suitable mains power supply point into which the power adapter for the AP can be plugged.

Only use the power adapter available from ip.access to power the AP:

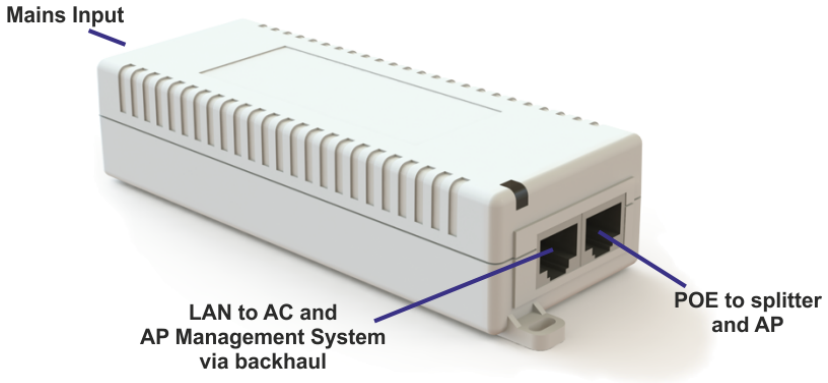
ip.access part number	PSA15R-090PV-R
Input	100-240V ~ 50/60Hz 0.5A
Output	+9VDC 1.67A

Power over Ethernet

POE requires the use of a power inserter and a splitter. The power inserter is positioned close to the backhaul network connection and mains supply, while the splitter is positioned close to the AP.

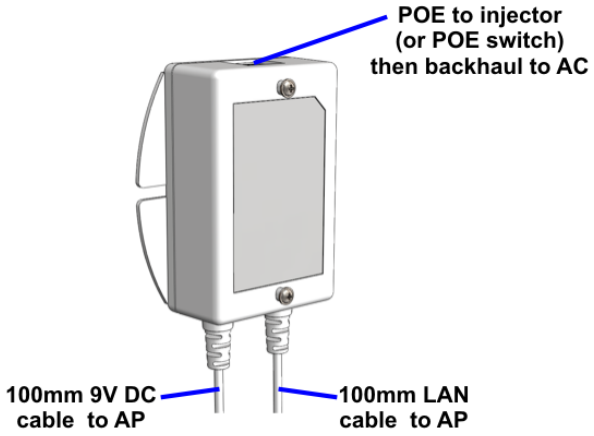
This is the POE inserter supplied by ip.access:

ip.access part number	236
Input	100/240V ~ 60/50Hz 0.5A
Output	48VDC 0.35A



Only use the POE splitter available from ip.access:

ip.access part number	222A
Input	48VDC 0.35A
Output	9VDC 1.33A



2.4.2 nano3G S16 AP Physical Requirements

A nano3G S16 AP may be installed in one of the following ways (see section 6.2.4):

- Free-standing on a flat stable surface.
- Attached to a wall or partition using two screws that engage in keyhole slots in the rear surface of the AP.
- Attached to a POE splitter using the two screws that engage in keyhole slots in the rear surface of the AP. The POE splitter in turn attaches to a wall or partition using two screws.

The unit **must** be vertical to ensure that air can circulate freely around it.

It is recommended to install the AP with its front surface facing the area requiring cellular coverage, unobstructed by walls or partitions that may cause significant RF attenuation.

Dimensions and weight	Height	176mm (without stand) 193mm (with stand)
	Width	170mm
	Depth	51mm
	Approximate Weight	0.42 kg (AP only)
Environmental	Cooling	Vents on the back at top and bottom
	Operating Temperature	0°C to 40°C
	Operating Humidity	10 to 70% non-condensing

2.4.3 nano3G S16 AP IP Bandwidth Requirements

At maximum capacity, a nano3G S16 AP will require:

- Downlink: 17Mbps
- Uplink: 1.9Mbps

This will deliver up to 16 voice calls and HSDPA services up to 14.4 Mbps.

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8 N User Configuration.

2.4.4 nano3G S16 AP Sundry Installation Equipment

To mount the POE splitter or the nano3G S16 AP onto the wall:

- 2 self tapping pan head screws, size No. 6 (approx 3.5mm (0.14in) in diameter)
- Wall plugs if required
- Suitable drills and screwdriver

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8 N User Configuration.

2.5 nano3G E8 AP and nano3G E16 AP Site Requirements

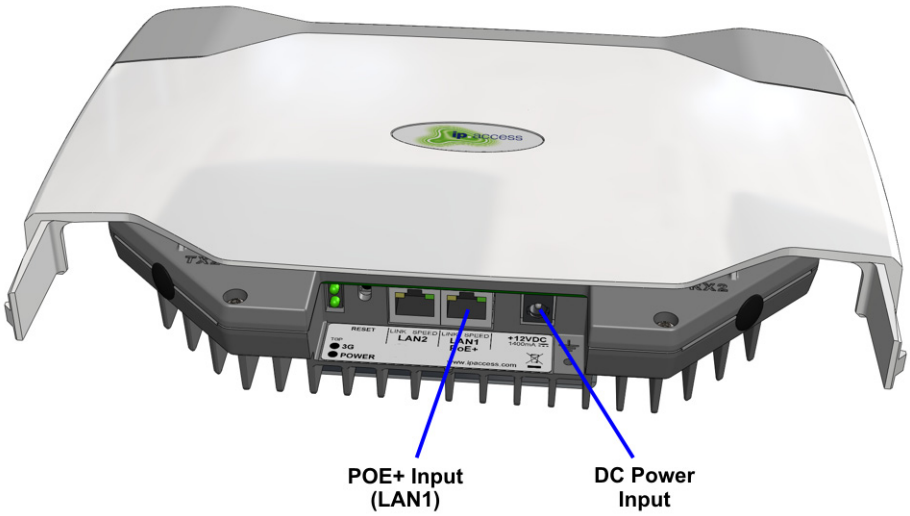
In addition to the site requirements for all APs, each E8 AP and E16 AP will require:

- A site for wall mounting
- Power supplied in one of the following ways:
  - From the supplied POE injector, which requires a suitable mains power supply point near the injector

  or

  - From a mains adaptor unit, supplied separately, which requires a suitable mains power supply point near the AP that is within reach of the adaptor's cabling

2.5.1 nano3G E8 AP and E16 AP Power Requirements



Maximum expected power consumption:

- 20 Watts (Rated +12V on the DC input or -48V DC on the POE+ input)

The nano3G E8 AP and E16 AP support the following power options:

- Power over Ethernet from a IEEE 802.3at compliant POE+ power source equipment - a suitable POE+ inserter is supplied with the AP
- Direct power from a suitable DC source (+12V, 2.5A rated centre positive 2.1mm jack) - a suitable mains adaptor is available separately

These power options are mutually exclusive. When POE+ is used, a DC power adapter must not be plugged in to the AP and vice versa.

The nano3G E8 AP and E16 AP can be used with any IEEE 802.3at compliant POE+ power source.

Note: The Ethernet cable carrying POE+ must be plugged into the LAN 1 port. The LAN 2 port, next to LAN 1, is not used and does not support POE.

POE+ Injector

The POE+ injector unit is supplied as standard with each nano3G E8 AP and E16 AP. The POE+ injector has two Ethernet connections, one for connection to the main LAN, the other for connection to the AP. The POE+ injector can be located anywhere on the cable run between the network switch and the AP, including locally at the AP or remotely at the network switch.

The POE+ injector is a pass-through connector for the LAN. Its function is to add POE+ to provide power to the AP. Therefore, the maximum cable run from the network switch to the AP is 100m, regardless of the placement of the POE+ injector.

The POE+ injector supplied by ip.access complies with LPS requirements in accordance with IEC/EN 60950-1.

2.5.2 nano3G E8 AP and E16 AP Physical Requirements

A nano3G E8 AP or E16 AP is installed by attaching its mounting plate to a wall or partition with screws, then sliding the rear surface of the AP onto the mounting plate (see section 6.4.6).

Pay attention to ensure that air can circulate freely around the unit. The unit must be vertical.

It is recommended to install the AP with its front surface facing the area requiring cellular coverage, unobstructed by walls or partitions that may cause significant RF attenuation.

Dimensions and weight	Height	211mm
	Width	274mm
	Depth	58.6mm
	Approximate Weight	1.75 kg
Environmental	Cooling	Vents on the back at top and bottom
	Operating Temperature	0°C to +45°C
	Operating Humidity	10 to 70% non-condensing

2.5.3 nano3G E8 AP IP Bandwidth Requirements

At maximum capacity and with IPsec in use, a nano3G E8 AP will require:

- Downlink: 17Mbps
- Uplink: 1.8Mbps

This will deliver up to 8 voice calls and HSDPA services up to 14.4 Mbps.

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8.

2.5.4 nano3G E16 AP IP Bandwidth Requirements

At maximum capacity and with IPsec in use, a nano3G E16 AP will require:

- Downlink: 17Mbps
- Uplink: 1.9Mbps

This will deliver up to 16 voice calls and HSDPA services up to 14.4 Mbps.

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8.

2.5.5 nano3G E8 AP and E16 AP Installation Tool Requirements

To mount the bracket onto the wall:

- 6 pan head screws, size No. 6 (approx 3.5mm (0.14in) in diameter) – 4 for the AP bracket, 2 for the POE+ adapter

  Note: No screws are supplied to mount the AP or the POE+ unit.
- Wall plugs if required.
- Suitable drills and screwdriver.

Note: If the available bandwidth on site does not meet the requirements see the Troubleshooting section 8 N User Configuration.

3 Pre-Provisioning a nano3G AP

The nano3G 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 relevant BSMIS APs PerAC object.

3.1 Pre-Provisioning Parameters

For the pre-provisioning parameters refer to section 2.2.3.

3.2 Create a Site for a New AP

Use the Create Site Wizard in the NOS Client to create a site 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.

3.2.1 Start the Create Site Wizard

1) Login to the NOS Client with a user ID that has Full Access rights to the required BSMIS APs per AC object.

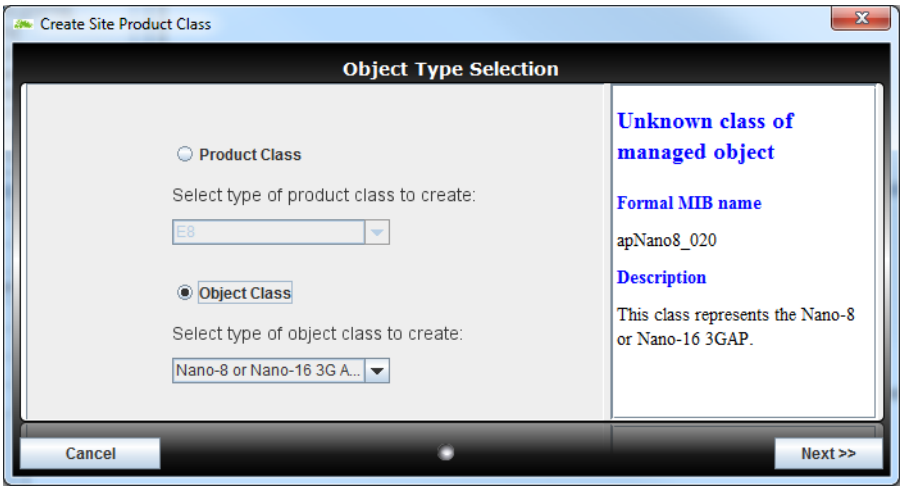
2) Find the required BSMIS APs Per AC object.

   Hence, drill down to the AP like this:

   Root > APs > BSMIS APs Per AC

   Note: The display name of the BSMIS APs Per AC object may have been changed to make the serving AC easier to identify.

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



4) Select the Object Class radio button and in the drop-down list on the left and select one of the following: This is applicable to E8 APs, E16 APs and S8 APs.

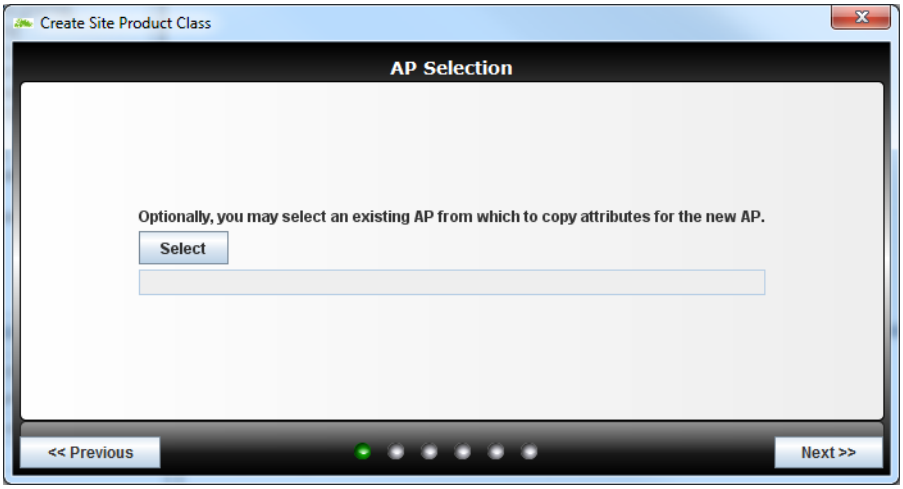
- **Nano-8 or Nano-16 3G AP (SR2.0 -). This applies to N3G_2.83 AP software.**
- **Nano 3G AP (SR2.4 -). This applies to N3G_2.85 or later AP software.**

Note: Do not select Nano-4 3G AP (SR2.0 -) as this is not supported in N3G_2.92.

Note: If they are present, do not choose either of the choices for (SR1.2 - PRE-SR2.0). These are only used for APs running software from a release prior to N3G_2.92. These choices must be present for backwards compatibility and they enable AP upgrades from previous releases.

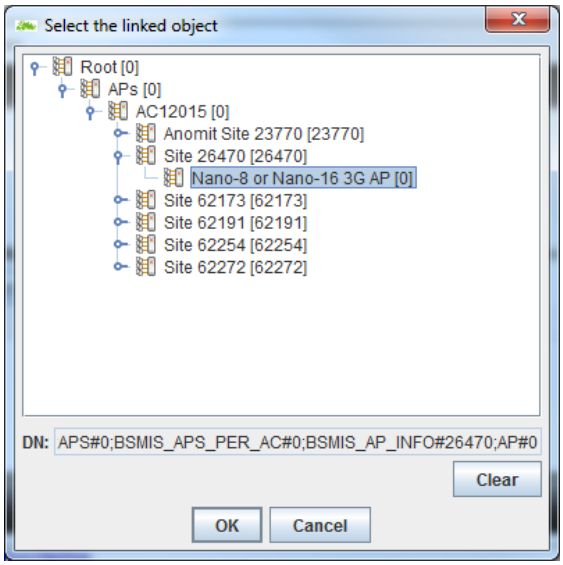
3.2.2 Optional - Use an Existing AP Configuration

5) Click **Next** and the AP Selection page of the wizard will appear:



Optionally use this page to copy the configuration of an existing AP.

6) To copy the configuration from an existing AP, click the **Select** button. The Select linked object browser will appear, initially showing the Root object in the NOS object hierarchy. Drill down to find the required AP. For example:

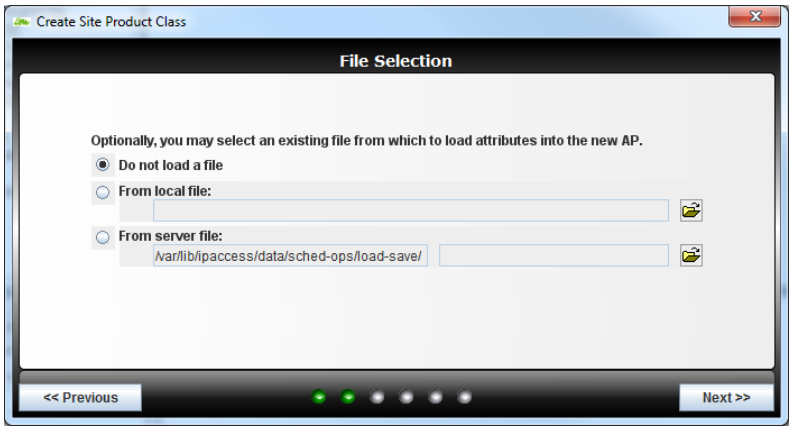


The DN box will show the Distinguished Name for the selected AP. This uniquely identifies the AP object within the object hierarchy on this NOS. The AP object must be the same type of AP object as has been selected for the new site.

7) Click **OK** and the DN will be shown on the AP Selection page of the wizard.

3.2.3 Optional - File Selection

8) Click **Next** and the File Selection page of the wizard will appear:



Optionally use this page to load a configuration file for the AP. The three options for file sources are:

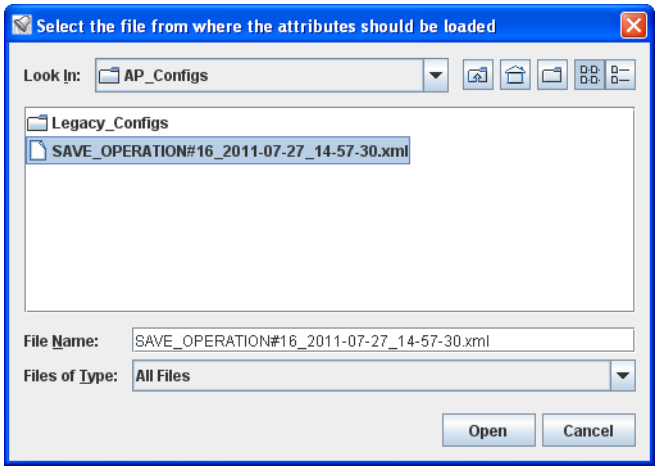
- Do not load a file - no configuration file will be loaded - if preferred, it is possible to load a configuration file later using the Load Attributes Wizard
- From local file - a configuration file stored on the local computer running the NOS Client
- From server file - a configuration file saved on the NOS server by saving the attributes from an AP

Although files can be selected for all sources, only the item for the selected radio button will be used on moving to the next page of the wizard. The AP type in the chosen configuration file must be the same type of AP object as has been selected for the new site.

For information on preparing an configuration file for an AP, see section 4.

Select a Local File

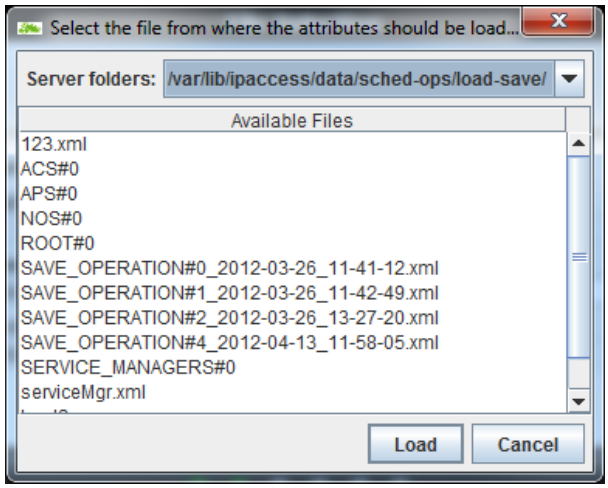
9) Click the radio button for **From local file**, then click the browse button on the right. The file browser will appear. Browse to the location of the required configuration file and select it. For example:



10) Click **Open** and the file name will be shown in the box for Local file.

Select a File Saved on the NOS Server

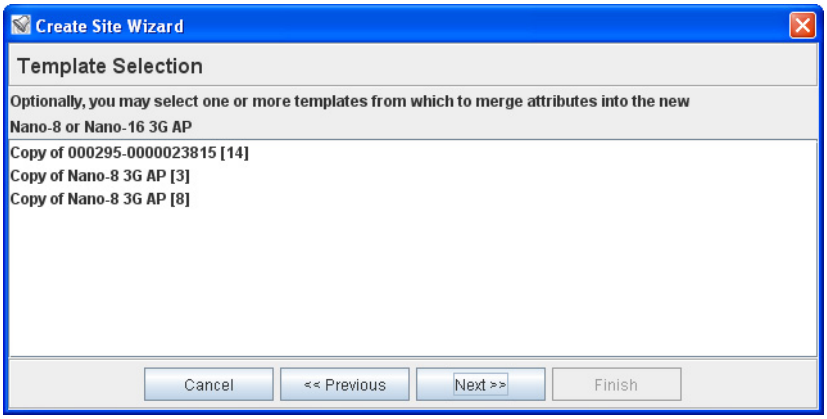
11) Click the radio button for **From server file**, then click the browse button on the right. A list of configuration files saved on the NOS server will appear. For example:



12) Click the required configuration file in the list, then click **Load**. The list will close and the file name will be shown in the box for Server file.

3.2.4 Optional - Select an AP Template

13) If any templates of the correct object type are available, the Template Selection page will appear:



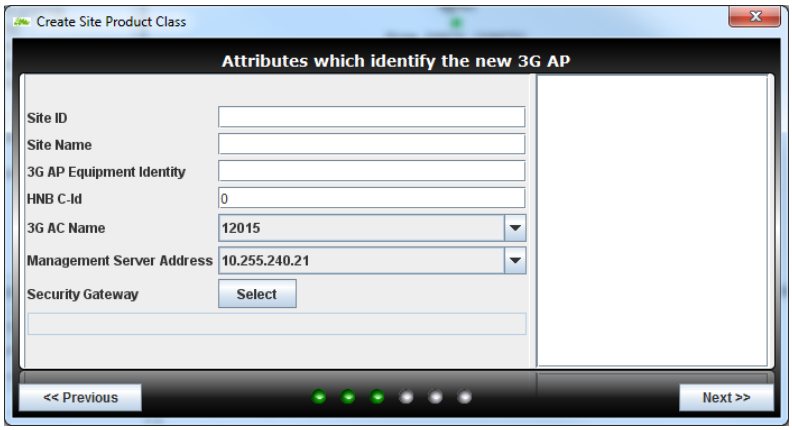
Optionally use this page to load a template for the AP. Typically the template can contain a reference configuration for the AP according to the AP's intended location and/or usage.

For information on working with templates, see [OPM_415].

14) To use a template, click the required template in the list, then click **Next**. If a template is not required for this AP, click **Next** without selecting anything in the list.

3.2.5 Enter AP Identification Details

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



Notice that the 3G AC Name, Management Server Address and Security Gateway are set automatically according to the BSMIS object selected for invoking the wizard. The 3G AC Name and Management Server Address may not be changed.

16) Click in the **Site ID** box and type a numeric ID. This must be unique within the parent AC object. 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 or the HNB C-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.

17) 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.

18) Click in the **3G 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.

19) Click in the **HNB C-Id** box and type a numeric ID. This must also be unique within the parent BSMIS object, and hence is unique within the HNB-GW, that is, the AC. This could be the same as the Site ID, depending on the network policy in place.

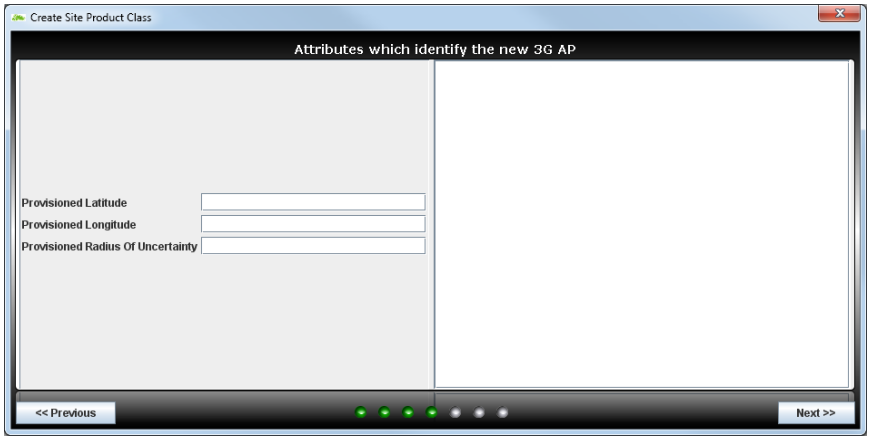
20) If the default Security Gateway is not correct for this AP, click the **Select** button and choose a different Security Gateway from the available gateways defined under Root > NOS > Security Gateways.

21) 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.

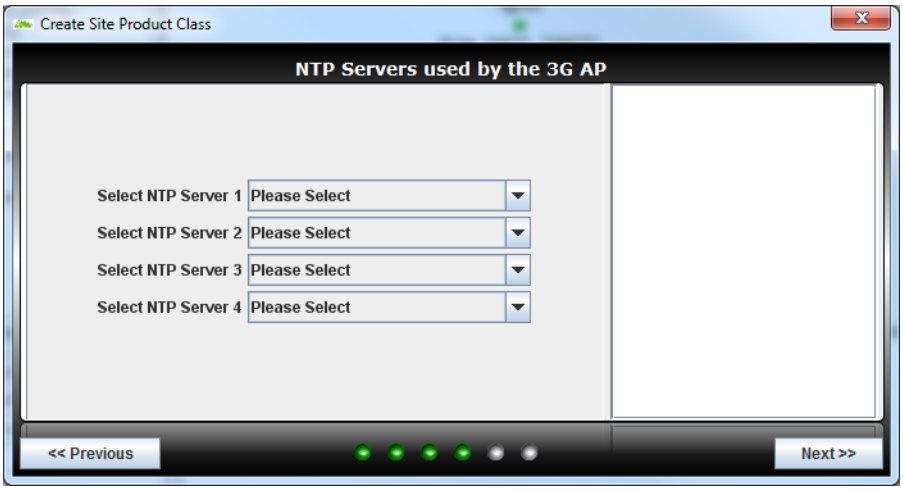
3.2.6 Select AP Location

1) To provide the location of the configured AP, enter the Latitude, Longitude and Radius of Uncertainty to the appropriate fields (optional), this will verify the AP, then click Next.



3.2.7 Select NTP Servers

2) The page for selecting NTP servers will appear:



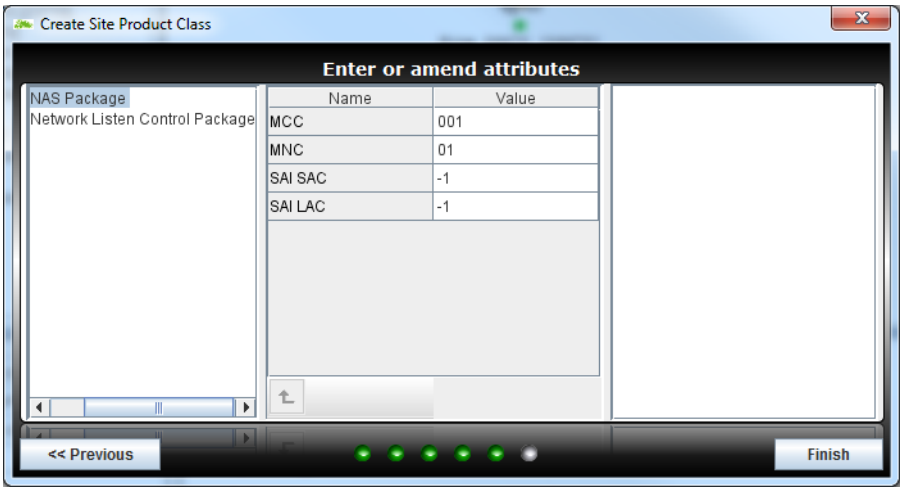
If an existing AP, template or file was chosen, the NTP servers may have been automatically selected from one of these sources. Any changes on this page of the wizard will override settings from an existing AP, template or file.

3) Click the drop-down lists to choose up to four NTP servers for the AP. The available NTP servers are defined under Root > NOS > NTP Servers. At least one NTP server must be selected.

4) Click **Next**.

3.2.8 Modify NAS and Network Listen Settings

5) The page for NAS and Network Listen details will appear:



The initial values on this page of the wizard are selected as follows:

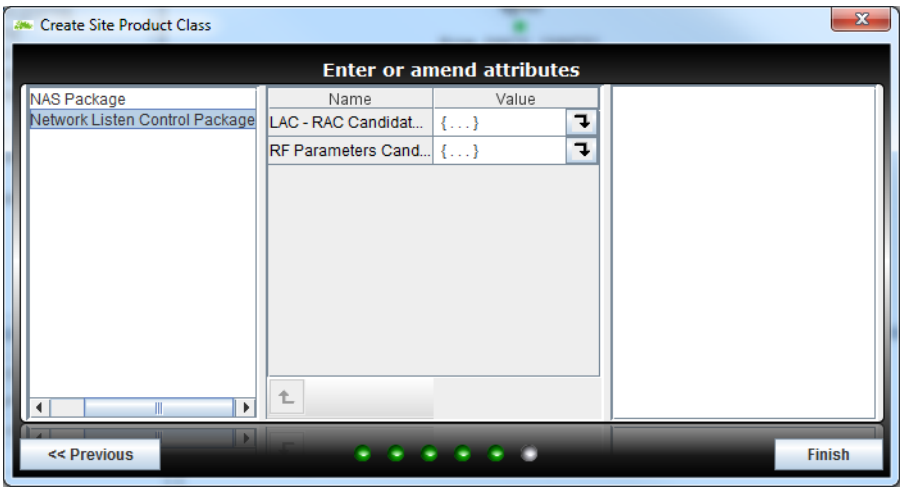
- MCC and MNC: These are copied from the target AC. That is, the AC associated with the parent AC Detail object. The RNC-Id is also copied, but this is not shown in the wizard.

- SAI SAC and SAI LAC: If an existing AP, template or file was chosen, the these values may have been automatically selected from one of these sources.
- LAC RAC Candidate List and RF Parameters Candidate List: These are under the Network Listen Control Package. If an existing AP, template or file was chosen, the these values may have been automatically selected from one of these sources.

In all cases, any changes on this page of the wizard will override any automatically selected settings.

6) If required, change the NAS entries. This is only necessary if the correct values have not been selected automatically.

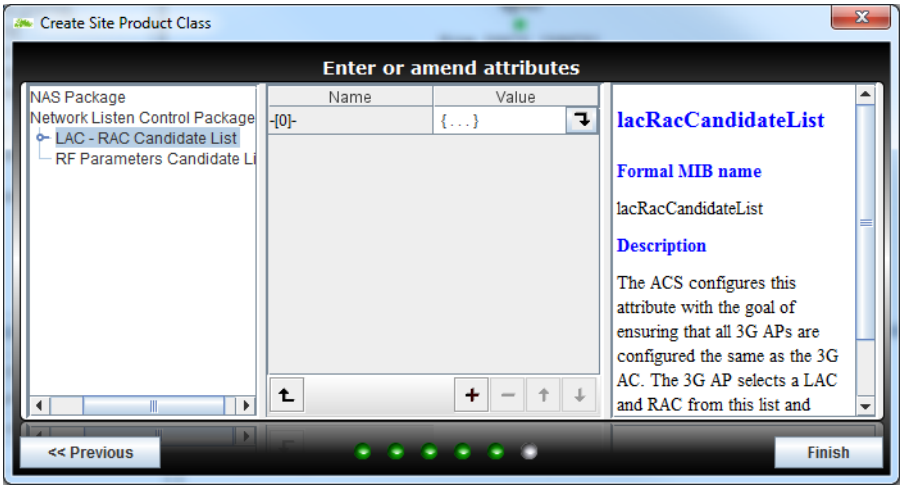
7) Click the **Network Listen Control Package**:



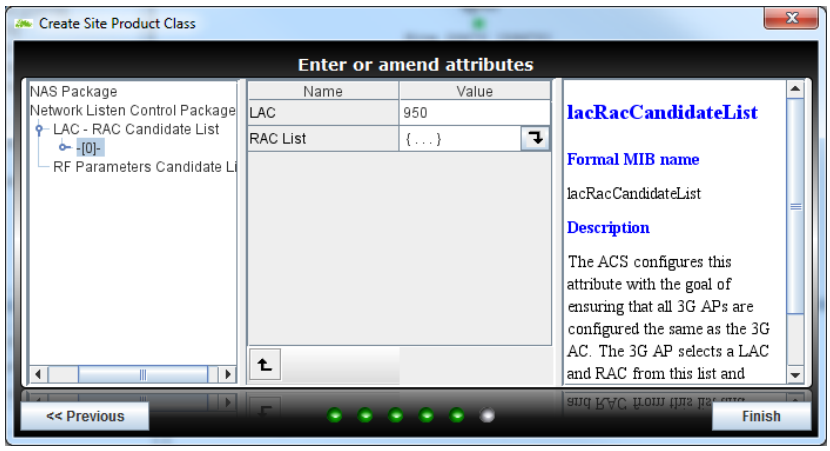
The number of entries within the lists in Network Listen Control Package will depend on how the AP is configured:

- Static configuration: If an AP will have a planned static configuration, enter only one set of values for each list. That is, one LAC-RAC combination and one set of RF Parameters. This is typically the scenario for enterprise deployments where the parameters have been determined by network planning.
- Dynamic configuration: If an AP will use Network Listen results to automatically select its parameter settings, in an attempt to choose optimal settings for its detected RF environment, enter multiple sets of values for each list. That is, multiple LAC-RAC combinations and multiple sets of RF Parameters. This is typically the scenario for domestic plug-and-play or SOHO deployments. Also, in this scenario, it is expected that an existing AP, template or file will have been selected which has pre-configured lists. If this is not the case, it may be more efficient to enter a single set of parameters in the wizard, and then either configure the AP object directly or load pre-configured lists against the AP object.

8) If the LAC/RAC entries are invalid, as in the example, drill down into the **LAC - RAC Candidate List** to find the invalid entry:

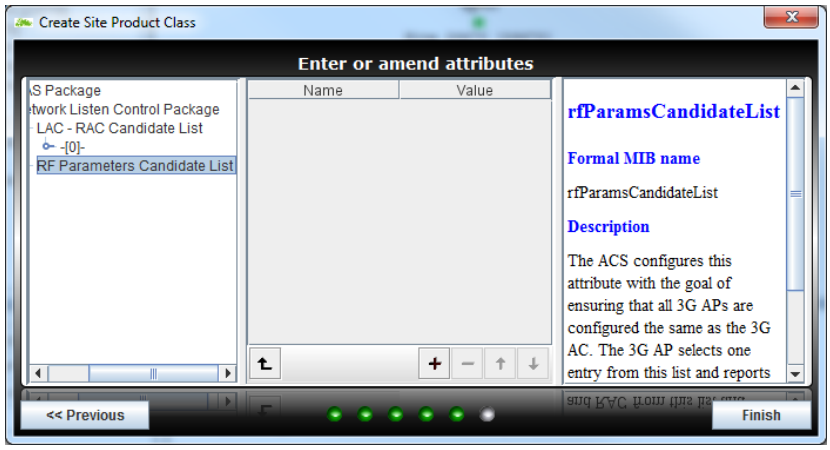


9) Enter a valid LAC/RAC combination that this AP can use, according to network planning for this AP. For example:

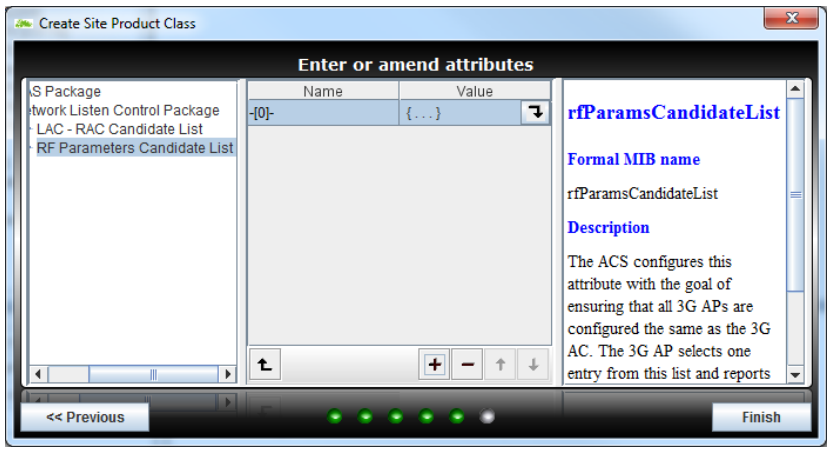


Multiple RACs can be configured for each LAC. At least one LAC/RAC combination must be provided.

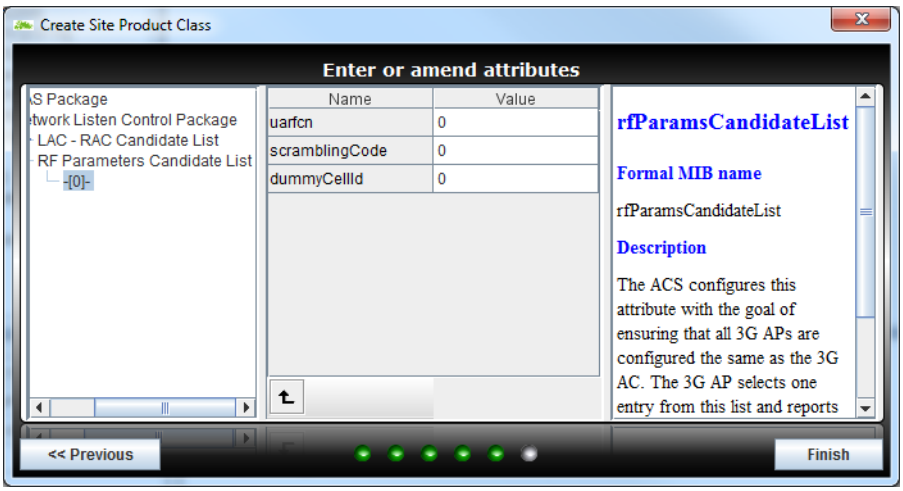
10) Select the RF Parameters Candidate List.



11) If the list is empty, click the + button to add a new entry to the list. For example:



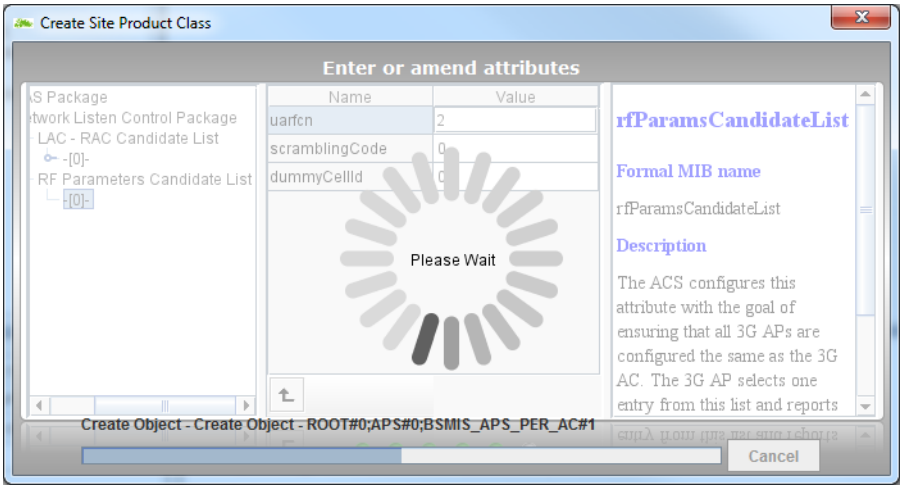
12) Drill down into the list entry. For a new list item, all the values will be zero, as in this example:



13) Enter or modify the **uarfcn**, **scramblingCode** and **dummyCellId** values for this AP.

14) Click **Finish**.

Progress will be displayed while the objects are created:



The site and the AP object will be added under the BSMIS APs Per AC object and can now be selected for further actions.

3.3 Apply an Attribute Configuration to the AP

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

- No AP configuration file or template was used as the basis for the AP's initial configuration
- There is a requirement to load multiple configuration files and/or templates, in addition to any file and/or template already loaded in the Create Site Wizard

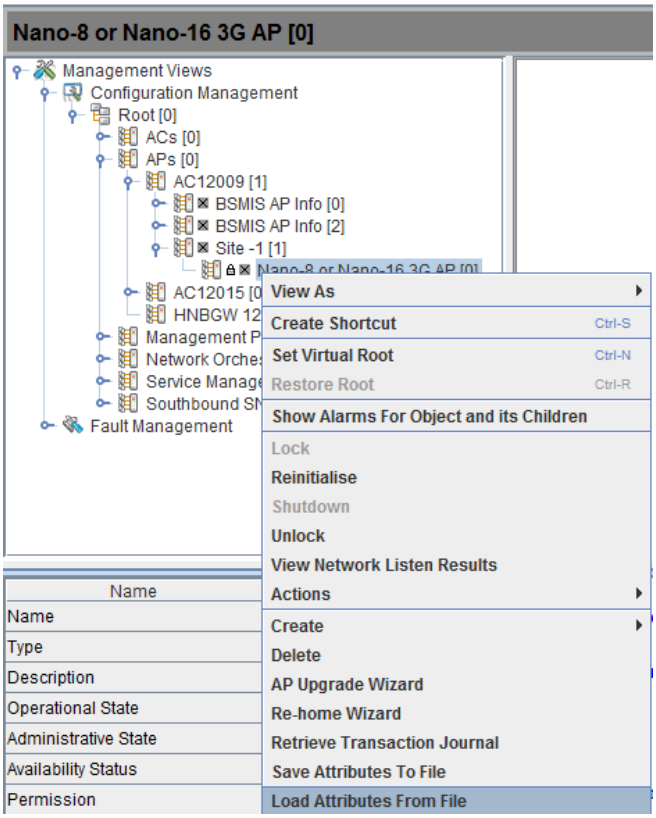
3.3.1 Load a Configuration File for the AP

For information on preparing a configuration file for an AP, see section 4.

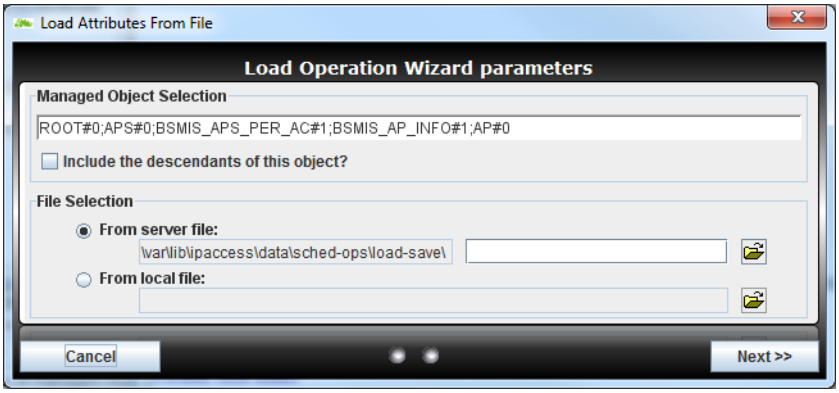
1) Ensure the configuration file is available on the NOS Server or the computer running the NOS Client.

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

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



4) The Load Attributes From File Wizard shows the chosen AP object:



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

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

7) 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**.

8) By default the operation is scheduled for Now, so click **Finish** to load and apply the configuration settings.

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

3.3.2 Apply an AP Template to the AP

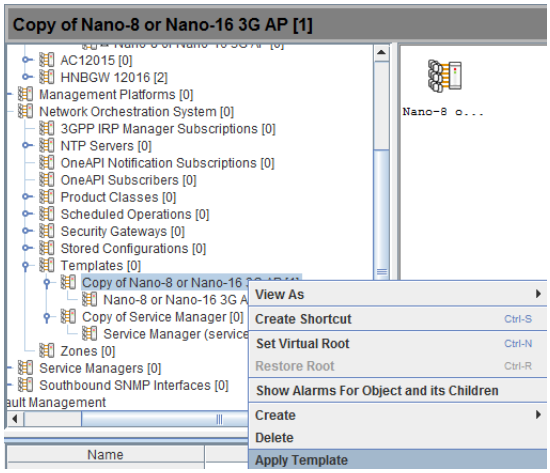
For information on working with templates, see [OPM_415].

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

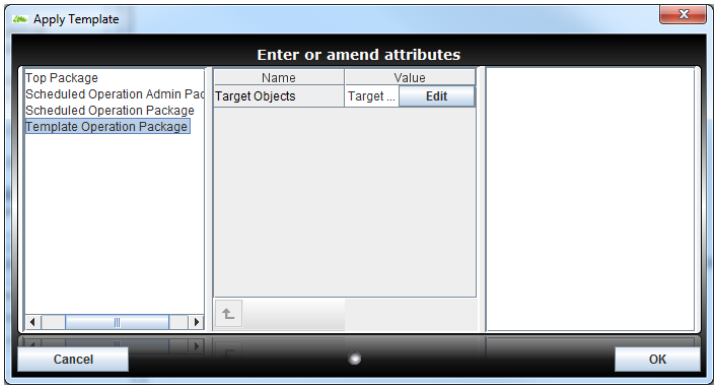
2) Find the required AP template under NOS > Templates.

   The object type must match. That is, use an apNano8_020 template for E8 APs, E16 APs and S8 APs. Choosing a template with a different object type will have no effect on the target AP.

3) Right-click Templates, select **Copy of Service Manager and then select Apply Template**.



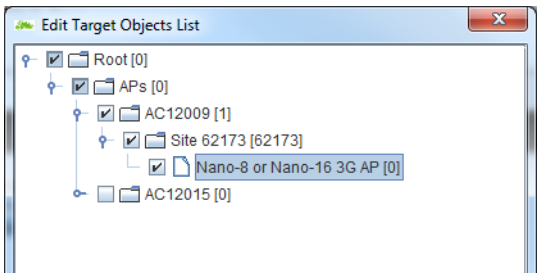
4) Select the **Template Operation Package**.



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

6) Browse to the correct AP object under **APs > AC > Site > AP**.

7) Click the check box next to the AP object. All of the AP's ancestor objects are also selected.



8) Click **OK** to set the target object and return to the Apply Template wizard.

9) Click **OK**. The attribute settings in the template will be applied to the AP object.

10) Repeat as needed, if there are multiple templates to apply.

4 Configuration File Preparation

The attribute values for configuring a nano3G AP can be stored in an XML file, and then loaded via the NOS Client to provision the AP. This configuration file of attributes can be loaded when creating the site for the AP or at any time after that once the AP object exists.

This section describes how to prepare one or more configuration files of attributes for provisioning nano3G APs. This can be done in combination with the Create Site Wizard and configuration adjustments from the NOS Client, according to whichever method is best suited for given configuration tasks.

4.1 Overview of Configuration Files

A configuration file is an XML file containing an AP object that has named attributes and the value for each attribute. Each attribute definition is of the form:

```
<cd:attribute registeredAs="NUM" name="NAME">VALUE</cd:attribute>
```

Where:

- NUM is the Registered As number, as specified in the MIB for this attribute
- NAME is the attribute name, as specified in the MIB for this attribute
- VALUE is the attribute value, which must conform to the attribute's definition in the MIB

The attribute types and values they may take are formally described in [REF_110].

Note: In the configuration file, the values of compound attributes, such as RAB types, are defined within brackets (). In the NOS Client, the compound types are the complex attributes that have multiple levels within the Navigation and Properties panes. To work with compound attributes in a configuration file, it is recommended to use the structure in the OMC-R Client as a guide to editing the compound attribute.

Note: In [REF_110], there is a distinction between expert and non-expert attributes. As a general rule, it is recommended to leave expert attributes at their default values.

The configuration file must contain the correct distinguished name (DN) for the target AP. The NOS Client will not load a file if the DN does not match. In the configuration file, the DN is the localDn field near the beginning of the file. To change which AP this file applies to, edit the last part of the DN which defines the connection instance (the site) and AP instance.

Although a configuration file can be created from scratch, it is more practical to save a file from within the NOS Client from an object of the same type and then edit the file for the target object. The resulting configuration file can then be imported against the target object, which in this case will be an AP.

Configuration files must be imported one at a time, but there is no restriction on the number of configuration files that can be imported to configure any given object. This means it is possible to create a generic configuration file, which contains attribute values common to all APs of the same type. Typically, this can be started by exporting the configuration from an AP that has already been fully configured, and then edited to remove non-generic attributes. Once the generic file has been created, it must be saved for each AP, with the correct DN.

Optionally also create a file for each individual AP with additional settings particular to each AP. However, if the majority of required settings are in the generic file, it may be easier to simply load the generic file then use the NOS Client for fine tuning the configuration of an individual AP.

Note: After initial provisioning from a configuration file the NOS Client can be used to set attributes or a configuration file can be edited to set more attributes, for example when using configuration information from a radio planning system. To obtain a sample file with all the attributes that can be configured, export a configuration file as described in section 4.2 and inspect its content.

4.2 Create a Configuration File for nano3G APs

4.2.1 Save Attributes to File for One AP

A configuration file can be created from an existing AP. It is recommended to do this in preference to starting a file from scratch.

To start a configuration file by saving the configuration of an existing AP:

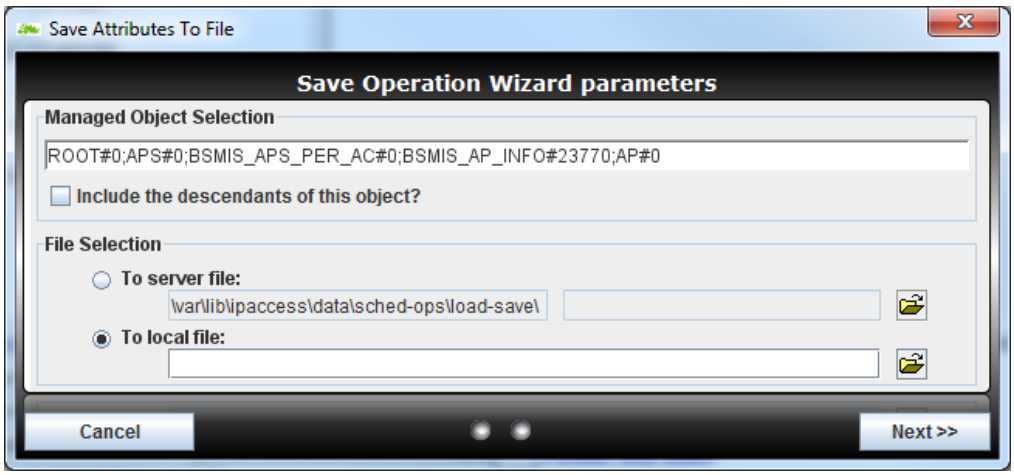
1) Login to the NOS Client with a user ID that has Full Access rights to the required AP.

2) Find the required AP within the APs area. Find the AC the AP is connected to (i.e. the BSMIS APs Per AC object) then locate the AP within its Site.

   Hence, drill down to the AP like this:

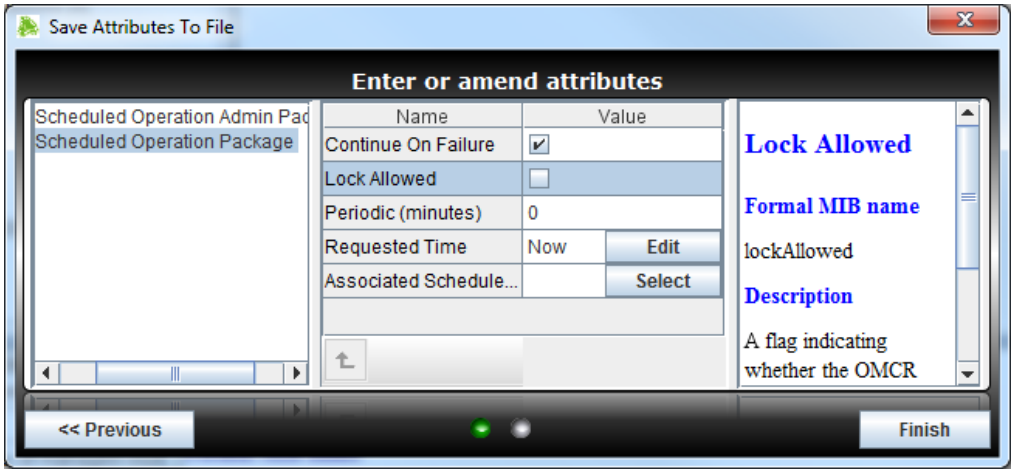
   Root > APs > BSMIS APs Per AC > Site > AP

3) Right-click the relevant AP object and select **Save Attributes to File**. The Save Attributes Wizard will appear.



4) Select To local file and use the browse button to choose a suitable directory on the client computer for saving the AP configuration file (the browser dialogue can also create new directories).

5) When a suitable directory has been selected or created, click Next. The Enter or amend attributes screen will appear:



6) Select the **Scheduled Operation Package** and uncheck Lock Allowed as this can cause service interruption. Click Finish. A confirmation message stating file copied successfully will appear, click OK.

7) One configuration file will be saved in the directory for each AP object.

4.2.2 Save Attributes to File for Multiple APs

Use this function to make a backup of the configuration attributes for all APs within the AC BSMIS of one AC. One configuration file will be saved for all AP objects below the selected AC BSMIS object. The file name is generated automatically with the following format:.

Bulk backup is local only (i.e. on the Client computer). It is not possible to bulk backup the AP configurations on the SDP Server.

The whole directory can be restored.

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

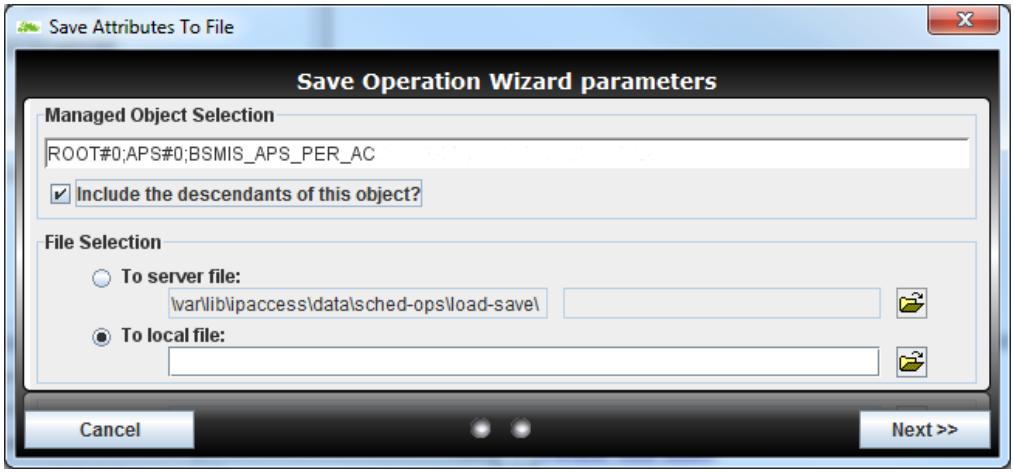
Note: For full information on using the NOS Client, see [OPM_415].

2) Find the required AP within the APs area. Find the AC the AP is connected to (i.e. the BSMIS APs Per AC object) then locate the APwithin its Site.

Hence, drill down to the AP like this:

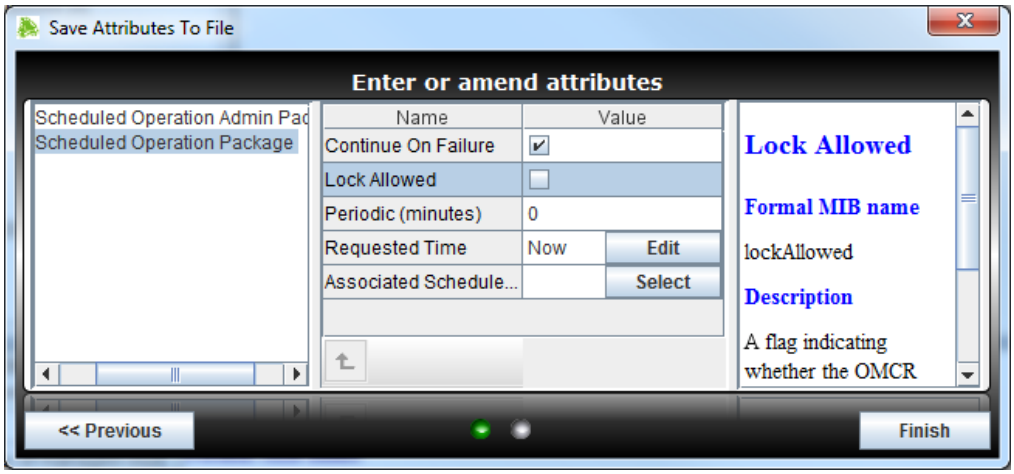
Root > APs > BSMIS APs Per AC

3) Right-click the relevant BSMIS object and select **Save Attributes to File**. The Save Attributes Wizard will appear:



4) Tick the check box to Include the descendants of this object. Select To local file and use the browse button to choose a suitable directory on the client computer for saving the AP configuration file (the browser dialogue can also create new directories).

5) When a suitable directory has been selected or created, click Next. The Enter or amend attributes screen will appear:



6) Select the **Scheduled Operation Package** and uncheck Lock Allowed as this can cause service interruption. Click Finish. A confirmation message stating file copied successfully will appear, click OK.

7) One configuration file will be saved in the directory for each AP object.

5 Commission a nano3G AP

This procedure configures the nano3G AP with the settings it needs to establish a connection with its serving NOS Server. Once commissioning is complete, use the NOS Client for any remaining configuration and to bring the AP into service.

An AP can be commissioned either in advance of the site visit via a commissioning computer or on site via a commissioning laptop. This procedure is identical in both cases. To allow for both of these scenarios, the term *commissioning terminal* is used to refer to any laptop or computer used for commissioning.

Note: For residential deployments, commissioning should have already been done at the factory or by the supplier. If in doubt, contact the supplier for confirmation. Where an AP is already commissioned, ignore all of section 5.

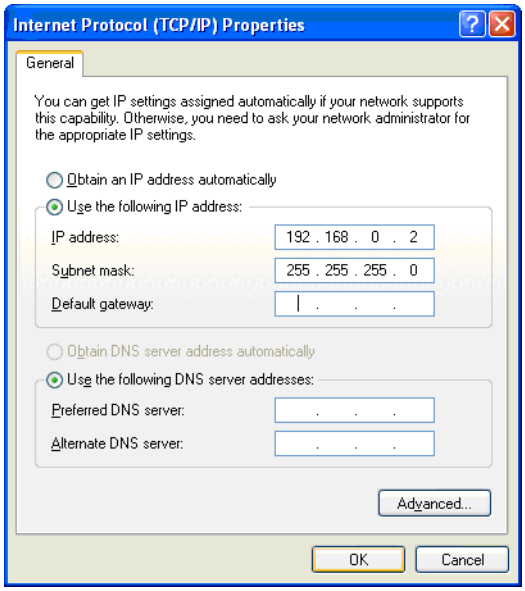
5.1 Configure a Commissioning Terminal to Connect to the AP

1) Open the Windows Control Panel on the terminal.

2) Go to **Network Connections**.

3) Right-click the relevant **Local Area Connection** and select Properties.

4) In the list of items on the General tab, select **Internet Protocol (TCP/IP)** and then click **Properties**. The following dialogue appears:



5) If it is not possible to leave this network connection permanently configured for AP commissioning, make a note of the current settings.

6) Click the **Use the following IP address** radio button.

7) Set the IP Address to **192.168.0.2**.

8) Set the Subnet Mask to **255.255.255.0**.

9) There is no default gateway, so ensure the default gateway address is cleared.

10) Click **OK** to close and save the changes in each of the two dialogues. Also close the Control Panel.

5.2 Start Up the AP

5.2.1 Start up a nano3G S8 AP

1) To power up an S8 AP or S16 AP, either.

   - Use the power supply provided with the AP

   or

   - Connect a POE source to the splitter unit, then connect the short power cable from the POE Splitter unit to the DC input on the AP

   Note: The AP may have been provided with only one of these options.

2) Connect the commissioning terminal directly to the AP with an Ethernet cable.

5.2.2 Start up a nano3G E8 AP or E16 AP

1) To power up a nano3G E8 AP or E16 AP, typically do one of the following:

   - Connect a cable to carry POE+ from the injector to the LAN1 port on the AP, then plug the POE+ injector into the mains

   or

   - Connect the optional power supply for the AP to the AP's 12V DC input

2) To establish an Ethernet connection between an E8 AP or E16 AP and the commissioning terminal, do one of the following according to how the AP has been powered up:

   - If using POE+ to power the AP, connect the Ethernet cable from the commissioning terminal to the LAN input on the POE+ injector unit

   or

   - If not using POE+, connect the Ethernet cable from the commissioning terminal directly to the LAN1 port on the AP

5.3 Access the Commissioning Web Page for the AP

The commissioning web page is only accessible after performing a factory reset. The login prompt for this web page is also only available for 60 seconds, after which the AP will attempt to boot normally.

1) Start a web browser on the commissioning terminal.

2) In the address bar, type in the pre-defined static IP address and port number for the web server, but do not press <Enter> yet:

   ```
   http://192.168.0.1:8089
   ```

3) Perform a factory reset on the AP:

   - Press and hold the reset button. Initially, the service LED blinks rapidly.
   - When the service LED changes from blinking rapidly to blinking slowly, release the reset button.
   - The LED continues to flash slowly until the factory reset completes, at which point the LED is extinguished and the AP reboots.

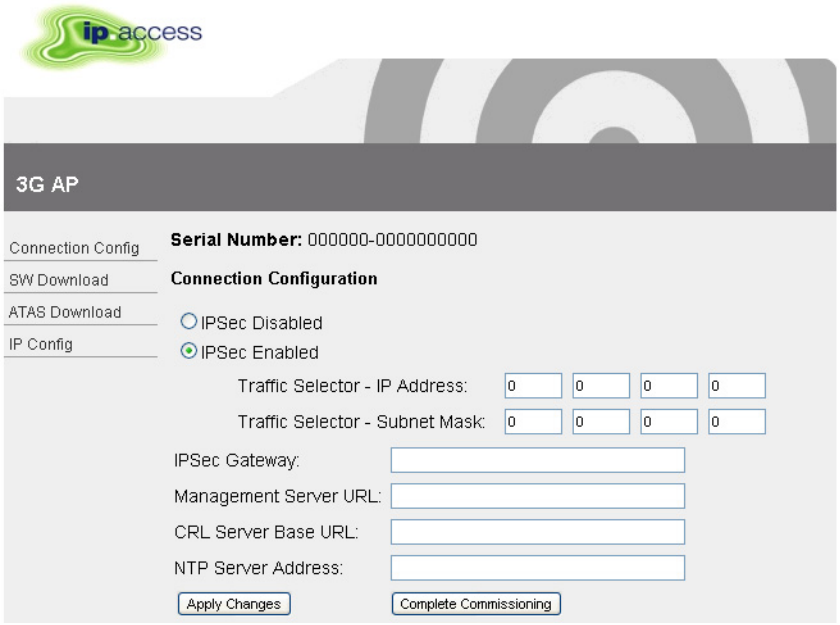
   Note: See section 8.3 for more information about factory reset.

4) Wait a few seconds, then press **<Enter>** in the web browser. A login screen should appear. If the login screen does not appear immediately, refresh the browser screen until it appears.

   ALERT: When the AP starts up, the login prompt for the commissioning web page is only available for 60 seconds. If the login prompt is missed, press the reset button to repeat the factory reset.

5) Enter the commissioning user name and the password (supplied separately for security reasons).

After entering the correct user name and password, the Connection Config page appears:



5.4 Download Activities

If it is necessary to download a software or ATAS package to the AP, this **must** be done before configuring the connection to the NOS Server. This is because the ATAS package in particular may be needed so that the AP can access the NOS Server through the security gateway. See section 2.2.11 for extra information about software and ATAS packages.

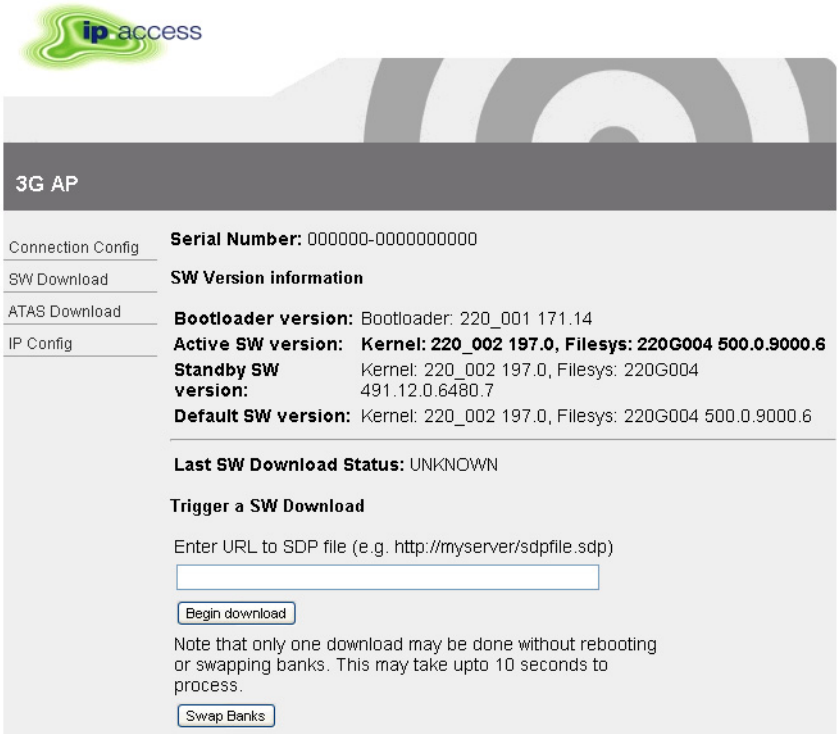
This can only be done if the commissioning terminal is running a web server that provides a path to any ip.access AP software download packages. That is, the required .sdp files must be present on the commissioning terminal.

Setting up a web server for this purpose on the commissioning terminal is outside the scope of this manual.

5.4.1 Optional - Software Download

Use the SW Download page to download a different version of AP software to the AP from the commissioning terminal to the standby memory bank. Then switch banks to the new software version, which restarts the AP.

6) Click the **SW Download** link on the left. The web page for downloading software will be shown. This also provides details about the current software installed on the AP.



7) In the text box, enter the URL for the SDP file stored on the commissioning terminal. For example, the URL of a software file for a nano3G E8 AP might be:

```
http://192.168.0.2/webservername/220H007_<ver>.sdp
```

Where <ver> is the actual build version of the required software package.

8) Click **Begin Download**.

9) Wait about a minute for the download to take place.

10) To restart the AP from the new software just downloaded, briefly press the reset button.

11) Once the AP has started, repeat the factory reset by holding down the reset button for at least 5 seconds. When the AP restarts this time, refresh the browser to access the login prompt and login again with the commissioning user name and password.

12) Click the **SW Download** link on the left.

13) Inspect the software version information to verify that the AP has booted from the downloaded software.

14) To ensure the standby bank also has the latest software version, repeat the software download, but do not restart the AP. It is not necessary to restart the AP once it is already running the updated software.

    This ensures the AP does not have old software on the standby bank. Hence, if the AP is commanded to switch banks, it will run up-to-date software.

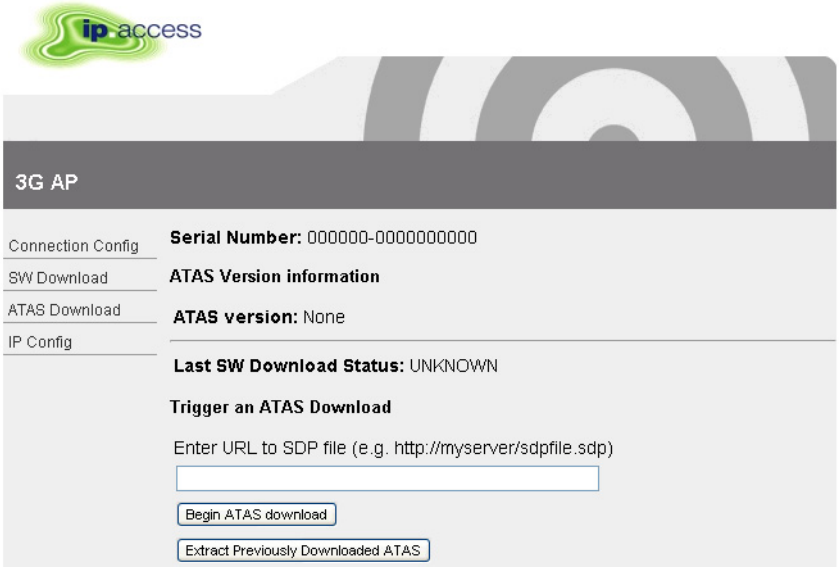
5.4.2 ATAS Check and Download

This is only required if the AP needs an additional ATAS package that is not already factory installed. For example, if the AP will use IPsec and the security gateway certificates are not supplied by ip.access Limited.

Use the ATAS Download page to check the current ATAS package. If necessary, also download a package of trust anchors that are appropriate for the AP's target network.

ALERT: The ATAS package on the AP must be correct according to the IPsec security gateway (SecGW) that will terminate the IPsec connection for the AP. If the ATAS package is incorrect, the AP will not connect to the SecGW and hence will be unable to enter service.

15) Click the **ATAS Download** link on the left. The web page for downloading an ATAS bundle will be shown. This will also show any current ATAS version information, if applicable.



16) Inspect the current **ATAS version** information. If the ATAS package is already correct then it is not necessary to re-download the ATAS package, so skip to section 5.5.

17) In the text box, enter the URL for the SDP file stored on the commissioning terminal, which contains the required ATAS bundle. For example:

```
http://192.168.0.2/webservername/atas_file.sdp
```

18) Click **Begin Download**.

19) Wait about a minute.

20) Click **Extract Previously Downloaded ATAS**.

21) Wait about a minute. If the ATAS version information is not refreshed, use the appropriate browser command to refresh the web page.

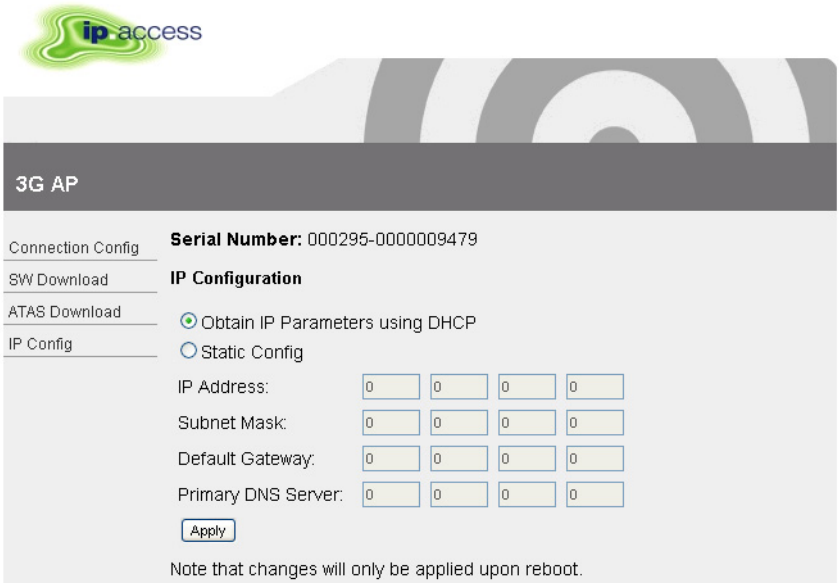
22) Inspect the **ATAS version** information on the ATAS Download page to verify it is now correct.

5.5 Configure the Connection to the NOS Server

5.5.1 Static IP Configuration

Obtaining an IP address with DHCP is recommended for the nano3G AP, and this is selected by default. Only execute this section if static IP configuration is needed. This must be done before completing the Connection Config page.

23) If static IP is required, click the **IP Config** link on the left. The IP Configuration page appears.



24) Click the **Static Config** radio button.

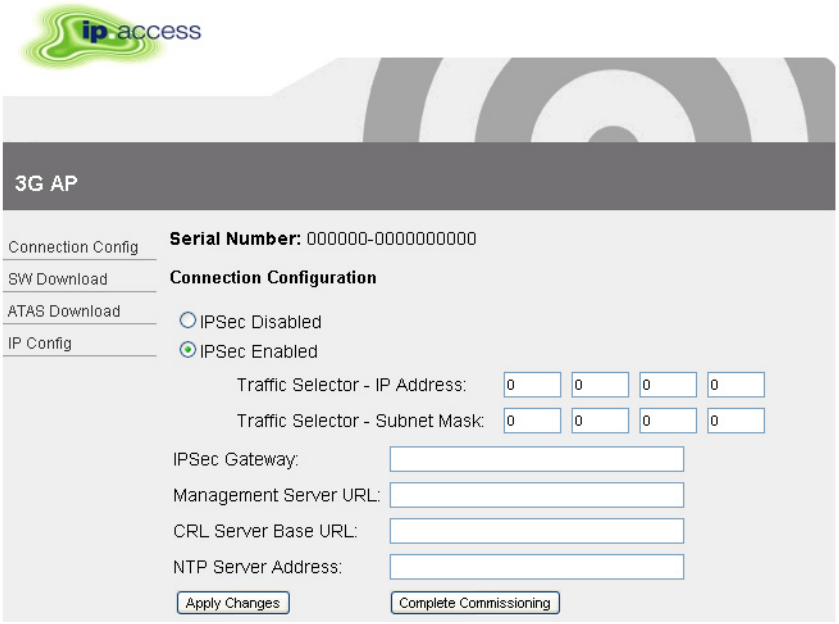
25) Edit the **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS Server** parameters as needed and then click **Apply**.

Note: At this point it may be useful to make a separate note of the parameter values entered in this screen. Alternatively, save a screenshot of the web page (information about how to take a screenshot is outside the scope of this manual).

26) Click the **Connection Config** link on the left.

5.5.2 Configure the NOS Server Connection

27) If a secure connection is required, select **IPSec Enabled**. Also enter the address for the **IPSec Gateway** and the **Traffic Selector** address and subnet mask.



28) Enter addresses for the NOS Server (Management Server URL), a suitable CRL server and the NTP server.

The settings applied on this page are retained permanently as the *default set* of these parameters, and can only be subsequently changed on this web page from a commissioning terminal.

Note: The NTP and CRL servers must be accessible to the AP on start up, before it has established an IPsec tunnel to the Security Gateway.

29) To save the configuration, click **Apply Changes**.

Note: At this point it may be useful to make a separate note of the parameter values entered in this screen. Alternatively, save a screenshot of the web page (information about how to take a screenshot is outside the scope of this manual).

5.5.3 Complete the AP Commissioning

30) Click the **Connection Config** link on the left, to ensure the correct page is showing.

31) To start the AP in normal operation mode, click **Complete Commissioning**.

32) Acknowledge the warning about changes in the IP configuration and click **OK**.

33) When the initial configuration is complete, power off the AP and disconnect it from the commissioning terminal.

At this point, the commissioning web page is no longer accessible. If there are configuration errors that prevent the AP connecting to its serving NOS Server, the commissioning procedure must be started again after resetting the AP with a factory reset. See section 8.3 for factory reset instructions.

5.6 Commissioning Finished

Commissioning the AP is now finished.

From this point on, the AP must be managed from the NOS Client, via the NOS Server. If the AP has not been pre-provisioned in the NOS Server, it must be configured before it is can enter service. See section 3 for information about AP provisioning.

5.6.1 Finished On Site Commissioning

If commissioning has been done on site, return to the site installation procedure in section 6.2.3 or 6.4.5, as appropriate.

5.6.2 Finished Advance Commissioning

If commissioning has been done in advance of sending the AP on site, it is advisable to ensure that the AP will connect to its serving NOS Server prior to sending the AP on site. To do this:

1) Verify that the AP has been pre-provisioned with a Site in the serving NOS Server.

2) Provide the AP with an appropriate network connection. If the AP has been commissioned to use IPsec, this means a network connection that will go via the Security Gateway, which is likely to require connection of the AP to an external network.

3) Power up the AP.

4) Use the NOS Client to verify that the AP has connected to its serving NOS Server. The Site for the AP and the AP object should have a green tick symbol against its icon.

5) After verifying this, re-pack the AP so that it is ready for delivery to its intended site.

6 nano3G AP Hardware Installation

This section documents the procedures for installing the nano3G AP hardware and physical connections.

The following hardware variants are described:

- *6.2 nano3G S8 AP Hardware Installation*
- *6.3 nano3G S16 AP Hardware Installation*
- *6.4 nano3G E8 AP and E16 AP Hardware Installation*

Note: If possible, the engineer should stay on site until the AP is brought into service, ready to make test calls to verify the AP has been configured correctly from the NOS.

Note: For residential deployments where an AP is installed by an end-user following an easy setup guide, ignore all of section 6.

6.1 Warnings and Regulatory Information

For all warnings and regulatory information, see section 9.

6.2 nano3G S8 AP Hardware Installation

6.2.1 Unpack the nano3G S8 AP

1) Unpack the nano3G S8 AP and its accessories.

Box contents may vary, but typically the box should contain the following:

- nano3G S8 AP unit
- nano3G S8 AP stand

Plus any combination of the following items, according to the options ordered:

- Mains adaptor unit
- POE injector unit and suitable mains cable
- POE splitter unit

Note: No screws are supplied to mount the AP or the splitter unit.

2) Check that the serial number on the nano3G S8 AP unit matches the label on the box.

3) Check that the items have not been damaged in transit.

For any damaged units, contact the supplier immediately for returns advice.

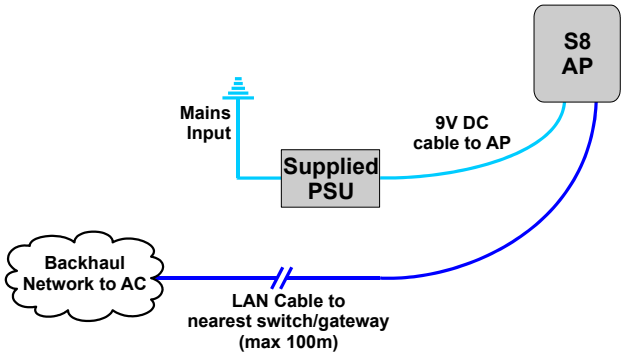
6.2.2 Commission the nano3G S8 AP

Configure the AP so that it will connect to its serving NOS Server. If this has not been done already, do this now, before installing the AP in its final location. For instructions, see section 5.

6.2.3 Cable Connections

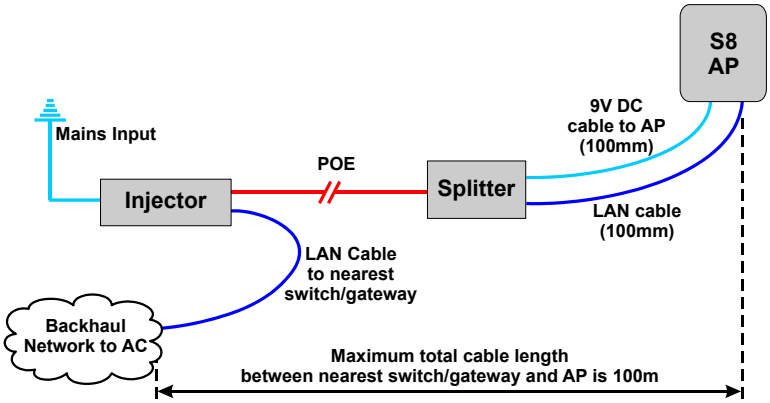
Use one of the cable connection schemes described below, to provide power and the LAN connection.

Supplied PSU and LAN



When the supplied PSU is used to power the AP, the POE injector and splitter units are not needed. However, this means that the mains socket providing power to the AP must be within reach of the cabling included with the supplied PSU (less than 2m).

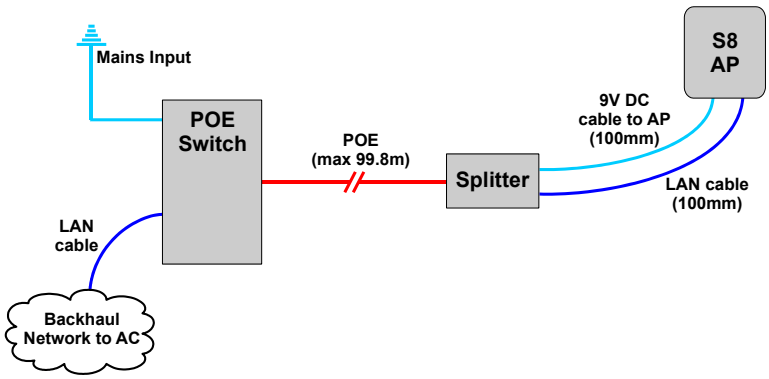
POE Injector and Splitter



This improves flexibility for locating the AP, as the AP can be up to approximately 100m from a mains power supply, depending on the placement of the POE Injector.

In this case, the PSU for the AP is not used. The injector takes a direct mains input using the supplied mains cable.

POE Switch and Splitter



In this case, the POE switch is a third-party item. This has similar benefits to using the POE injector, but a POE switch will typically only be used if there are multiple APs on site and/or there is other equipment that can take advantage of POE. The supplied POE splitter must be used with the AP.

Notice that the POE cable to the splitter should not exceed 99.8m in length. This will ensure that the total cable run from the POE switch to the AP is within the Ethernet limit of 100m.

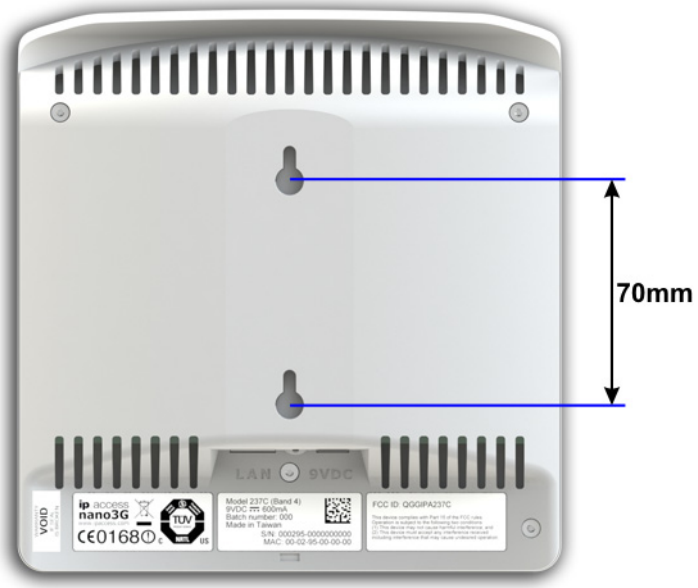
6.2.4 Mount the nano3G S8 AP

Note: The nano3G S8 AP should be installed in a position so that it is at least 2m away from the area where handsets are normally used.

The nano3G S8 AP **must** be mounted vertically in a location that allows air circulation around the unit. The AP can be mounted in the following ways:

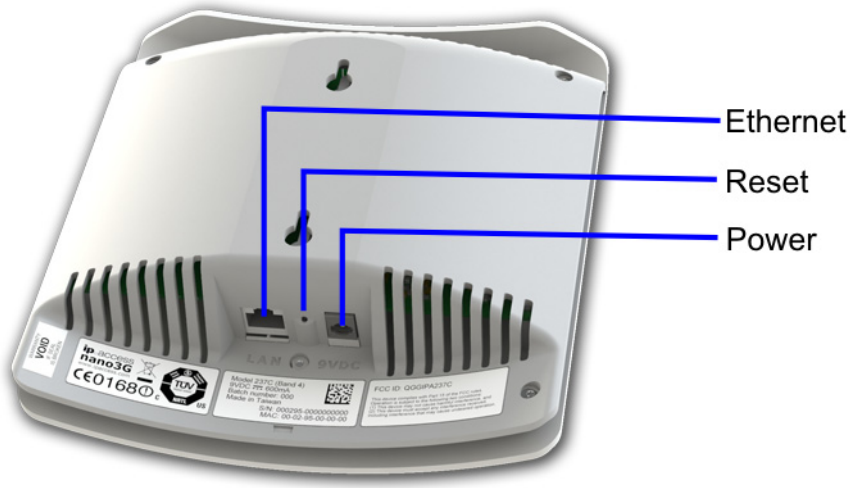
- On a stand
- Directly onto the wall at or above head height
- Onto the splitter unit on the wall at or above head height

The nano3G S8 AP has two holes at the back for direct wall mounting or mounting on the POE splitter:



Mount the nano3G S8 AP on a Stand

1) Plug the Ethernet cable and the power cable into the AP or plug the cables from the POE splitter into the AP.



2) Slide the AP onto the stand.

3) Place the AP on its stand on a stable flat surface.

Mount the nano3G S8 AP directly onto the wall

1) Drill two holes 70mm (2.76in) apart vertically for the two screws.

2) Insert wall plugs (if required) and secure the screws leaving approximately 3mm (0.12in) clearance between the screw heads and the wall.

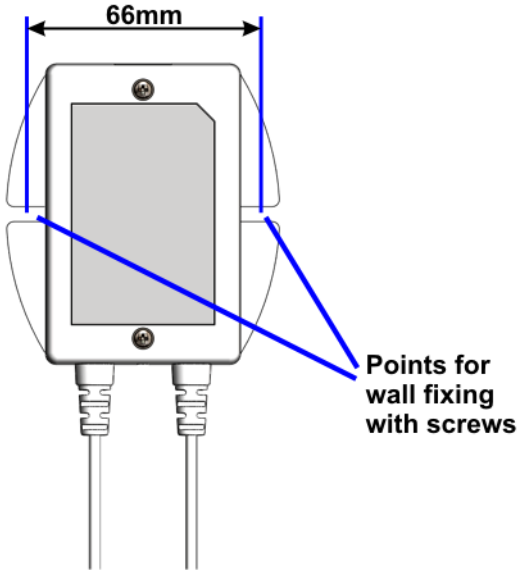
3) Plug the Ethernet cable and the power cable into the AP.

Note: If using the POE splitter when wall mounting the AP, it is recommended to mount the AP directly on the POE splitter, as in the following section. In some cases, it may be necessary to mount the AP and the POE splitter on the wall separately to minimise how far the AP projects from the wall. In this case, position the POE splitter below the AP where the 100mm cables will reach the AP.

4) Slide the AP onto the 2 screws.

Mount the nano3G S8 AP onto the splitter unit on the wall

1) Drill two holes 66mm (2.6in) apart horizontally for the two screws.



2) Secure the splitter unit to the wall using two screws.

   Ensure that the Ethernet socket is at the top.

3) Plug the Ethernet cable into the top of the splitter unit.

4) Plug the captive Ethernet cable and the power cable from the splitter unit into the AP.

5) Mount the AP onto the 2 screws that are already fixed onto the splitter unit.

6.3 nano3G S16 AP Hardware Installation

6.3.1 Unpack the nano3G S16 AP

1) Unpack the nano3G S16 AP and its accessories.

Box contents may vary, but typically the box should contain the following:

- nano3G S16 AP unit
- nano3G S16 AP stand

Plus any combination of the following items, according to the options ordered:

- Mains adaptor unit
- POE injector unit and suitable mains cable
- POE splitter unit

Note: No screws are supplied to mount the AP or the splitter unit.

2) Check that the serial number on the nano3G S16 AP unit matches the label on the box.

3) Check that the items have not been damaged in transit.

For any damaged units, contact the supplier immediately for returns advice.

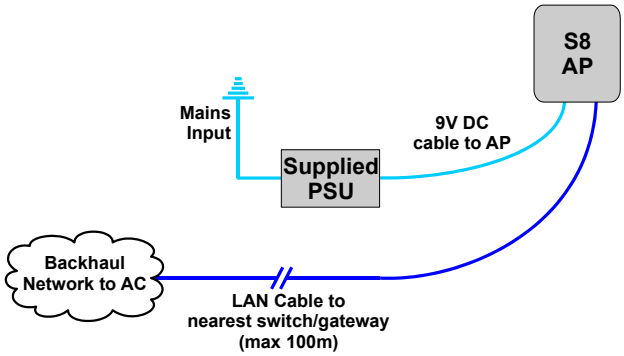
6.3.2 Commission the nano3G S16 AP

Configure the AP so that it will connect to its serving NOS Server. If this has not been done already, do this now, before installing the AP in its final location. For instructions, see section 5.

6.3.3 Cable Connections

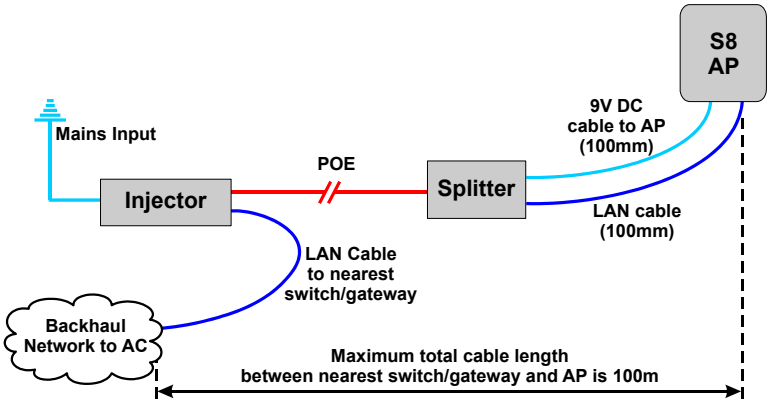
Use one of the cable connection schemes described below, to provide power and the LAN connection.

Supplied PSU and LAN



When the supplied PSU is used to power the AP, the POE injector and splitter units are not needed. However, this means that the mains socket providing power to the AP must be within reach of the cabling included with the supplied PSU (less than 2m).

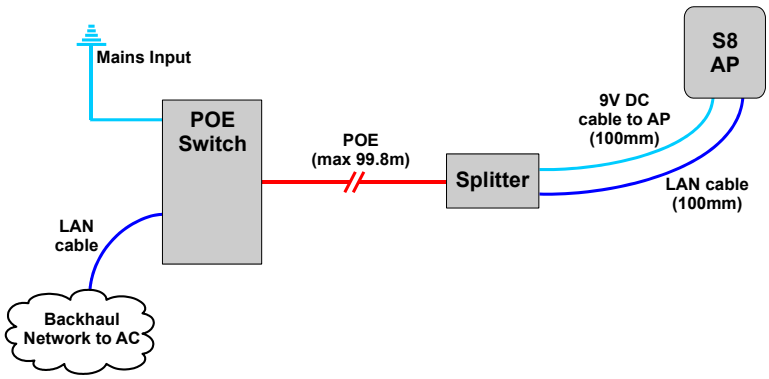
POE Injector and Splitter



This improves flexibility for locating the AP, as the AP can be up to approximately 100m from a mains power supply, depending on the placement of the POE Injector.

In this case, the PSU for the AP is not used. The injector takes a direct mains input using the supplied mains cable.

POE Switch and Splitter



In this case, the POE switch is a third-party item. This has similar benefits to using the POE injector, but a POE switch will typically only be used if there are multiple APs on site and/or there is other equipment that can take advantage of POE. The supplied POE splitter must be used with the AP.

Notice that the POE cable to the splitter should not exceed 99.8m in length. This will ensure that the total cable run from the POE switch to the AP is within the Ethernet limit of 100m.

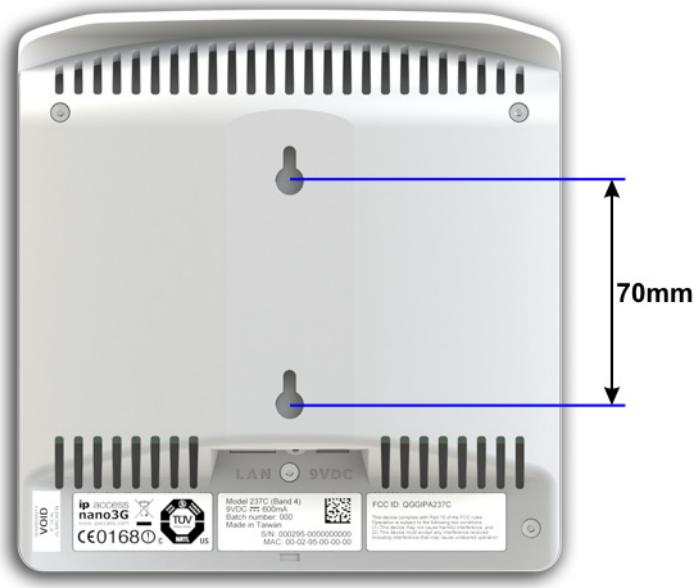
6.3.4 Mount the nano3G S16 AP

Note: The nano3G S16 AP should be installed in a position so that it is at least 2m away from the area where handsets are normally used.

The nano3G S16 AP **must** be mounted vertically in a location that allows air circulation around the unit. The AP can be mounted in the following ways:

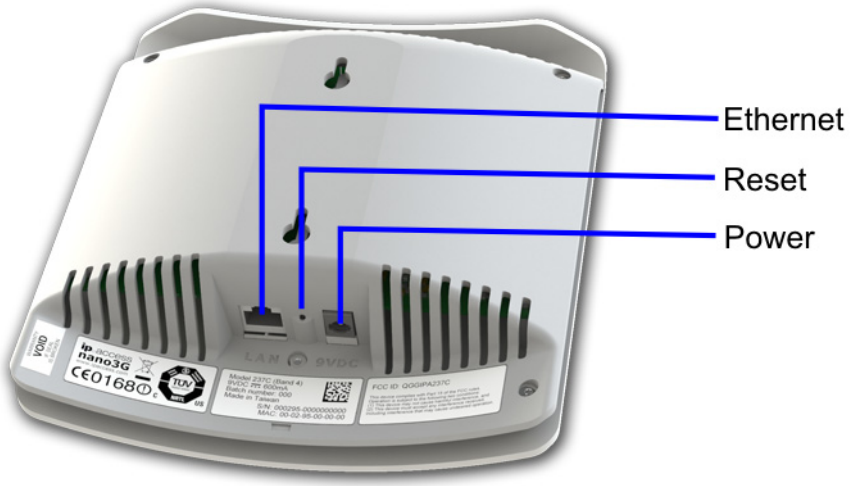
- On a stand
- Directly onto the wall at or above head height
- Onto the splitter unit on the wall at or above head height

The nano3G S16 AP has two holes at the back for direct wall mounting or mounting on the POE splitter:



Mount the nano3G S16 AP on a Stand

1) Plug the Ethernet cable and the power cable into the AP or plug the cables from the POE splitter into the AP.



2) Slide the AP onto the stand.

3) Place the AP on its stand on a stable flat surface.

Mount the nano3G S16 AP directly onto the wall

1) Drill two holes 70mm (2.76in) apart vertically for the two screws.

2) Insert wall plugs (if required) and secure the screws leaving approximately 3mm (0.12in) clearance between the screw heads and the wall.

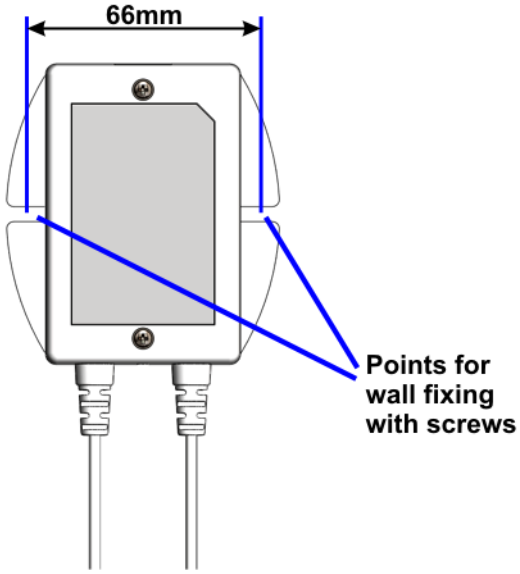
3) Plug the Ethernet cable and the power cable into the AP.

   Note: If using the POE splitter when wall mounting the AP, it is recommended to mount the AP directly on the POE splitter, as in the following section. In some cases, it may be necessary to mount the AP and the POE splitter on the wall separately to minimise how far the AP projects from the wall. In this case, position the POE splitter below the AP where the 100mm cables will reach the AP.

4) Slide the AP onto the 2 screws.

Mount the nano3G S16 AP onto the splitter unit on the wall

1) Drill two holes 66mm (2.6in) apart horizontally for the two screws.



2) Secure the splitter unit to the wall using two screws.

   Ensure that the Ethernet socket is at the top.

3) Plug the Ethernet cable into the top of the splitter unit.

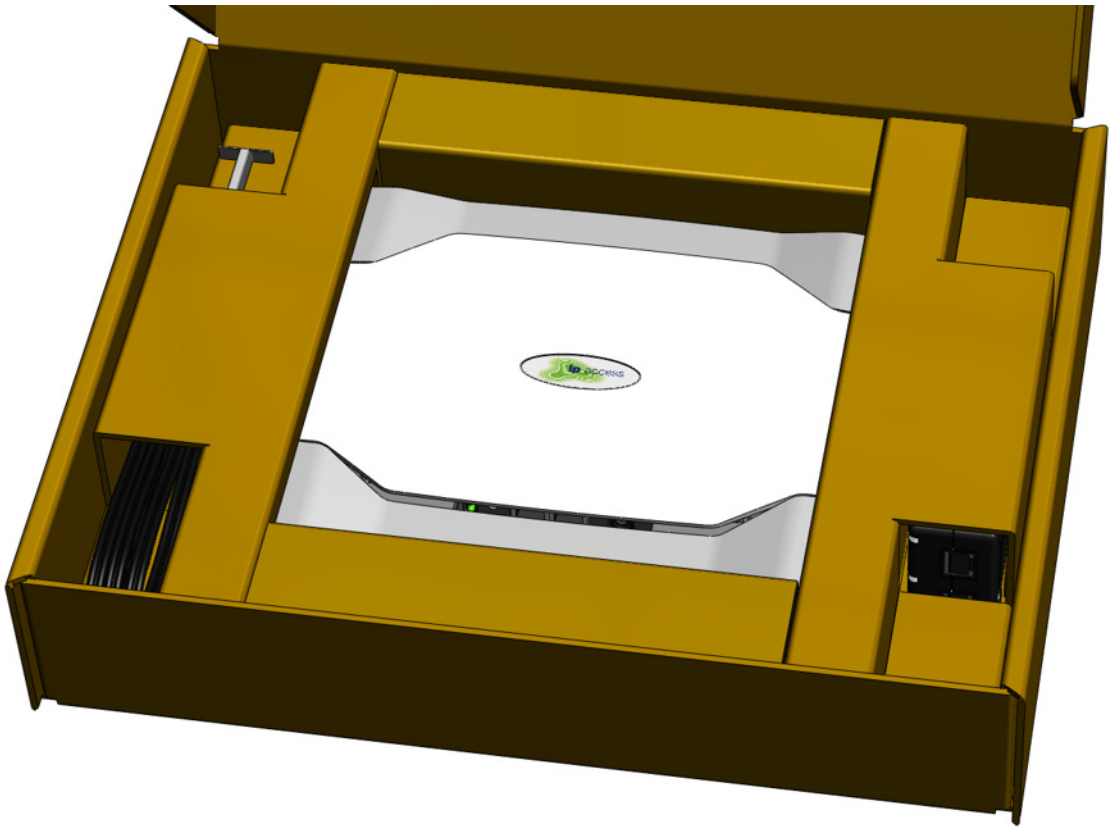
4) Plug the captive Ethernet cable and the power cable from the splitter unit into the AP.

5) Mount the AP onto the 2 screws that are already fixed onto the splitter unit.

6.4 nano3G E8 AP and E16 AP Hardware Installation

6.4.1 Unpack the nano3G E8 AP or E16 AP

1) Unpack the AP and its accessories.



Box contents may vary, but typically the box should contain the following:

- nano3G E8 AP or E16 AP unit with wall bracket attached
- Extraction tool for removing the AP from its wall bracket
- Injector unit for POE+
- Mains cable for the POE+ injector

2) Check that the serial number on the AP unit matches the label on the box.

3) Check that the items have not been damaged in transit.

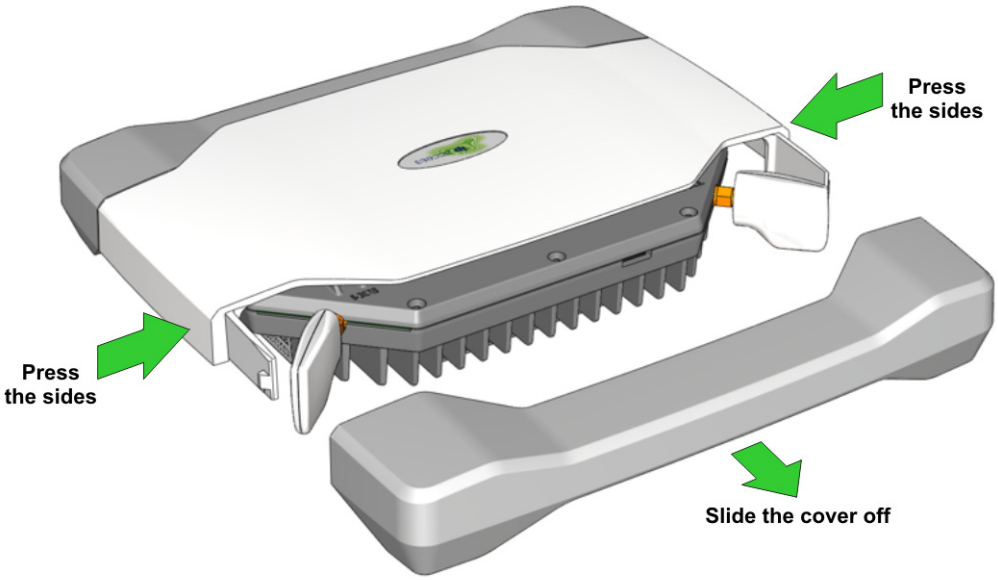
For any damaged units, contact the supplier immediately for returns advice.

6.4.2 Removable Cable and Antenna Covers

The nano3G E8 AP and E16 AP have two removable covers. The top cover goes over the antennae, and the bottom cover goes over the cable sockets.

1) Place the unit on a flat surface.

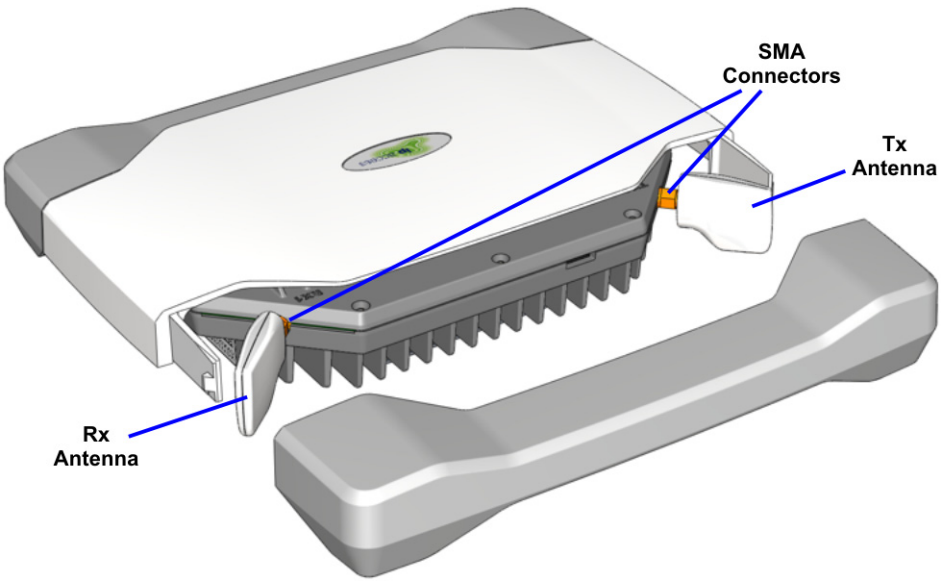
2) Press the sides of the unit next to the cover to be removed. Do not apply excessive force.



3) Slide the cover off.

4) To refit the cover, simply slide it back onto the tabs on the main cover until it snaps into place.

6.4.3 Antennas



The antennas must be oriented perpendicular to the unit, as shown, so that the cover fits correctly without stressing the connectors.

To fit external antennas, first remove the plastic cover from the antenna side of the unit. Unscrew the antennas to expose the SMA connectors. Connect external antennas directly to the SMA connectors. Route the cables out of the way of the antenna cover, then refit the cover.

6.4.4 Commission the AP

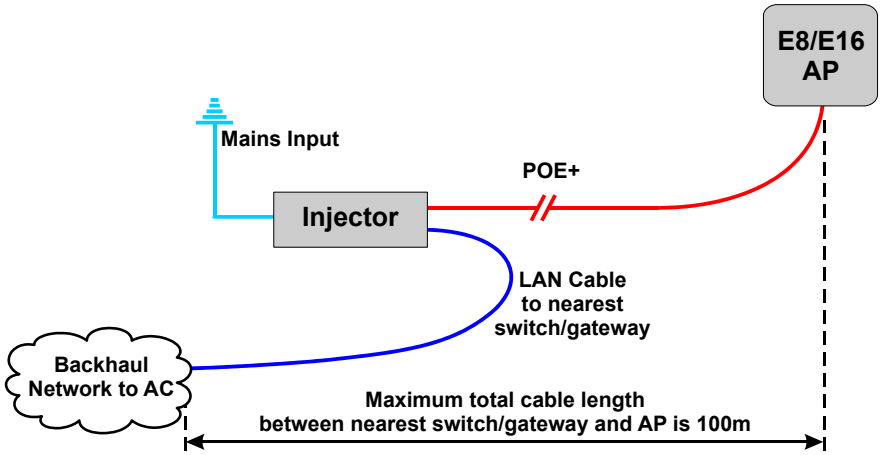
Configure the AP so that it will connect to its serving NOS Server. If this has not been done already, do this now, before installing the AP in its final location. For instructions, see section 5.

6.4.5 Cable Connections

Two power supply modules are available from ip.access, designed for use with the ip.access nano3G E8 AP and E16 AP, that are compliant with the IEEE 802.3at standard:

- The POE+ injector, as supplied, is commonly used for single site installations
- Direct power from the mains via an optional power adapter

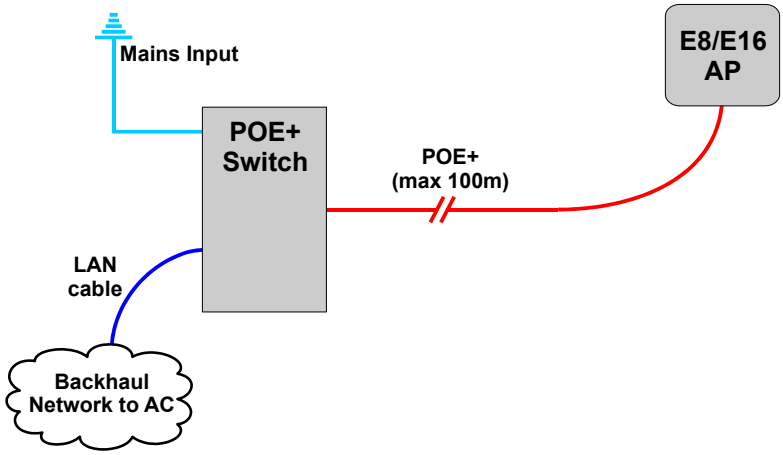
POE+ Injector



The AP can be up to 100m from the switch/gateway to the backhaul, but allow approximately 0.1m for routing through the injector. The injector can be positioned anywhere on this cable run. Hence the injector can be at the most convenient point for providing power, without restricting the location of the AP.

The injector takes a direct mains input using the supplied mains cable. Use a CAT5 Ethernet cable that is capable of carrying POE from the injector to the AP.

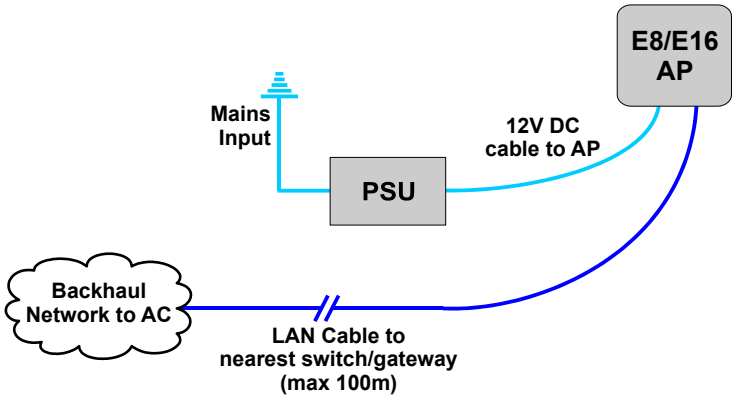
POE+ Switch



In this case, the POE+ switch is a third-party item. The cable run from the switch to the AP can be a full 100m.

A POE+ switch will typically only be used if there are multiple APs on site and/or there is other equipment that can take advantage of POE+.

PSU and LAN



When a suitable PSU is used to power the AP (see section 2.5.1) the POE+ injector unit is not needed. However, this means that a mains socket providing power to the AP must be within reach of the cabling included with the PSU. This is typically less than 2m. The PSU for the E8 AP or E16 AP is an optional extra.

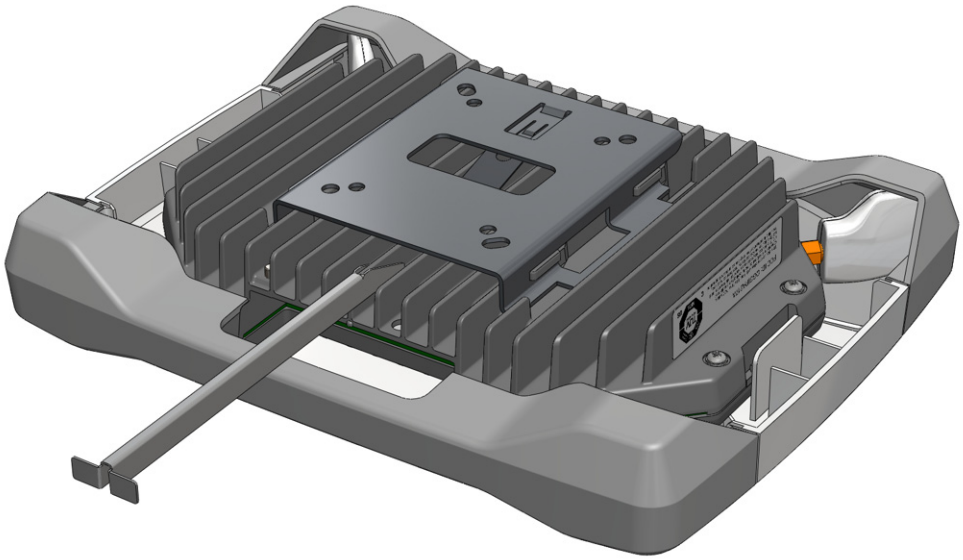
6.4.6 Mount the nano3G E8 AP or E16 AP on a Wall

Note: The nano3G E8 AP or E16 AP should be installed in a position so that it is at least 2m away from the area where handsets are normally used.

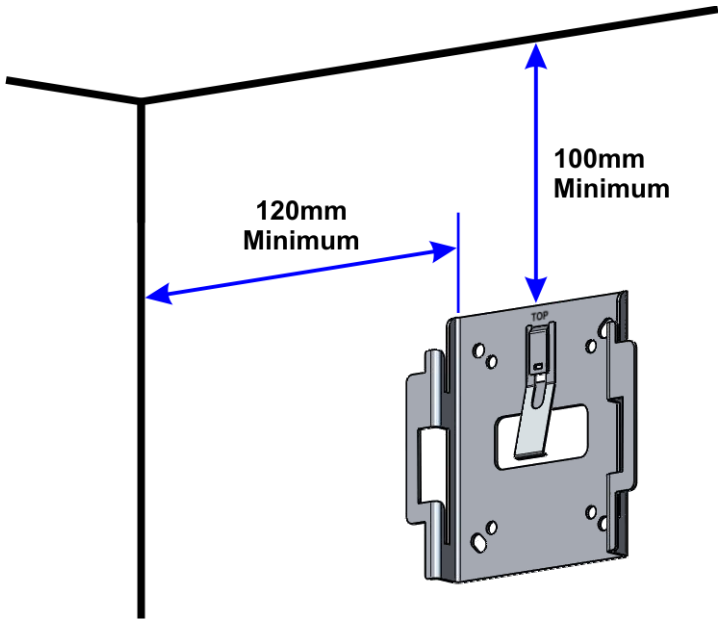
The nano3G E8 AP and E16 AP must be mounted vertically to ensure air circulation around the unit.

The location of each nano3G E8 AP and E16 AP should be shown on an installation floor plan produced at the network planning stage. For example, it must take into account that all APs must be at least 2m from any mobile equipment. The network wiring must be complete before the nano3G E8 AP or E16 AP can be installed and commissioned. The nano3G E8 AP and E16 AP should be placed on a wall at or above head height.

1) Remove the nano3G E8 AP or E16 AP from the wall bracket. Lay the AP on a flat surface with the wall bracket upwards. Slide the removal tool over the central fin between the bracket and the body of the unit to disengage the locking spring, then slide the bracket to separate it from the AP. The removal tool may be inserted from the top or bottom of the AP.



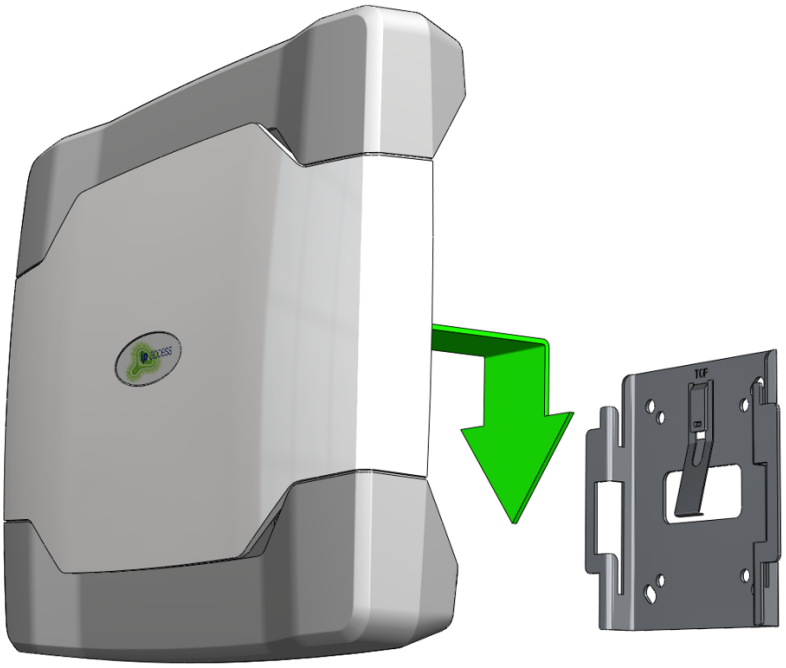
2) Position the bracket on the wall with its flat surface against the wall and the clip part towards the top. Ensure the bracket is level and sufficient clearance is maintained to allow the AP to be fitted to the bracket. Allow at least 100mm from the bracket to the top of wall, and 120mm from the side of the bracket to a side wall.



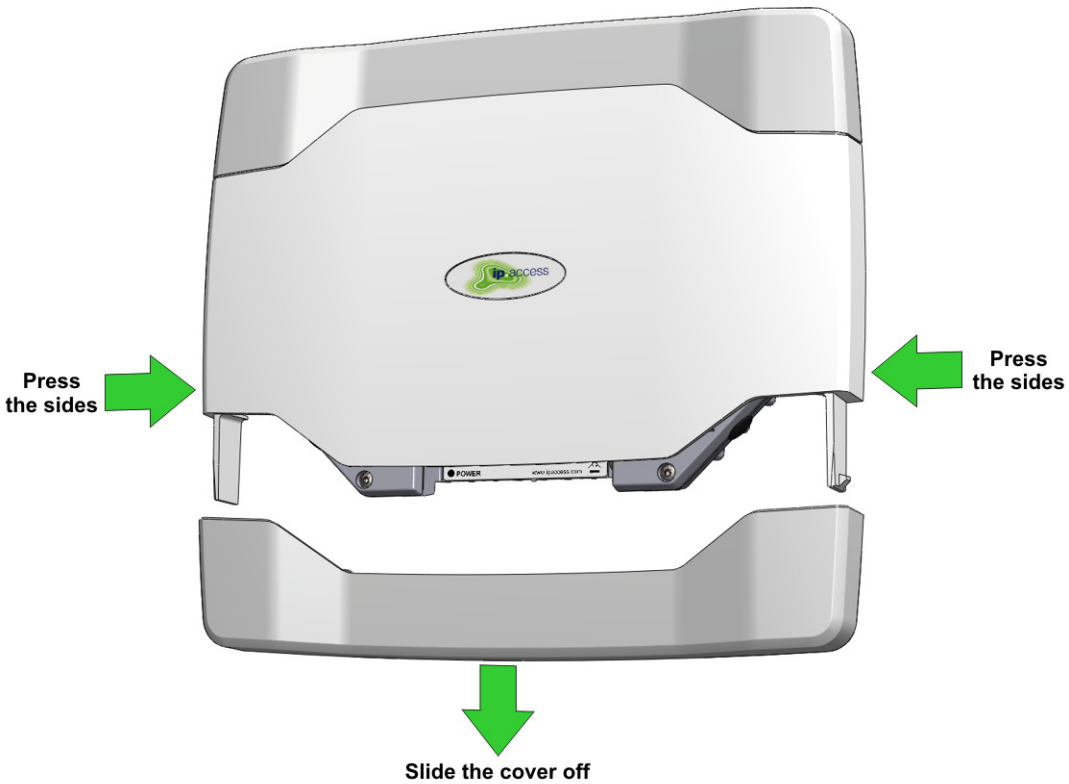
3) Mark the position of the four screw holes.

4) Drill the four holes in the positions marked previously and insert wall plugs (if required) and fix the mounting bracket securely to the wall. The bracket is designed to allow the nano3G E8 AP or E16 AP unit to be mounted with the connections either at the top or at the bottom of the unit.

5) Slide the nano3G E8 AP or E16 AP onto the bracket and ensure that the retaining spring engages into the indent at the rear of the unit.



6) Remove the lower cover to reveal the cable ports and LEDs.

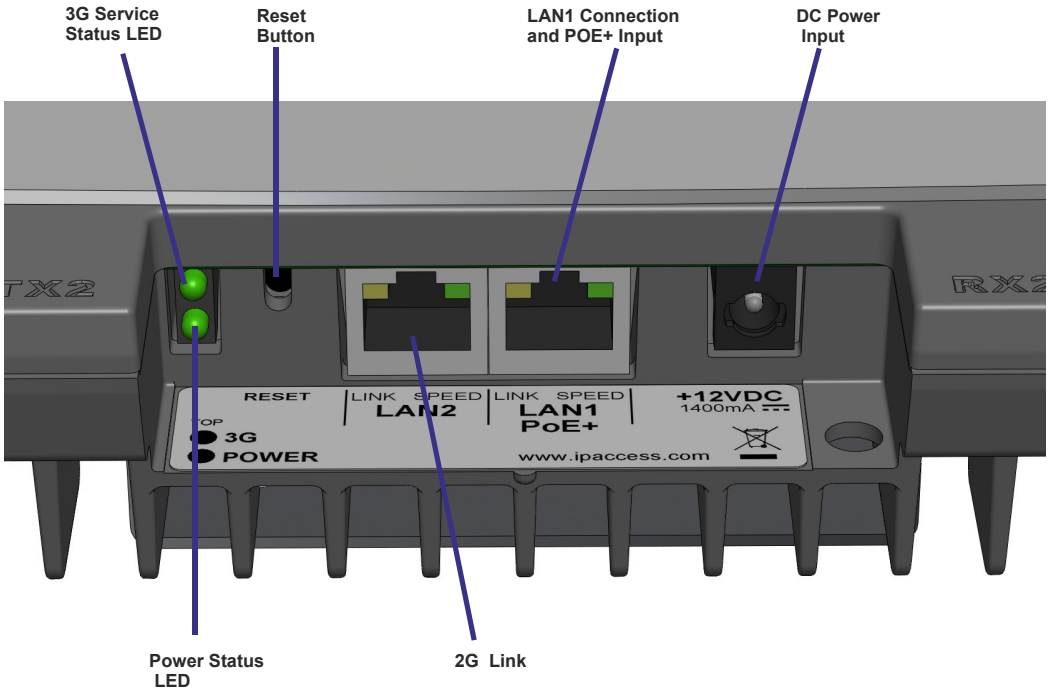


7) Plug in the required cables. Either:

- Plug an Ethernet cable from the POE+ injector or POE+ switch into LAN1

or

- Plug an Ethernet cable from a switch/gateway (no POE+) into LAN1 and an optional power supply into the +12V DC input



Note: Do not connect an Ethernet cable to LAN2. This will have no effect.

8) To refit the lower cover, slide it onto the tabs on the main cover until it snaps into place.

7 Finalize Installation

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

7.1 Check and Upgrade the nano3G 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.

7.1.1 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) Find the required AP within the AP area. Find the AC the AP is connected to (i.e. the BSMIS APs Per AC object) then locate the AP within its Site.

   Hence, drill down to the AP like this:

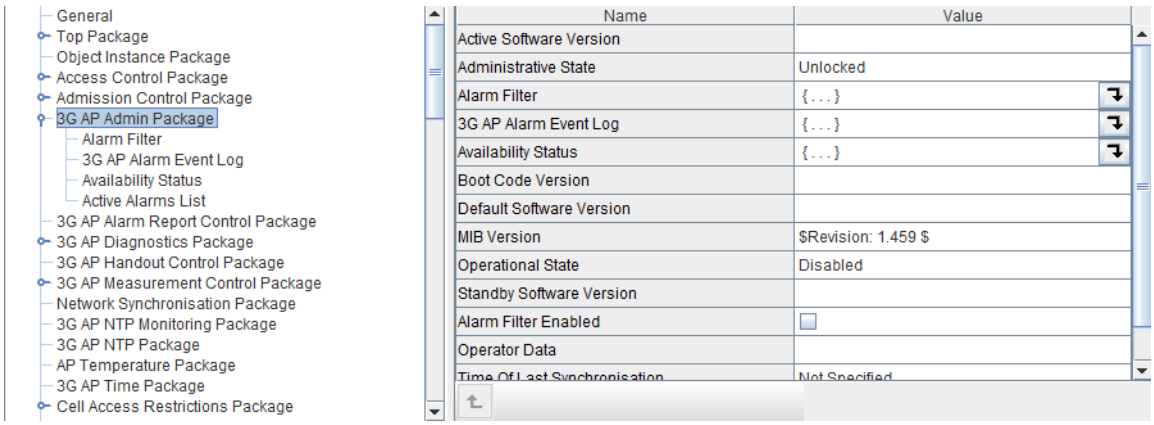
   Root > APs > BSMIS APs Per AC > Site > AP

   Note: For full information on using the NOS Client, see [OPM_415].

3) Verify that the **Site** has a green tick, to show that the AP is connected to the NOS Server. The AP object, below the Site, may be currently locked. The AP will remain locked if it is not ready to provide service.

4) In the Navigation pane, browse to the **AP Admin Package**.

5) Check the values of the **Active SW Version** and **Standby SW Version** attributes.



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 7.1.2.

7.1.2 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 [OPM_440].

1) Select the AP in the NOS Client.

2) Right-click the AP, select **Actions** and then **Perform Software Download**. The Perform Software Download Actions dialogue box will appear.

3) Change the **SW Download Operations** to Download, Swap and Reboot.

4) Click in the **SW Image Download URL** box and enter the URL of the required SDP file using the following URL pattern:

   `http://<server>/download/sw/<filename>.sdp`

   Where <server> is the IP address or host name of the required NOS Server, and <filename>.sdp is the required software download package file.

5) Press **<TAB>** or **<Enter>** to set the URL.

6) Click **Finish** and the download will take place. On the AP, download progress is indicated by the flashing network LED. When the download is complete, the AP will reboot under the new software. This may take several minutes.

7) Wait for the AP to be shown as connected to the NOS.

8) Select the **3G AP Admin Package** for the AP object and verify that the Filesys version reported by the **Active Software Version** matches the SDP file that was downloaded.

7.2 Finalize Configuration

7.2.1 Final Attribute Changes and Checks

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

2) Make any AP-specific configuration changes that have not already been applied by the Create Site Wizard or loading configuration files. In particular, ensure the static neighbour lists are correctly configured. See [OPM_300] for information on neighbour list configuration.

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

   - Cell Package
   - NAS Package
   - Location Package

7.2.2 Automatic Stored Configurations

This feature provides storage of a number of previous configurations for a collection of managed objects and provides a command whereby a user can revert the configuration of some of the system to a selected stored configuration. Each stored configuration is identified by:

- The name of the user who made the changes represented by the stored configuration
- The Date and Time (start and stop timestamps) during which the changes represented by the stored configuration were made
- A description, generated automatically but which can be edited by the user, which provides information about how or why this set of changes were made

A stored configuration contains information about what changes need to be made to a managed object sub-tree in order to return its configuration to what it was at a particular point in time.

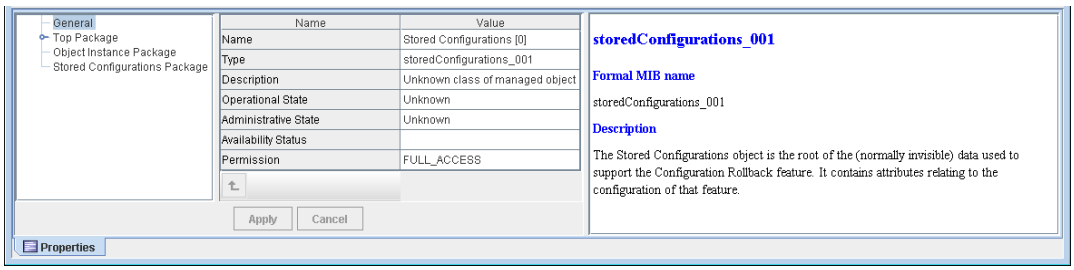
The first time any managed Object is created, there is no configuration stored. Only when the Managed Object has changes applied will the configuration first store the original configuration and also the changed configuration. For each Managed Object there isa maximum number of stored configurations that can be stored. This number can vary depending on the Managed Object. To find out how many stored configurations a Managed Object is allowed, look in the Stored Configurations Package Attribute for a specific Managed Object.

When a stored configuration maximum has been reached the oldest stored configuration will be deleted to make way for the newly stored configuration of a Managed Object.

Modified Stored Configuration Attributes

1) Select the **Stored Configurations** object under Network Orchestration System node. The attributes for this Managed Object are displayed in the properties pane:

2) Select the **Stored Configuration Package**.



3) Edit the attributes of the **Stored Configuration Package**. The configurable attributes of this managed object are:

Configuration Timeout	This attribute specifies in hours how long a gap between two amendments to the same managed object or group of objects counts as long enough that the later modification creates a new stored configuration
Maximum Number of Configurations	Specifies the maximum number of stored configurations that will be kept for each managed object or group of objects for which configuration Rollback is possible

4) Click **Apply** to save the changes, click **Cancel** to abandon any changes.

7.2.3 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) Select the AP object within the managing AP Management Service, AC Detail and Site. Select its 3GAP Time package, then wait a few seconds for the Up Time attribute to update. Verify that this is at least 1200, which is 20mins, 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. If necessary, wait until the Up Time passes 1200 seconds.

3) An AP must be locked to execute a Network Listen scan. Right-click the AP object and select **Lock**, then wait until a small padlock symbol is shown against the AP icon.

4) To execute a Network Listen scan, right-click the AP object, select **Actions** and then select **Start Sequential NWL Scan**.

5) When the scan is complete, view the results and verify there is some radio activity detected, and ideally some neighbour cells. This will confirm the radio is working.

6) Only if a suitable macro neighbour has been detected, a correction can be applied to ensure that the oscillator frequency is correct. Select **Actions** and then select **Apply Frequency Correction**.

   Note: Assuming there is a suitable macro neighbour, this should be repeated approximately 24 hours after the AP is brought into service. This will allow time for the oscillator crystal to stabilize, at which time the frequency correction should be re-applied.

7.3 Bring the AP into 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.

In most cases, a correctly pre-provisioned AP will start providing service once it has obtained its configuration from the NOS Server. These steps are only necessary when an AP is not yet enabled for service, or has been locked to apply additional configuration. An AP that is administratively Locked will have a small padlock symbol next to the AP icon.

1) To bring the AP into service, right-click the 3G AP object in the NOS Client and select **Unlock**. The padlock symbol next to the 3G AP icon will be removed.

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

7.4 Disable Web Interface from NOS

From the NOS it is possible to disable and re-enable the APs web interface. This setting is preserved across a Factory Restore.

Use the following flag in AP_Diag Tuning for this purpose:

- WEBIF_CTRL_PERMANENT_DISABLED_CMD = 1 will disable it
- WEBIF_CTRL_PERMANENT_DISABLED_CMD = 0 will re-enable it

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

2) Find the required AP within the APs under BSMIS APs Per AC.

   Hence, drill down to the AP like this:

   Root > APs > BSMIS APs Per AC > Site > relevant AP

3) In the Navigation Pane, select the 3G AP Diagnostics Package and drill down into the Diagnostic Tuning attribute.

4) Click the + button under the Attribute pane to add a new instance to the Diagnostic Tuning list.

5) Drill down into the new instance.

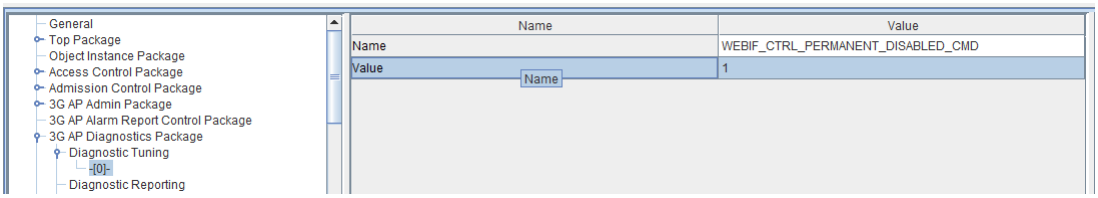
6) In the Name, enter:

   WEBIF_CTRL_PERMANENT_DISABLED_CMD

   This must be entered exactly as shown. If there is any variation, this will not have the desired effect.

7) In the Value, enter 1 to disable the web interface:

   For example:



Note: To re-enable to web interface, change the Value to 0.

8) Click Apply to save the changes.

   If the Apply button is not available, use the TAB key to exit field entry first.

9) Right-click the AP object and select Reinitialise. This restarts the AP so that it uses the configuration change.

8 Troubleshooting

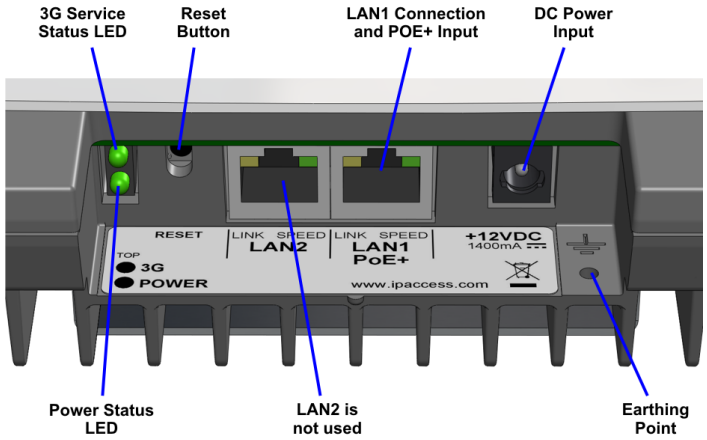
This section covers the following topics that may be useful for troubleshooting APs during installation and commissioning:

- *8.1 LED Status Indicators*
- *8.2 nano3G E8 AP or E16 AP Does Not Start Up*
- *8.3 Factory Reset*
- *8.4 Options for a Low Bandwidth Connection*

For more information on AP troubleshooting, see [TRB_300].

8.1 LED Status Indicators

8.1.1 nano3G E8 AP and nano3G E16 AP LEDs



The following table shows the meaning of the status indicators under normal and fault conditions.

3G	Off	The AP is not provisioned, it has no IP address. This may be a temporary condition when the AP is switched on for the first time, or after factory reset.
	Green	The AP is provisioned and unlocked, it is connected to the AC and is providing service.
	Flashing green (evenly, slowly)	The AP is provisioned but has lost connection to the AC, for example because the AC is not available or there is a DNS problem. The AP is locked.
	Flashing green (evenly, fast)	The AP has been reinitialized (the reset button was pressed but for less than 5 seconds).
	Off, with short green blinks on	Factory reset is in progress in the AP (the reset button was pressed for more than 5 seconds).
	On, with short green blinks off	Software download is in progress to the AP.

Power	Off	The AP is not switched on.
	Green	The AP is powered up normally.
	Flashing green	Self-test is running.
	Red	There is a fault with the AP.
Ethernet Link	Amber	This is on to show the link is active, or flashes when there is network activity.
Ethernet Speed	Green	Shows the network speed. On for 100Mbps or off for 10Mbps.

8.1.2 nano3G S8 AP LEDs

The following table shows the meaning of the status LEDs under normal and fault conditions.

 Power	Off	The nano3G AP is not switched on.
	Green	The nano3G AP is powered up normally.
	Flashing green	Self-test is running.
	Red	There is a fault with the nano3G AP.
 Network	Off	Unable to detect a network. This is usually because there is no network cable connected, or there is no network connection at the other end of the cable (for example, the router or broadband modem may have failed).
	Green	The 100Mbps connection is OK.
	Flashing green	Indicates activity on the network at 100Mbps speed (that is, the nano3G AP is sending and/or receiving data across the LAN).
	Amber	The 10Mbps connection is OK.
	Flashing amber	Indicates activity on the network at 10Mbps speed (that is, the nano3G AP is sending and/or receiving data across the LAN).
 Service	Off	The nano3G AP is not provisioned, it has no IP address. This may be a temporary condition when the AP is switched on for the first time, or after factory reset.
	Green	The nano3G AP is provisioned and unlocked, it is connected to the AP and is providing service.
	Flashing green (evenly, slowly)	The nano3G AP is provisioned but has lost connection to the AC, for example because the AC is not available or there is a DNS problem.
	Flashing green (evenly, fast)	The nano3G AP has been reinitialized (the reset button was pressed but for less than 5 seconds).
	Off, with a short green blink every 3 seconds	The nano3G AP is administratively Locked.
	Off, with short green blinks on	Factory reset is in progress in the nano3G AP (the reset button was pressed for more than 5 seconds).
	On, with short green blinks off	Software download is in progress to the nano3G AP.

8.1.3 nano3G S16 AP LEDs

The following table shows the meaning of the status LEDs under normal and fault conditions.

 Power	Off	The nano3G AP is not switched on.
	Green	The nano3G AP is powered up normally.
	Flashing green	Self-test is running.
	Red	There is a fault with the nano3G AP.
 Network	Off	Unable to detect a network. This is usually because there is no network cable connected, or there is no network connection at the other end of the cable (for example, the router or broadband modem may have failed).
	Green	The network connection is OK.
	Flashing green	Indicates activity on the network (that is, the nano3G AP is sending and/or receiving data across the LAN).
 Service	Off	The nano3G AP is not provisioned, it has no IP address. This may be a temporary condition when the AP is switched on for the first time, or after factory reset.
	Green	The nano3G AP is provisioned and unlocked, it is connected to the AP and is providing service.
	Flashing green (evenly, slowly)	The nano3G AP is provisioned but has lost connection to the AC, for example because the AC is not available or there is a DNS problem.
	Flashing green (evenly, fast)	The nano3G AP has been reinitialized (the reset button was pressed but for less than 5 seconds).
	Off, with a short green blink every 3 seconds	The nano3G AP is administratively Locked.
	Off, with short green blinks on	Factory reset is in progress in the nano3G AP (the reset button was pressed for more than 5 seconds).
	On, with short green blinks off	Software download is in progress to the nano3G AP.

8.2 nano3G E8 AP or E16 AP Does Not Start Up

Check the following:

- Check the power-over-Ethernet inserter: it must be a POE+ unit.
- Verify the Ethernet cable from the POE+ inserter is plugged into the correct socket (LAN1).
- If using a DC power supply instead of POE+, verify the power supply is a 12V supply with the correct polarity.

8.3 Factory Reset

A factory reset will delete an AP's configuration except for the *default set* of these five parameters, as set on the AP's commissioning web page:

- Management Server URL, which is the address of the default SCP server
- NTP server address
- IPsec enabled or disabled
- Security Gateway address (only relevant when IPsec is enabled)
- Remote traffic selector address and netmask (only relevant when IPsec is enabled)

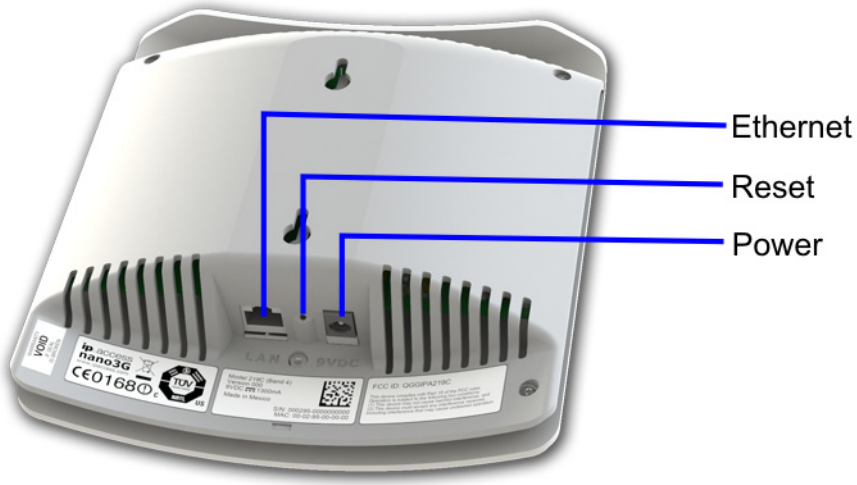
Therefore, executing a factory reset will mean that the AP will reconnect to the servers currently specified on the commissioning web page. If any of these servers are no longer valid, for example something has been decommissioned, the AP may be unable to re-enter service automatically after a factory reset. If it necessary to change any of these settings, physical access to the AP is required, so that it can be connected to a commissioning terminal.

Note: If the reset button is released before the factory reset starts, the AP will reboot. It will not return to the factory reset state.

Note: If the AP has been disabled as in section 7.4. It will not be possible to recommission the AP. The AP will reconnect to the servers currently specified on the commissioning web page.

8.3.1 nano3G S8 AP Factory Reset

1) Use a thin rod to press and hold the reset button.



2) Keep the reset button pressed until the Service LED changes from blinking fast (50ms on, 50ms off) to blinking slowly (200ms on, 200ms off).

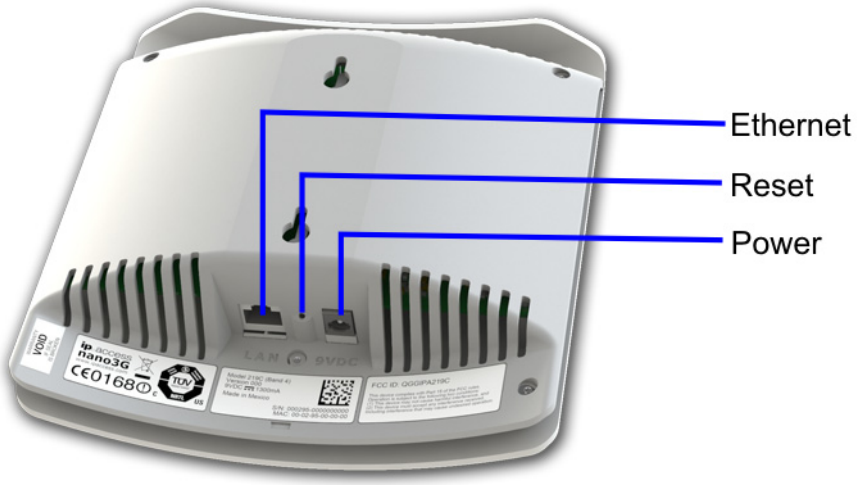
   The Service LED blinks fast (50ms on, 50ms off) until the factory reset commences, then it blinks slowly (200ms on, 200ms off). When the factory restore process is complete, the LED extinguishes and the AP automatically reboots, takes the fixed IP address and enables the web interface for commissioning.

3) If required, use a connected commissioning terminal to login to the AP's web interface. The login to the web interface is only available for 60 seconds. If the AP times out, it will boot up using the *default set* of parameters, as per the current entries on the commissioning web page.

4) See section 5 for the commissioning procedure.

8.3.2 nano3G S16 AP Factory Reset

1) Use a thin rod to press and hold the reset button.



2) Keep the reset button pressed until the Service LED changes from blinking fast (50ms on, 50ms off) to blinking slowly (200ms on, 200ms off).

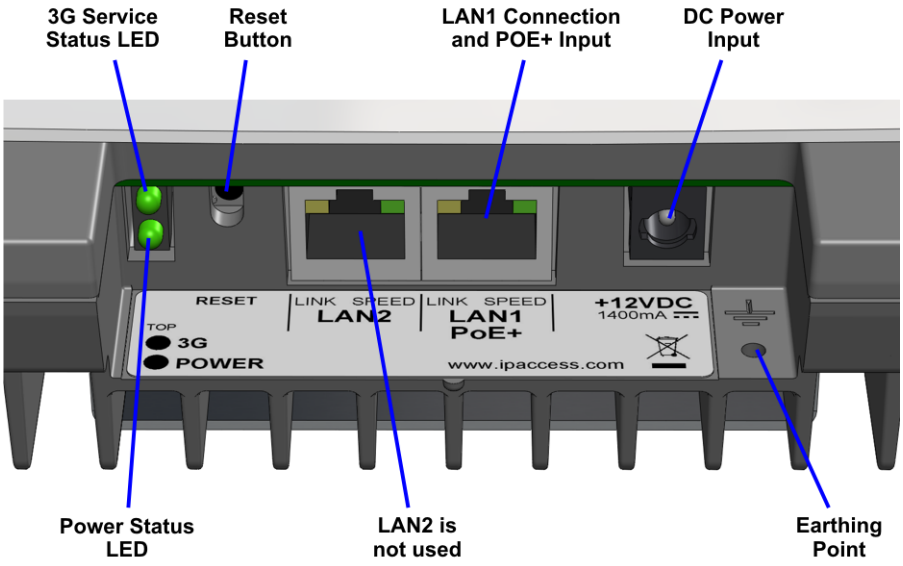
   The Service LED blinks fast (50ms on, 50ms off) until the factory reset commences, then it blinks slowly (200ms on, 200ms off). When the factory restore process is complete, the LED extinguishes and the AP automatically reboots, takes the fixed IP address and enables the web interface for commissioning.

3) If required, use a connected commissioning terminal to login to the AP's web interface. The login to the web interface is only available for 60 seconds. If the AP times out, it will boot up using the *default set* of parameters, as per the current entries on the commissioning web page.

4) See section 5 for the commissioning procedure.

8.3.3 nano3G E8 AP and nano3G E16 AP Factory Reset

1) Use a thin rod to press and hold the reset button.



2) Keep the reset button pressed until the 3G LED changes from blinking fast (50ms on, 50ms off) to blinking slowly (200ms on, 200ms off).

   The 3G LED blinks fast (50ms on, 50ms off) until the factory reset commences, then it blinks slowly (200ms on, 200ms off). When the factory restore process is complete, the LED extinguishes and the AP automatically reboots, takes the fixed IP address and enables the web interface for commissioning.

3) If required, use a connected commissioning terminal to login to the AP's web interface. The login to the web interface is only available for 60 seconds. If the AP times out, it will boot up using the *default set* of parameters, as per the current entries on the commissioning web page.

4) See section 5 for the commissioning procedure.

8.4 Options for a Low Bandwidth Connection

8.4.1 N User Configuration

It may be useful to reduce the number of active UEs on an AP when an AP has a backhaul link with limited bandwidth. N-User Configuration allows for a reduction in the maximum number of active UEs on a nano3G AP by controlling how many CELL_DCH users are allowed on an AP.The maxNumCellDchEues attribute reports the hardware capability of an AP.

Below is a table with minimum bandwidth required to support a specific number of DCH UEs and vice versa. If the AP is configured to support a specific number of UEs in DCH then bandwidth limits should be set accordingly (AP will ignore bandwidth settings if it is lower than dictated by the DCH UE number)

Each reduction in max users will reduce the max requirement for CS by 65Kbps in DL and 20Kbps in UL.

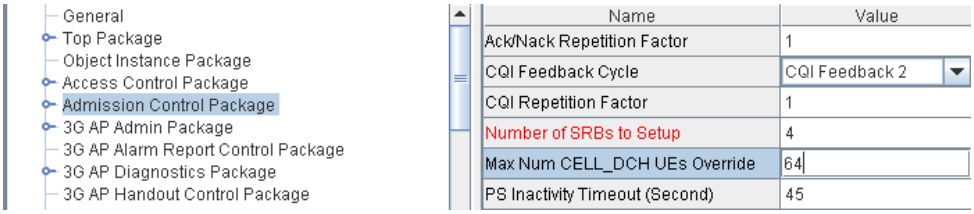
DCH Ues	Downlink Backhaul Bit Rate (Kbps)	Uplink Backhaul Bit Rate (Kbps)
0	80	80
1	98	142
2	117	205
3	137	269
4	157	334
5	177	397
6	197	462
7	217	525
8	237	589
9	257	654
10	277	717
11	297	782
12	317	845
13	337	909
14	357	974
15	377	1037
16	397	1102

There is no effect if the override value in maxNumCellDchUesOverride is equal or greater than the hardware capability.

1) Log into the NOS Client and find the AP. The user ID must have Full Access rights to the AP.

   Hence find, Root > APs > BSMIS APs Per AC > Site > relevant AP.

2) Select Admission Control Package from the Navigation Pane.



3) Select the attribute maxNumCellDchUesOverride and set to the relevant value.

4) Click Apply to save changes.

8.4.2 Dynamic Backhaul Management (DBM)

The DBM feature addresses the need to make optimal usage of backhaul bandwidth in scenarios where backhaul bandwidth is limited.

Note: Where a nano3G AP is deployed without IPsec enabled and the Backhaul ISP or other routers between the nano3G AC and the AP are aeroing out DSCP marking applied by the AC on the downlink, then the DBM feature on the DL should NOT be enabled. This only affects the DL as the AP does not control DL DSCP marking.

Note: On the UL the AP is the source of the packets. Hence, prioritisation and bandwidth limiting occurs before DSCP marks are zeroed out by routers or ISPs.

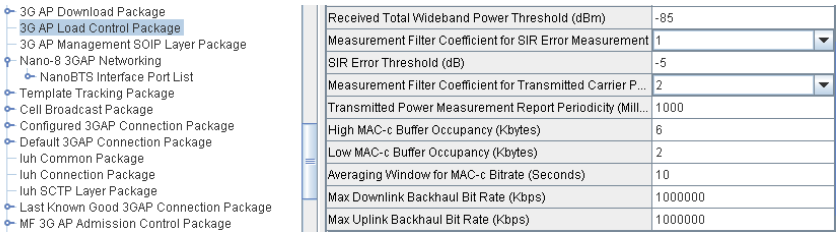
Note: Where APs use IPsec, the AP will inspect the inner packet, which should not have its DSCP mark removed, and should continue to function with the DBM DL limit applied.

To set a limit on total AP bandwidth usage of the backhaul and prioritise CS voice traffic to ensure that voice quality is maintained, do the following:

1) Log into the NOS Client and find the AP. The user ID must have Full Access rights to the AP.

   Hence find, Root > APs > BSMIS APs Per AC > Site > relevant AP.

2) Select 3G AP Load Control Package from the Navigation Pane.



3) Select the attribute max Downlink Backhaul Bit Rate (Kbps) and set to the relevant value.

4) Select the attribute max Uplink Backhaul Bit Rate (Kbps) and set to the relevant value.

5) Click Apply to save changes.

9 nano3G AP and PSU Regulatory Information

This chapter provides the customer with safety and regulatory warnings, cautions and information for the ip.access Ltd range of products.

9.1 Warnings and Cautions

Electrical Safety

	CAUTION The nano3G AP is intended for dry indoor applications only. If evidence of condensation is present do not apply power to the nano3G AP.
	CAUTION The nano3G AP is designed to be operated as a fixed system device and must be located away from the user. It must be mounted in a manner to ensure that all users and bystanders are kept a minimum of 20cm away from the integral antennas at all times.
	WARNING Do not immerse any part of the nano3G AP or its power supply in water or any other liquid. Do not install or use the nano3G AP or its power supply near open water. Do not spill liquids of any type on the nano3G AP or its power supply.
	WARNING Do not use liquid, solvent or aerosol cleaning agents on or near the nano3G AP or its power supply.
	CAUTION To avoid the risk of fire and/or electrical shock, do not push objects through openings into the nano3G AP or its power supply (except when operating the Reset switch on the nano3G AP).
	CAUTION Do not disassemble the nano3G AP or its power supply.
	CAUTION The nano3G AP must only be powered using the ip.access power supply provided for use with the nano3G AP.
	CAUTION Before using the power supply, verify that the mains voltage is within the range specified by the voltage printed on the power supply.
	CAUTION The PSU supplied with the nano3G AP must not be used for powering any other equipment.
	CAUTION To avoid the risk of fire and/or electrical shock, do not overload power outlets or extension cables.
	CAUTION When disconnecting the power supply from the mains, pull the plug. Pulling the cable may result in damage to the cable.

Interference with Electronic Devices

	CAUTION If using a pacemaker, ensure you are using the device in accordance with its safety requirements with respect to RF devices. Consult your doctor if you have questions about RF signals and your pacemaker.
	CAUTION If using a hearing aid, RF devices may cause interference.
	CAUTION Unshielded electronic devices should not be used near the nano3G AP. Conversely, the nano3G AP should not be installed adjacent to unshielded electrical or electronic devices (such as unshielded speakers).

Other Warnings and Cautions

	WARNING Do not install the nano3G AP in a position where the power supply cable or network cable may cause a tripping or choking hazard.
	WARNING Do not install the nano3G AP or the power supply on an unstable surface. All caution must be observed to prevent the device from falling and causing injury to a person and/or damage to the device.
	WARNING The nano3G AP should not be disposed of in household waste bins. Please follow local regulations for disposal of electronic devices.
	CAUTION Do not install the nano3G AP in a position where the power supply cable or network cable may be damaged by walking on the cables.
	CAUTION Do not attempt to fit an external antenna or antenna cabling to the nano3G S8 AP.

9.2 Regulatory Statements for nano3G S8 AP

9.2.1 US FCC Compliance

- FCC CFR47 Part 15B: Variants 237B, BA, C, CA
- FCC CFR47 Parts 22, 24: Variants 237B, BA
- FCC CFR47 Part 27: Variants 237C, CA

Note: Changes or modifications not expressly approved by the party responsible for compliance may void the user's authority to operate this equipment.

The FCC IDs for nano3G S8 AP model variants are:

Model	**FCC ID**
nano3G 237B	QGGIPA237B
nano3G 237BA	QGGIPA237BA
nano3G 237C	QGGIPA237C
nano3G 237CA	QGGIPA237CA

WARNING
This is a class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Note: This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

9.2.2 EU Regulatory Compliance

Models nano3G 237A and 237AA conform to the following regulatory standards:

Health (Art 3.1(a)):	EN50385: 2002
Safety (Art 3.1(a)):	EN60950-1: 2006
EMC (Art 3.1(b)):	EN 301 489-23 V1.3.1, EN 301 489-1 V1.8.1
Spectrum (Art 3.2):	EN 301 908-1 V4.2.1, EN 301 908-3 V4.2.1

This product is intended for use in all Member States of the European Union.

"Hereby, ip.access Ltd, declares that this nano3G S8 AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC."

A copy of regulatory compliance documentation may be obtained in writing from "IP Access Ltd, Building 2020, Cambourne Business Park, Cambourne, Cambridge, CB23 6DW, UK".

CE0168

9.2.3 Safety Standards

- IEC 60950-1:2005 (2nd Edition), EN 60950-1:2006 and UL60950-1:2007

The power adapter, as well as the POE inserter and splitter supplied by ip.access comply with LPS requirements in accordance with IEC/EN 60950-1.

9.3 Regulatory Statements for nano3G E8 AP

9.3.1 US FCC Compliance

- FCC CFR47 Parts 15B, 27

Note: Changes or modifications not expressly approved by the party responsible for compliance may void the user's authority to operate this equipment.

Model nano3G 217C has FCC ID QGGIPA217C

	WARNING This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Note: This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

9.3.2 EU Regulatory Compliance

Model nano3G 217A conforms to the following regulatory standards:

Health (Art 3.1(a)):	EN50385: 2002
Safety (Art 3.1(a)):	EN60950-1: 2006
EMC (Art 3.1(b)):	EN 301 489-23 V1.3.1, EN 301 489-1 V1.8.1
Spectrum (Art 3.2):	EN 301 908-1 V4.2.1, EN 301 908-3 V3.2.1

This product is intended for use in all Member States of the European Union.

"Hereby, ip.access Ltd, declares that this nano3G E8 AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC."

A copy of regulatory compliance documentation may be obtained in writing from "IP Access Ltd, Building 2020, Cambourne Business Park, Cambourne, Cambridge, CB23 6DW, UK".

CE0168①

9.3.3 Safety Standards

- IEC 60950-1:2005 (2nd Edition) and EN 60950-1:2006

The POE+ inserter supplied by ip.access complies with LPS requirements in accordance with IEC/EN 60950-1.

9.3.4 Environmental Standards

- ETSI 300 019-2-3
- ETSI 300 019-2-2

9.4 Regulatory Statements for nano3G S16 AP

9.4.1 US FCC Compliance

- FCC CFR47 Part 15B: Variants 237B, BA
- FCC CFR47 Parts 22, 24: Variants 237B, BA

Note: Changes or modifications not expressly approved by the party responsible for compliance may void the user's authority to operate this equipment.

The FCC IDs for nano3G S16 AP model variants are:

Model	FCC ID
nano3G 243B	QGGIPA243B
nano3G 243BA	QGGIPA243BA

WARNING
This is a class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Note: This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

9.4.2 EU Regulatory Compliance

Models nano3G 243A and 243AA conform to the following regulatory standards:

Health (Art 3.1(a)):	EN50385: 2002
Safety (Art 3.1(a)):	EN60950-1: 2006
EMC (Art 3.1(b)):	EN 301 489-1 V1.8.1 (2008-04), EN 301 489-23 V1.5.1 (2011-11)
Spectrum (Art 3.2):	EN 301 908-3 V5.2.1 (2011-05), EN 301 908-1 V5.2.1 (2011-05)

This product is intended for use in all Member States of the European Union.

"Hereby, ip.access Ltd, declares that this nano3G S16 AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC."

A copy of regulatory compliance documentation may be obtained in writing from "IP Access Ltd, Building 2020, Cambourne Business Park, Cambourne, Cambridge, CB23 6DW, UK".

CE0168①

9.4.3 Safety Standards

- IEC 60950-1:2005 (2nd Edition), EN 60950-1:2006 and UL60950-1:2007

The power adapter, as well as the POE inserter and splitter supplied by ip.access comply with LPS requirements in accordance with IEC/EN 60950-1.

9.5 Regulatory Statements for nano3G E16 AP

9.5.1 US FCC Compliance

- FCC CFR47 Parts 15B, 27

Note: Changes or modifications not expressly approved by the party responsible for compliance may void the user's authority to operate this equipment.

Model nano3G 239B has FCC ID QGGIPA239B

Model nano3G 239C has FCC ID QGGIPA217C

WARNING
This is a class B product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Note: This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

9.5.2 EU Regulatory Compliance

Model nano3G 239C conforms to the following regulatory standards:

Health (Art 3.1(a)):	EN50385: 2002
Safety (Art 3.1(a)):	EN60950-1: 2006 + A11:2009
EMC (Art 3.1(b)):	EN 301 489-23 V1.3.1, EN 301 489-1 V1.8.1
Spectrum (Art 3.2):	EN 301 908-1 V5.2.1, EN 301 908-3 V3.2.1

This product is intended for use in all Member States of the European Union.

"Hereby, ip.access Ltd, declares that this nano3G E16 AP is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC."

A copy of regulatory compliance documentation may be obtained in writing from "IP Access Ltd, Building 2020, Cambourne Business Park, Cambourne, Cambridge, CB23 6DW, UK".

CE0168①

9.5.3 Safety Standards

- IEC 60950-1:2005 (2nd Edition) and EN 60950-1:2006

The POE+ inserter supplied by ip.access complies with LPS requirements in accordance with IEC/EN 60950-1.

9.5.4 Environmental Standards

- ETSI 300 019-2-3
- ETSI 300 019-2-2