casa systems

User Guide

AurusPRO 5G Outdoor CPE

3GPP Release 16

Model CFW-2832

Doc No. UG01427

Important notice

This device, like any wireless device, operates using radio signals which cannot guarantee the transmission and reception of data in all conditions. While the delay or loss of signal is rare, you should not rely solely on any wireless device for emergency communications or otherwise use the device in situations where the interruption of data connectivity could lead to death, personal injury, property damage, data loss, or other loss. Casa Systems accepts no responsibility for any loss or damage resulting from errors or delays in transmission or reception, or the failure of the Casa Systems AurusPRO Global 5G Outdoor CPE to transmit or receive such data.

Safety and hazards

⚠ Warning – Do not connect or disconnect cables or devices to or from the USB port, SIM card tray, or Ethernet port in hazardous locations such as those in which flammable gases or vapours may be present, but normally are confined within closed systems; are prevented from accumulating by adequate ventilation; or the location is adjacent to a location from which ignitable concentrations might occasionally be communicated.

Copyright

Specifications are subject to change without notice. Images shown may vary slightly from the actual product.

ⓘ Note – This document is subject to change without notice.

Document history

This document applies to the following CPE model:

AurusPRO 5G Outdoor CPE – CFW-2832

Ver.	Document description	Date
v1.01	Initial document release for 3GPP Release 16 devices	23 September, 2022

Table i. – Document revision history

Contents

1 Document overview

1.1 Introduction

This document provides you all the information you need to set up, configure and deploy the CFW-2832 in the Casa Systems AurusPRO Global 5G Outdoor CPE antenna.

1.2 Target audience

This document is intended for experienced hardware installers who understand telecommunications terminology and concepts.

1.3 Prerequisites

If local regulations require the use of a CBRS Spectrum Access Server then the AurusPRO Global 5G Outdoor CPE must be professionally installed by a Certified Professional Installer (CPI) in order to function.

Before continuing with the installation of the CPE please confirm that you have:

- A mobile device (tablet or smartphone) with the Aurora Installation application installed.
- Read the entire Safety and product care section of this document and RF Exposure information.

You will also require wrenches or sockets and screwdrivers and other tools and materials depending on how you plan to mount the device.

1.3.1 Notation

The following symbols may be used in this document:

ⓘ Note – This note contains useful information.

⚠ Important – This is important information that may require your attention.

⚠ Warning – This is a warning that may require immediate action in order to avoid damage or injury.

2 Product introduction

2.1 Product overview

Rural and regional homes and businesses, remote commercial sites and metropolitan fringe districts located beyond the reach of fixed line infrastructure rely on mobile networks to access broadband Internet.

Designed to optimise signal strength in weak signal areas, the AurusPRO 5G Outdoor CPE is positioned on the exterior of the premises to overcome distance limitations and geographical obstructions and deliver high-speed 5G connectivity to wired and wireless clients in the property via an indoor router.

2.2 Package contents

The in-box contents include:

- 1 x AurusPRO Global 5G Outdoor CPE
- 1 x Assembled mount bracket

Accessories used in this solution (packaged separately):

- 1 x Antenna Power Supply (POE-03) – used to power the AurusPRO during normal operation
- 1 x 5G Smart Antenna Tool – used to power and provide a wireless interface to the AurusPRO 5G Outdoor CPE during installation.

If any of these items are missing or damaged, please contact your sales representative immediately.

3 Physical dimensions and interfaces

3.1 Physical dimensions

3.1.1 CFW-2832

Below are details of the layout and physical dimensions of the CFW-2832.

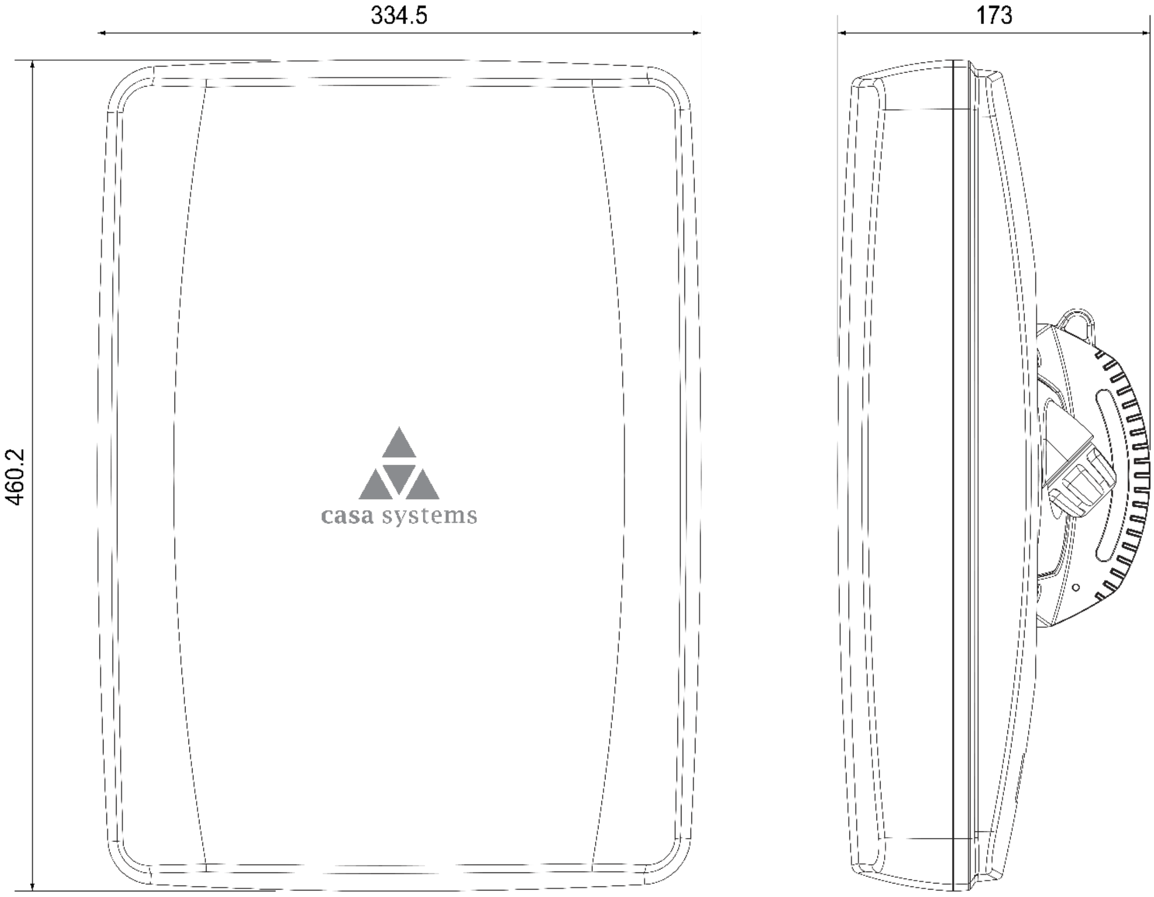


Figure 1 – CFW-2832 5G Outdoor CPE dimensions

CFW-2832 Dimensions

Height	460mm (18.1 in)
Width	335mm (13.2 in)
Depth (excluding mount)	184mm (7.25 in)
Weight (excluding mount)	2.875kg (6 lb 5.4 oz)

Table 1 - CFW-2832 device dimensions

3.2 Interfaces

3.2.1 CFW-2832

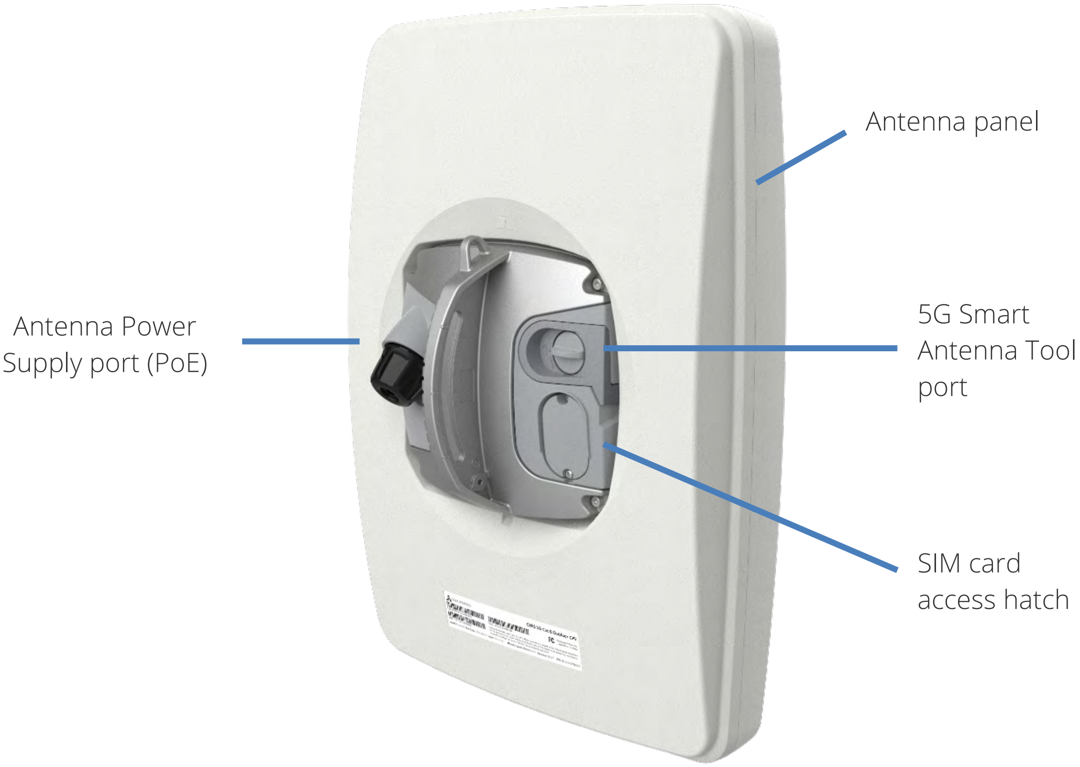


Figure 2 – Interfaces – CFW-2832

Item	Description
Antenna panel	Includes 2 x pairs Cross polarised antennas and GPS antenna
5G Smart Antenna Tool port	Connect the 5G Smart Antenna Tool here
SIM hatch	Open the hatch to insert SIM here
Antenna Power Supply port (PoE)	Provides power and data connectivity to the AurusPRO 5G Outdoor CPE with Ethernet cable

Table 2 – Interfaces – CFW-2832

3.3 Insert SIM card

All models in the AurusPRO Global 5G Outdoor CPE series employ SIM cards in Micro-SIM (2FF) format.

Follow the instructions below to insert a SIM card.

1. On the back of the AurusPRO, locate the SIM hatch. Using a screwdriver, unscrew the two screws on the SIM hatch then remove the cover to reveal the SIM card slot.

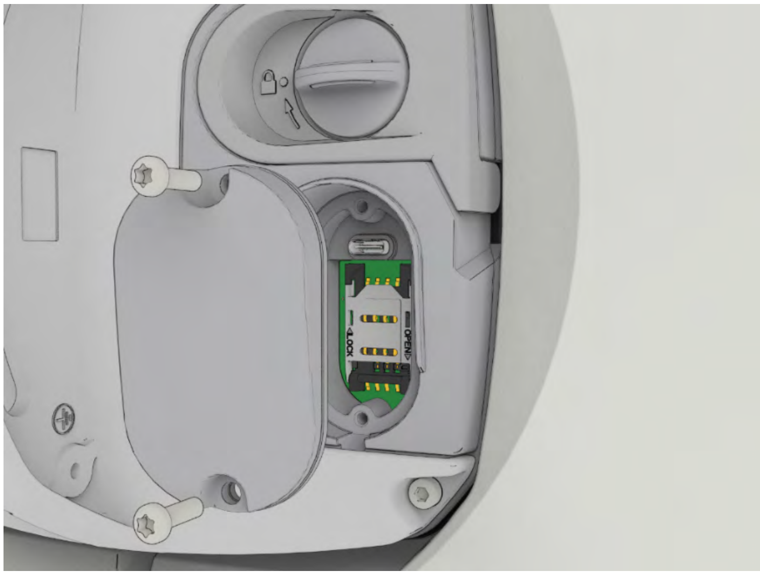


Figure 3 - Removing screws from the SIM hatch

Note – Screws used to fix the SIM hatch vary, may be: T10 torx or Pozidriv
Installer to provide correct screwdriver.

2. Swing the SIM card locking mechanism down to allow insertion of the SIM card.

3 Place the SIM card into the tray as shown below.

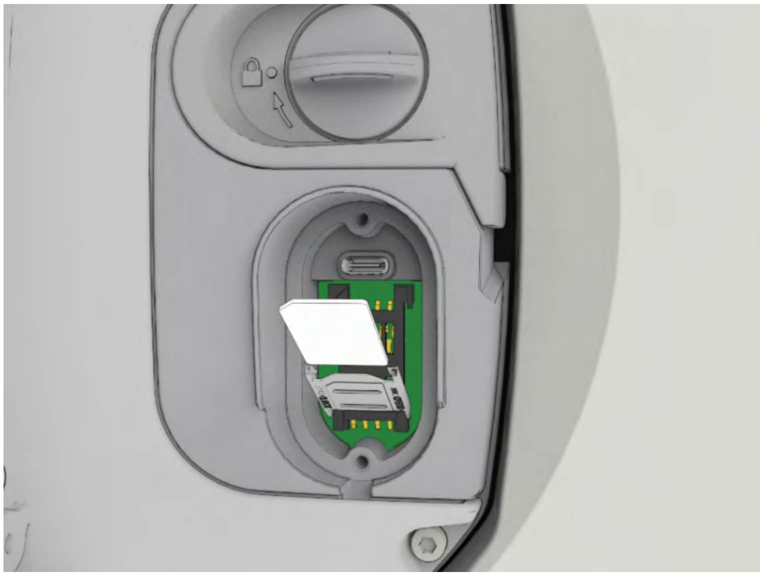


Figure 4 – Placing the SIM card into the SIM card reader

4 Swing the locking mechanism up and ensure that it clips into place to secure the SIM card.

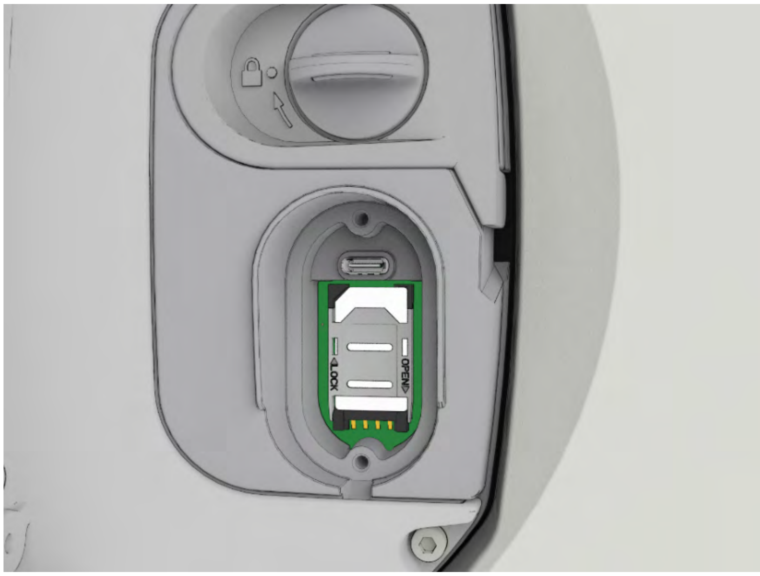


Figure 5 – SIM card locked in place

5 Replace the SIM hatch and seal, insert the two screws and firmly hand tighten them using a T10 torx or Pozidriv screwdriver.

3.4 Assemble and attach the mounting bracket

The AurusPRO Global 5G Outdoor CPE series of antennas use the same mounting bracket (MKIT-00011-000).

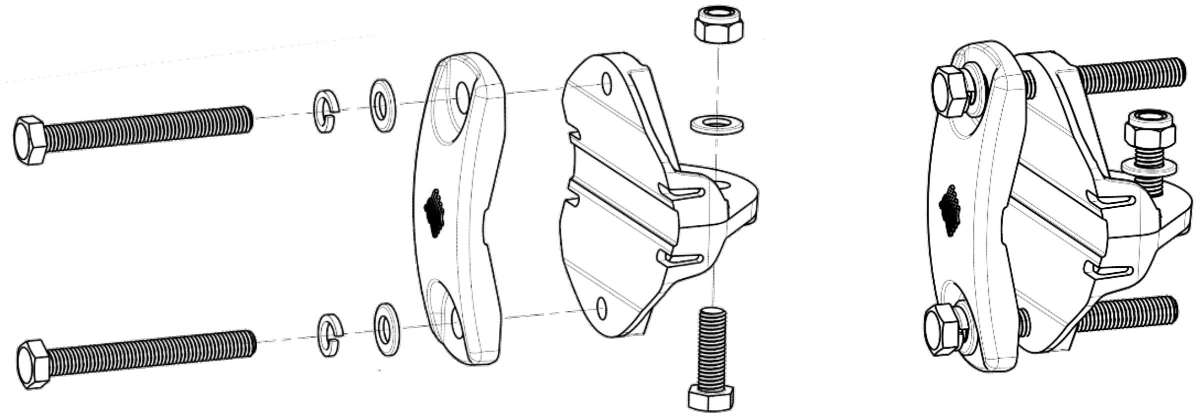


Figure 6 – Standard mounting bracket (MKIT-00011-000)

Note – Other types of mounting brackets are available, contact Casa Systems sales or product support if required..

3.4.1 Mounting bracket assembly instructions

1 Place the mast bracket onto the antenna housing as shown below.

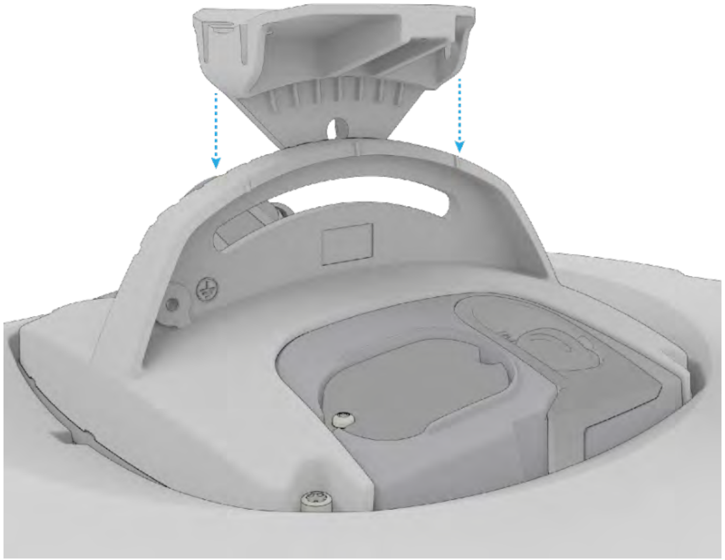


Figure 7 – Elevation control components

2 Insert the elevation setting bolt into the mast bracket, then place the washer and nut over the elevation setting bolt as shown below.

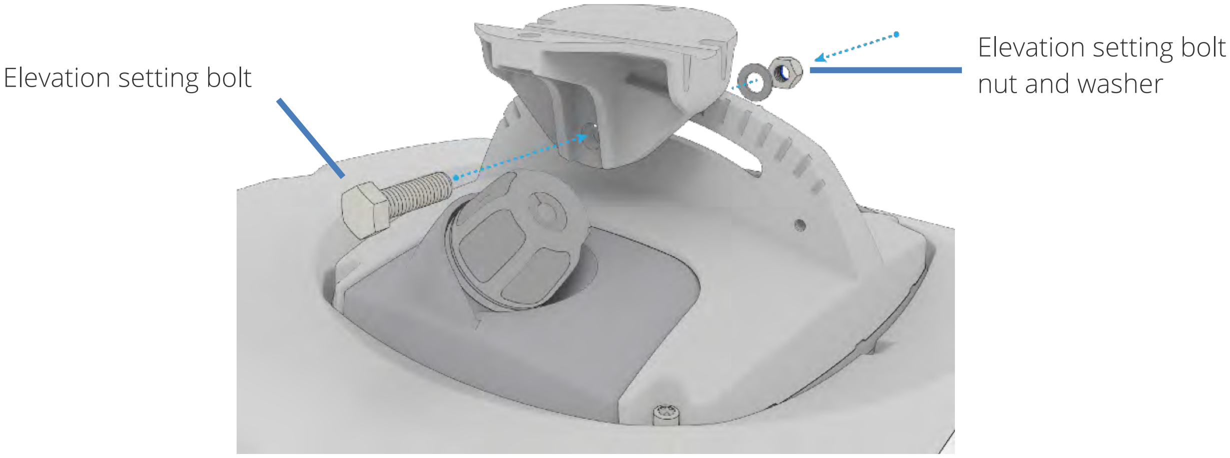


Figure 8 - Attaching the mounting bracket to the AurusPRO 5G Outdoor CPE

3 Tighten the lock nut so that the mast bracket and antenna housing do not swivel easily. Do not overtighten the elevation setting bolt as some adjustment may be required later.

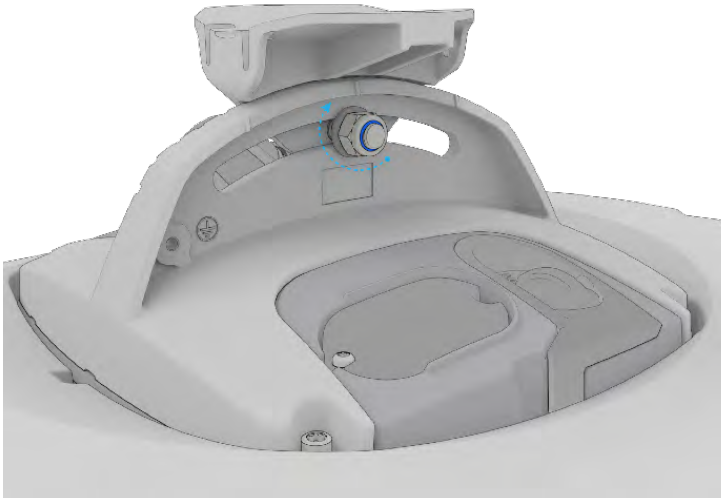


Figure 9 - Assembling mast bracket to mast

4 Alternately tighten the left and right bracket bolts to maintain even pressure on the pipe, to 65 in-lb.

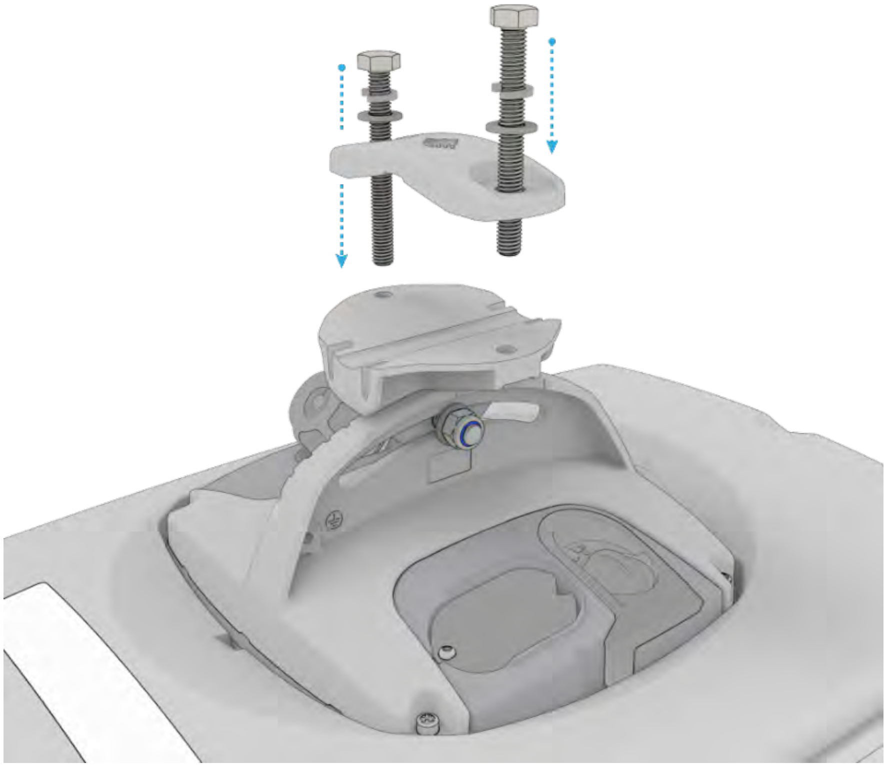


Figure 10 - Tightening bracket bolts

3.4.2 Overview of completed mounting

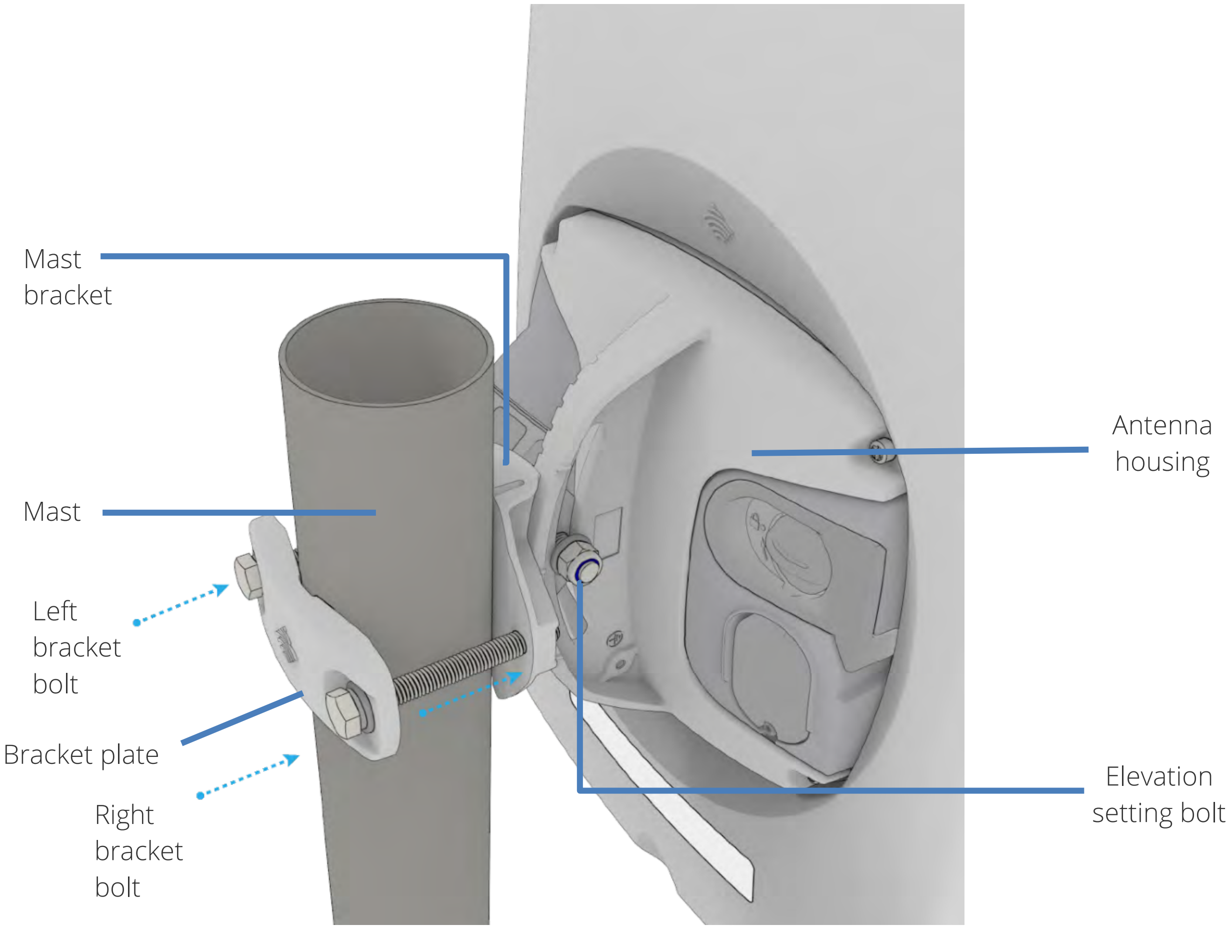


Figure 11 - CFW-2301 / CFW-2331 / CFW-2351 / CFW-2352 / CFW-2382 / CFW-2631 mounting bracket and bolts

Notes on mounting:

- Use a standard 13mm socket wrench for all bolts
- Tighten bolts to the following torque settings:
  - Elevation setting bolt: 7 Nm / 65 in-lbs
  - Left and right bracket bolts: 7 Nm / 65 in-lbs
- Do not over-tighten bolts

4 Installing the AurusPRO

The image below illustrates a typical installation of the AurusPRO 5G Outdoor CPE.

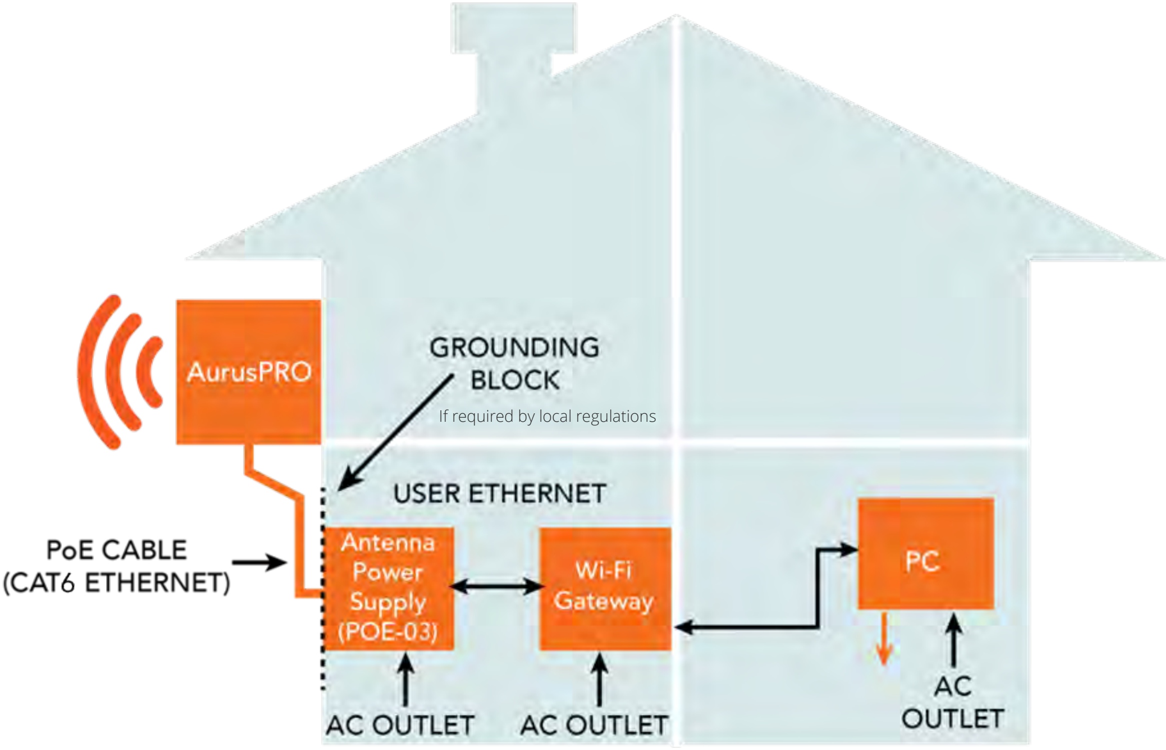

AurusPRO
GROUNDING BLOCK
If required by local regulations
USER ETHERNET
PoE CABLE (CAT6 ETHERNET)
Antenna Power Supply (POE-03)
Wi-Fi Gateway
PC
AC OUTLET
AC OUTLET
AC OUTLET

Figure 12 - Typical AurusPRO 5G Outdoor CPE installation

4.1.1 Installation considerations

⚠ Important – If local regulations require the use of a **CBRS Spectrum Access Server** then the AurusPRO Global 5G Outdoor CPE must be professionally installed by a **Certified Professional Installer (CPI)** in order to function.

As the AurusPRO 5G Outdoor CPE is aligned specifically for each individual property, please take note of the following when installing the equipment:

- The Antenna Power Supply (POE-03) and Wi-Fi Gateway must be installed in a well-ventilated area and near a dedicated power outlet which allows easy visibility of the indicator lights.
- Use a high-grade CAT6 Ethernet cable which is suitable for outdoor use as it will be partially exposed to the elements.
- The equipment must be protected from running water, steam and excessive heat and must be installed according to the guidelines in this document.

- Keep trees and branches away from the AurusPRO 5G Outdoor CPE.
- After alignment, do not move, place anything in front of, or adjust the position of the AurusPRO 5G Outdoor CPE since this will likely have a negative impact on the signal quality and performance of the wireless service.
- If construction work has been carried out on the exterior of the property, the antenna may need to be re-aligned to ensure the installation is still operating at peak performance.
- The AurusPRO 5G Outdoor CPE's location is determined by radio frequency performance and it may not be possible to relocate the antenna when moving to a new property. It is advised that a site survey be conducted before initiating the installation process.

4.2 Determine the best location for the AurusPRO

Determining the best location for the AurusPRO 5G Outdoor CPE involves:

1. Performing a survey of the site using the 5G Smart Antenna Tool and Aurus Installation application.
2. Consulting the customer about mounting location, grounding and cable routing based on results of the RF test, aesthetics and any planned renovations to the property.

   When selecting a location to mount the AurusPRO 5G Outdoor CPE, ensure that:

   - lock of the desired cell and optimal signal level is achieved.
   - the mounting position is unobtrusive and aesthetically pleasing where possible.
   - the mount/antenna is not closer than three feet from other antenna equipment.
   - the customer has obtained local planning authority/homeowner association/zoning approval for installation if required. This is the sole responsibility of the customer.

   Where possible, avoid mounting the AurusPRO 5G Outdoor CPE so that it is aimed back over the roof of the property.

4.3 5G Smart Antenna Tool

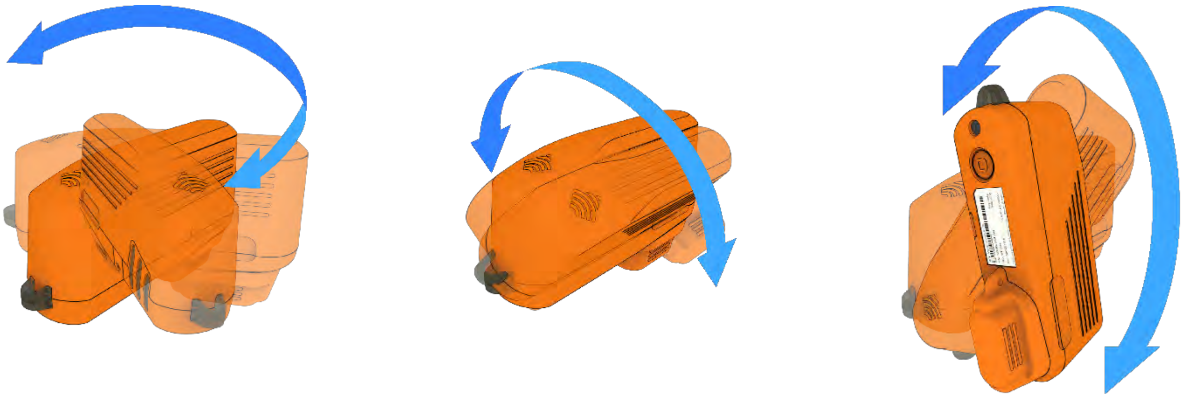
Use a fully charged 5G Smart Antenna Tool to support site survey with the companion application for the best signal from a nearby cell tower.

Push the power button on the 5G Smart Antenna Tool to turn it on.

After a few seconds, the LEDs illuminate. On each start up, the 5G Smart Antenna Tool LEDs flash both red and green twice a second, indicating that the compass requires calibrating.

4.3.1 Calibration

To calibrate the device, first isolate it from any magnetic field or metal structures (for example, vehicles, the antenna pole, power lines, etc) and then slowly and steadily rotate the unit fully through all three axes. See the diagrams below.



The LEDs stop flashing when calibration has been performed successfully.

4.4 Connect the 5G Smart Antenna Tool to the AurusPRO

⚠ Important – The AurusPRO's Ethernet power cable **SHOULD NOT BE CONNECTED** to the Antenna Power Supply (POE-03) during this scanning process.

The power required during the scanning process will be supplied by the 5G Smart Antenna Tool.

Ensure that the 5G Smart Antenna Tool's battery is fully charged before commencing the scanning process.

1 Turn the plug on the console port hatch counter-clockwise so that it is in the unlocked (vertical) position as shown in the image below.

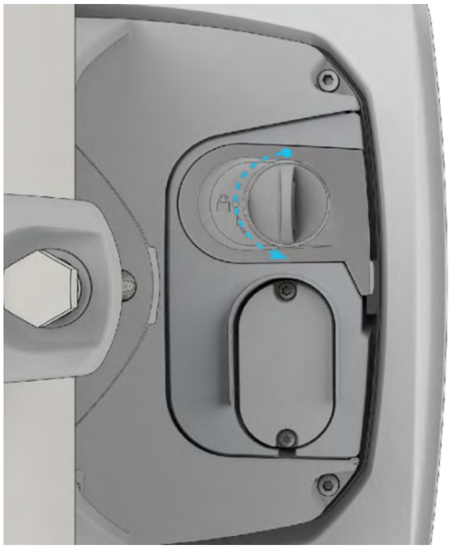


Figure 13 - Unlocked console port hatch

2 Pull the plug out to reveal the console port.

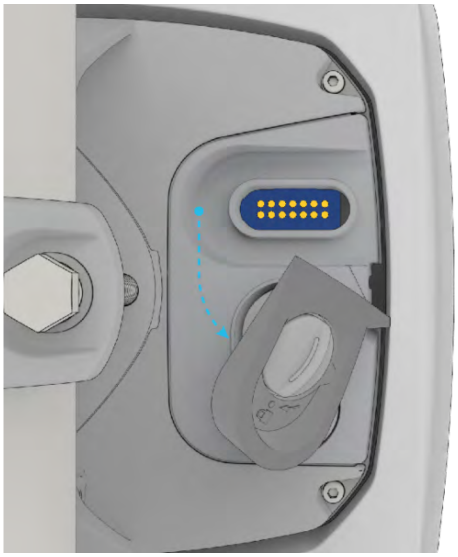


Figure 14 - Console port

3 Remove the cap from the head of the 5G Smart Antenna Tool and insert it into the console port as shown in the picture below.

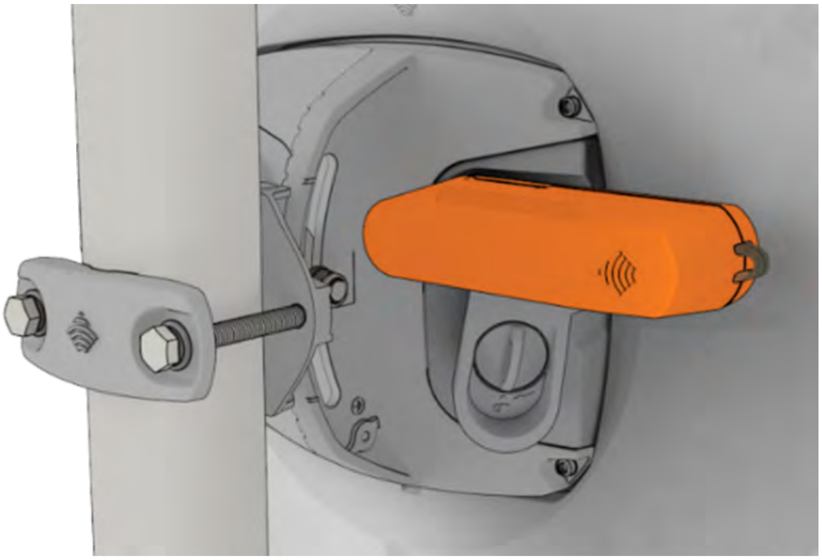


Figure 15 - Attached 5G Smart Antenna Tool

4.5 Perform site survey and installation

1 Pair your smartphone to the 5G Smart Antenna Tool over Bluetooth. The Bluetooth ID is printed on the label of the 5G Smart Antenna Tool.

2 Open the Installation app and follow the instructions in the app to complete the installation.

4.6 Fix to mounting

When you have found the best spot to install the AurusPRO, install the mount (pole, j-mount, etc.) using appropriate materials.

Securely fix the antenna to the mount facing the direction as indicated by the app, refer to section *3.4.2 Overview of completed mounting*, above, for additional mounting details.

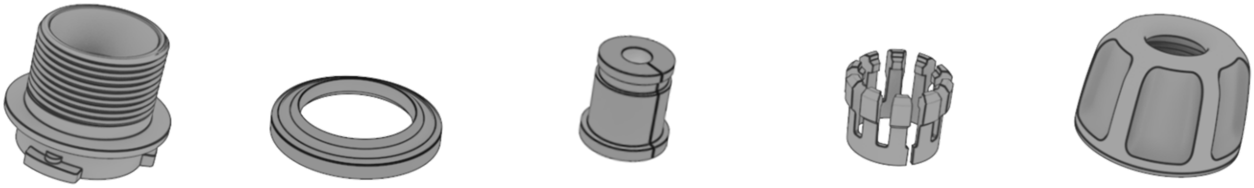
4.7 Antenna power supply weather seal

The AurusPRO power supply weather seal must be properly attached to prevent dust and water from entering the AurusPRO's housing.

To connect a PoE Ethernet cable through the power supply weather seal:

1. The power supply weather seal is shipped assembled and screwed into the AurusPRO 5G Outdoor CPE antenna housing.

   The five components of the weather seal assembly have to be separated in order to pass the cable through the weather seal during the installation process.



Body *Sealing washer* *Cable seal* *Collar* *Clamp*

Figure 16 - Weather seal in five parts

   Disassemble weather seal as follows:

   a Twist the assembled weather seal counter-clockwise to remove it from the antenna housing.

   b Unscrew the clamp from the body and remove the sealing washer and the collar and cable seal assembly from inside the clamp.

   c Separate the cable seal and collar.

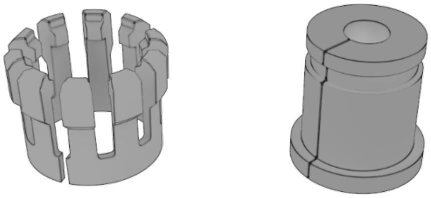


Figure 17 - collar and cable seal

2 Push the Ethernet cable through the hole in the clamp, as shown below.

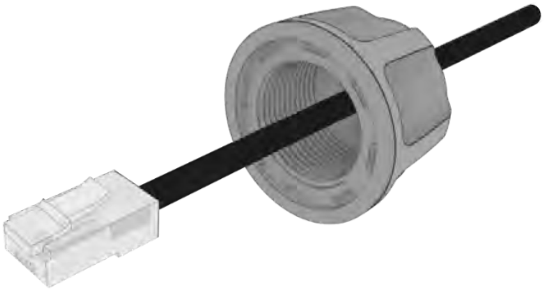


Figure 18 - Ethernet cable passed through clamp

3 Place the collar over the Ethernet cable as shown, making sure that the “teeth” are facing the clamp.

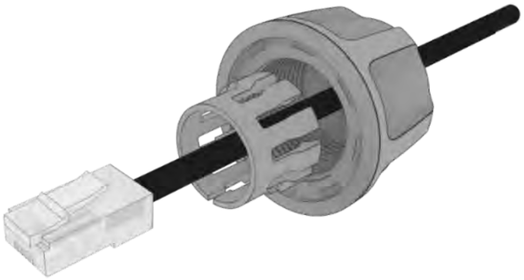


Figure 19 – Collar placed over Ethernet cable

4 Pry open the split in the rubber and place the cable seal over the Ethernet cable with the wide end toward the RJ45 plug and away from the collar and clamp. See the image below for the correct orientation.

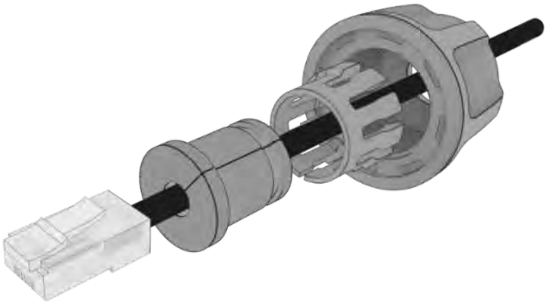


Figure 20 - Cable seal placed over Ethernet cable

Note – The rubber cable seal has a split that may be difficult to detect. If the split is not obvious, roll the cable seal between your fingers to crack the split so that you can slip it over the cable.

Do not use a sharp blade to open the split or cut another.

5 Push the collar over the cable seal to prevent it from coming apart (the “teeth” will fit into an indentation near the clamp end of the cable seal).

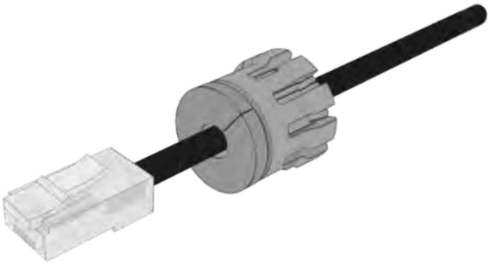


Figure 21 – Collar placed over the cable seal

6 Place the sealing washer over the Ethernet cable as shown below.

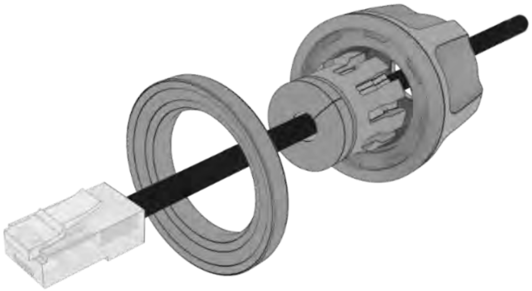


Figure 22 – Sealing washer placed over Ethernet cable

⚠ Important – Ensure that the side of the sealing washer with a protruding inside lip is facing the clamp and the side with an protruding outside lip faces the body.

7 Push the Ethernet cable through the body as shown below.

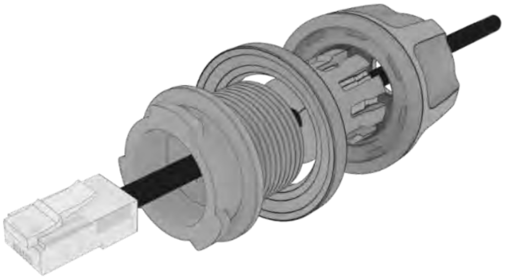


Figure 23 - Body placed over Ethernet cable

8 Plug the Ethernet cable into the Ethernet port of the CPE.

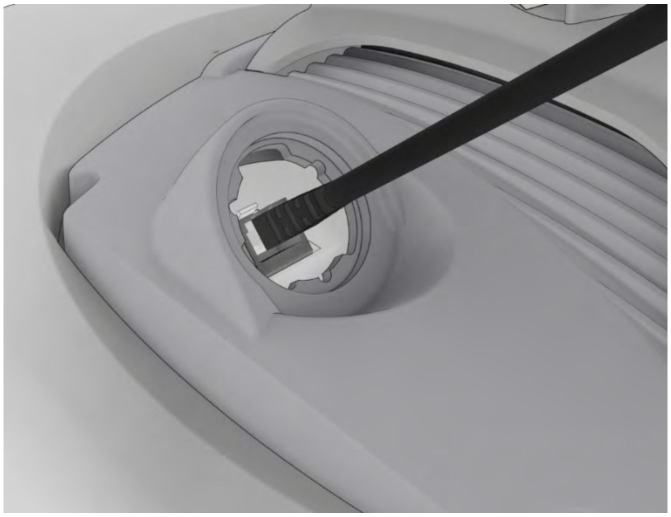


Figure 24 - Plugging in the Ethernet cable

9 Put the body into the opening on the CPE antenna housing and turn the body clockwise until it locks in place.

10 Push the cable seal and collar along the Ethernet cable into the body.

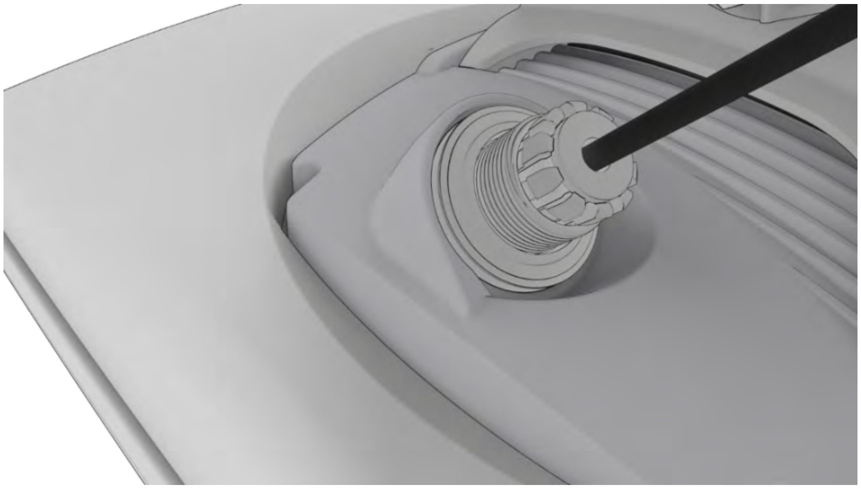


Figure 25 - Cable seal and collar inserted into neck

11 Turn the clamp clockwise to tighten the sealing washer against the housing and to allow the cable seal and collar to compress and grip the cable to prevent dust and moisture entering the unit. Continue turning the clamp until tightly assembled.

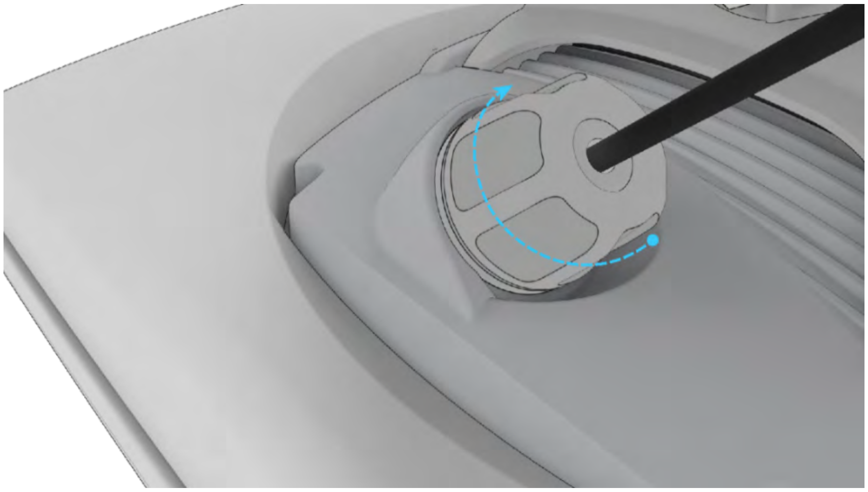


Figure 26 - Turn the clamp clockwise until tight

5 Setting up the AurusPRO

The AurusPRO Global 5G Outdoor CPE series of antennas use the same firmware.

The AurusPRO comes with pre-configured settings that should suit most customers.

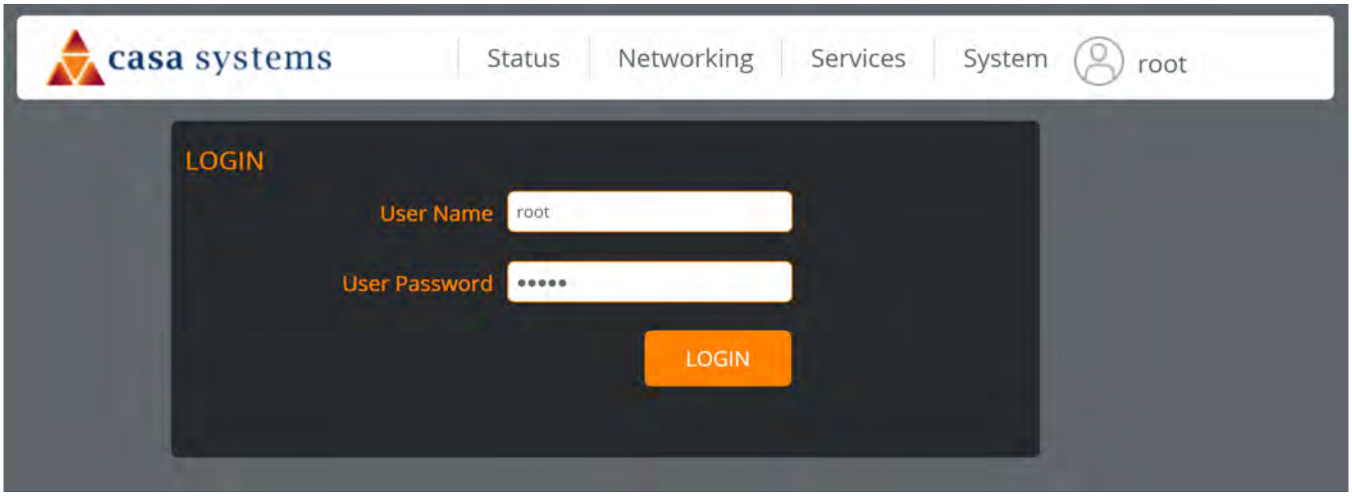
For advanced configuration, log in to the web-based user interface of the AurusPRO as an administrator.

5.1 Log in as Administrator via Web UI

To log in to the web-based user interface:

1 Open a web browser (e.g. Chrome, Safari, etc.), type http://192.168.1.1 into the address bar and press **Enter**.

2 The web-based user interface **Login** screen is displayed.



LOGIN

User Name: root

User Password: •••••

Figure 27 – Log in prompt for the web-based user interface

3 Enter the login **User Name** and **User Password**.

Administrator account

User Name	root
User Password	admin

Table 3 - Management account login details – Administrator account

5.2 Confirming a successful connection

To confirm the connection status, click the **Status** menu item at the top of the page to display the **Status** page. Select the **CELLULAR CONNECTION STATUS** and **WWAN CONNECTION STATUS** items to expand them.

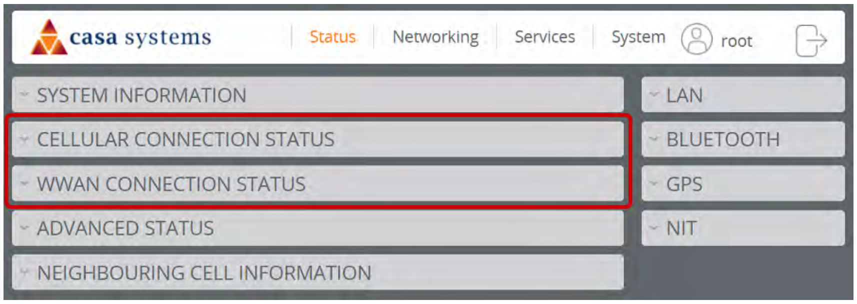
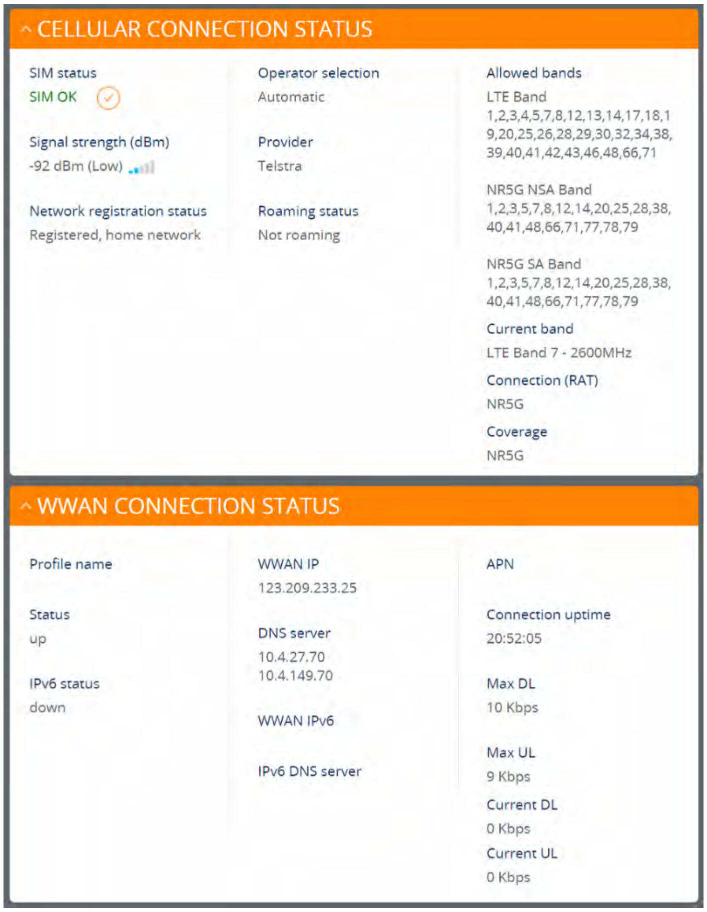


Figure 28 - Main menu items

The details of the connection are displayed.



CELLULAR CONNECTION STATUS

SIM status
SIM OK ✓

Signal strength (dBm)
-92 dBm (Low)

Network registration status
Registered, home network

Operator selection
Automatic

Provider
Telstra

Roaming status
Not roaming

Allowed bands
LTE Band
1,2,3,4,5,7,8,12,13,14,17,18,19,20,25,26,28,29,30,32,34,38,39,40,41,42,43,46,48,66,71

NR5G NSA Band
1,2,3,5,7,8,12,14,20,25,28,38,40,41,48,66,71,77,78,79

NR5G SA Band
1,2,3,5,7,8,12,14,20,25,28,38,40,41,48,66,71,77,78,79

Current band
LTE Band 7 - 2600MHz

Connection (RAT)
NR5G

Coverage
NR5G

WWAN CONNECTION STATUS

Profile name

Status
up

IPv6 status
down

WWAN IP
123.209.233.25

DNS server
10.4.27.70
10.4.149.70

WWAN IPv6

IPv6 DNS server

APN

Connection uptime
20:52:05

Max DL
10 Kbps

Max UL
9 Kbps

Current DL
0 Kbps

Current UL
0 Kbps

Figure 29 - Cellular Connection Status and WWAN Connection Status

If the device is connected, the **Status** field displays "**up**".

6 User interface

The AurusPRO features a user interface with top and left-sided menus. The menu across the top of the screen is the highest-level menu.

There are four main menu items: Status, Networking, Services and System

The Networking, Services and System menus each feature a submenu on the left of the screen that allow you to navigate to different features within that area.

The Status screen is somewhat different in that it contains various windows which can be expanded to display information about the device.

6.1 Status

The Status page of the web interface provides system related information and is displayed when you log in to the AurusPRO management console.

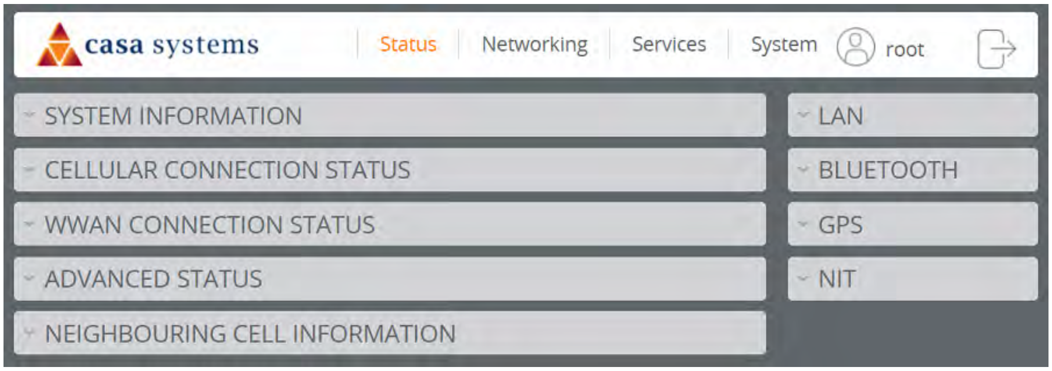


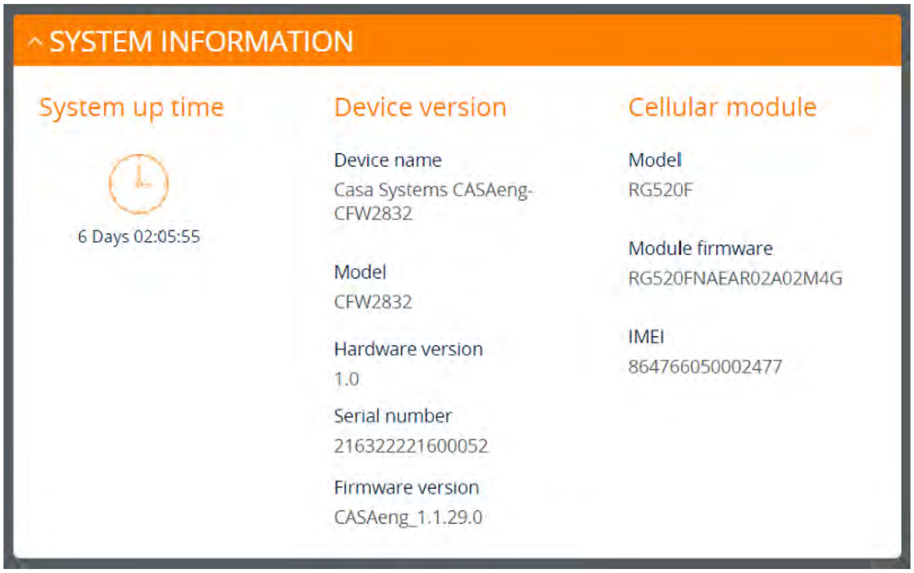
Figure 30 - The Status menu page upon first log in

The status page has links to pages displaying

- SYSTEM INFORMATION
- CELLULAR CONNECTION STATUS
- WWAN CONNECTION STATUS
- ADVANCED STATUS
- NEIGBOURING CELL INFORMATION
- LAN details
- BLUETOOTH MAC address details
- GPS connection details
- NIT Smart Antenna Tool readings

Toggle the display of the sections by clicking the ⌄ or ⌃ buttons to show or hide them.

6.1.1 System information



SYSTEM INFORMATION

System up time

6 Days 02:05:55

Device version

Device name
Casa Systems CASAeng-CFW2832

Model
CFW2832

Hardware version
1.0

Serial number
216322221600052

Firmware version
CASAeng_1.1.29.0

Cellular module

Model
RG520F

Module firmware
RG520FNAEAR02A02M4G

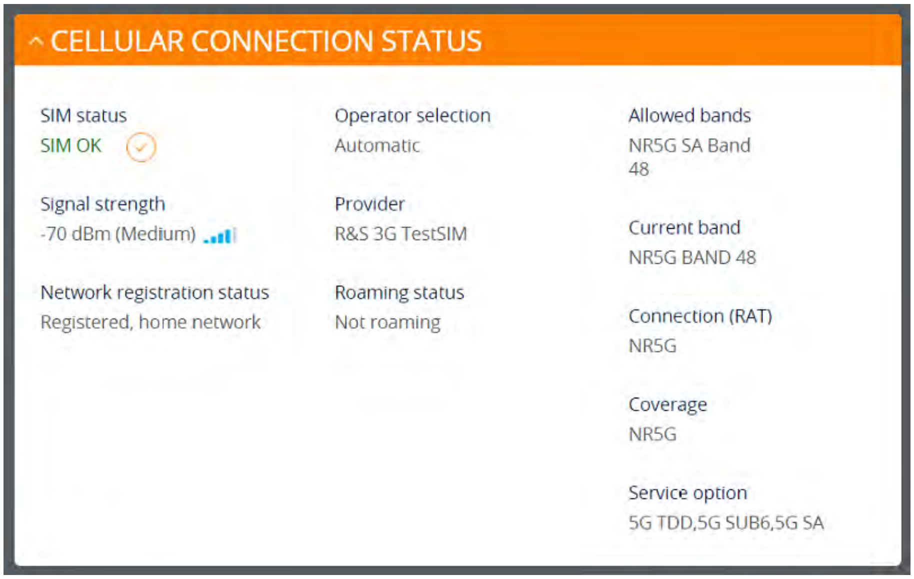
IMEI
864766050002477

Figure 31 - System Information

System Information	
System up time	The current uptime of the AurusPRO.
Device name	The manufacturer's name of this device.
Model	The manufacturer's model number.
Hardware version	The hardware version of the AurusPRO.
Serial Number	The serial number of the AurusPRO.
Firmware version	The firmware version of the AurusPRO
Model	The type of phone module
Module firmware	The firmware revision of the phone module.
IMEI	The International Mobile Station Equipment Identity number used to uniquely identify a mobile device.

Table 4 - System Information fields

6.1.2 Cellular connection status



CELLULAR CONNECTION STATUS

SIM status
SIM OK ✓

Signal strength
-70 dBm (Medium)

Network registration status
Registered, home network

Operator selection
Automatic

Provider
R&S 3G TestSIM

Roaming status
Not roaming

Allowed bands
NR5G SA Band 48

Current band
NR5G BAND 48

Connection (RAT)
NR5G

Coverage
NR5G

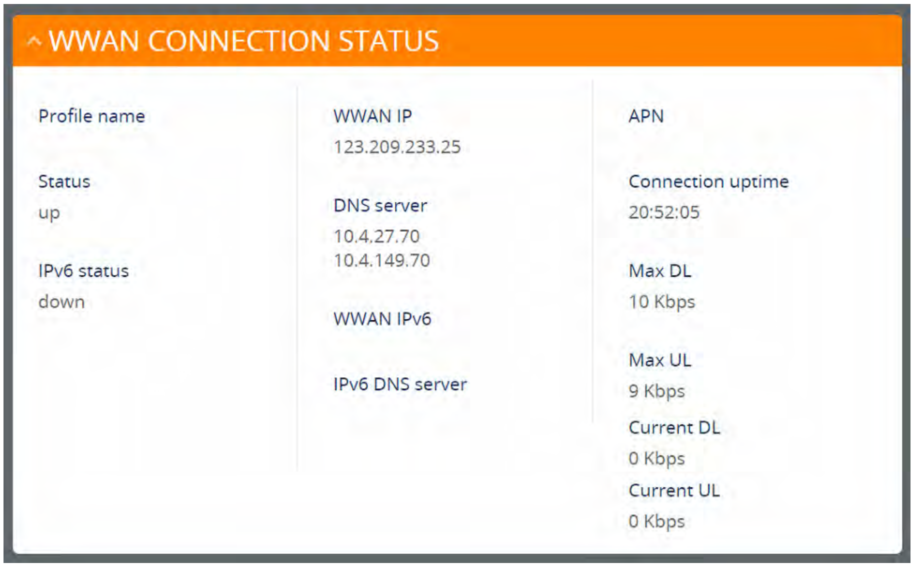
Service option
5G TDD,5G SUB6,5G SA

Figure 32 - Cellular Connection Status

Cellular Connection Status	
SIM status	Displays the activation status of the AurusPRO on the carrier network.
Signal strength (dBm)	The current signal strength measured in dBm.
Network registration status	The status of the AurusPRO's registration for the current network.
Operator selection	The mode used to select an operator network.
Provider	The current operator network in use.
Roaming status	The roaming status of the AurusPRO.
Allowed bands	The bands to which the AurusPRO may connect.
Current band	The current band being used by the AurusPRO.
Coverage	The type of mobile coverage being received by the AurusPRO.

Table 5 - Cellular Connection Status fields

6.1.3 WWAN connection status



WWAN CONNECTION STATUS

Profile name

Status
up

IPv6 status
down

WWAN IP
123.209.233.25

DNS server
10.4.27.70
10.4.149.70

WWAN IPv6

IPv6 DNS server

APN

Connection uptime
20:52:05

Max DL
10 Kbps

Max UL
9 Kbps

Current DL
0 Kbps

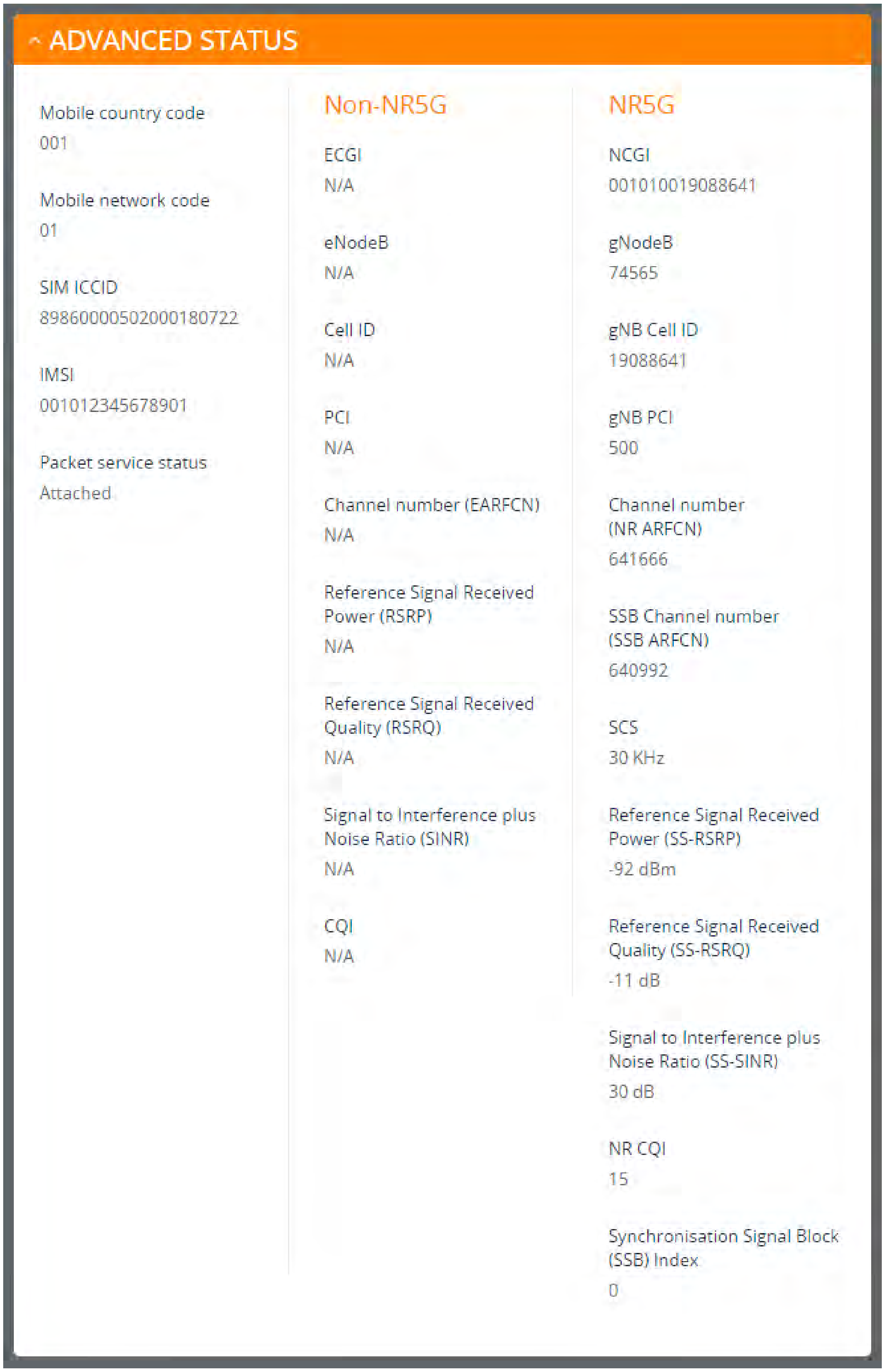
Current UL
0 Kbps

Figure 33 - WWAN Connection Status

WWAN Connection Status	
Profile name	The name of the active profile.
Status	The IPv4 connection status of the active profile.
IPv6 status	The IPv6 connection status of the active profile.
WWAN IP	The IPv4 address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary IPv4 DNS servers for the WWAN connection.
WWAN IPv6	The IPv6 address assigned by the mobile broadband carrier network.
IPv6 DNS server	The primary and secondary IPv6 DNS servers for the WWAN connection.
APN	The Access Point Name currently in use.
Connection uptime	The length of time of the current mobile connection session.
Max DL	Maximum download speed in Kbps (Kilobits Per Second)
Max UL	Minimum upload speed in Kbps (Kilobits Per Second)
Current DL	Current download speed in Kbps (Kilobits Per Second)
Current UL	Current upload speed in Kbps (Kilobits Per Second)

Table 6 - WWAN Connection Status fields

6.1.4 Advanced status



ADVANCED STATUS

Mobile country code
001

Mobile network code
01

SIM ICCID
89860000502000180722

IMSI
001012345678901

Packet service status
Attached

Non-NR5G

ECGI
N/A

eNodeB
N/A

Cell ID
N/A

PCI
N/A

Channel number (EARFCN)
N/A

Reference Signal Received Power (RSRP)
N/A

Reference Signal Received Quality (RSRQ)
N/A

Signal to Interference plus Noise Ratio (SINR)
N/A

CQI
N/A

NR5G

NCGI
001010019088641

gNodeB
74565

gNB Cell ID
19088641

gNB PCI
500

Channel number (NR ARFCN)
641666

SSB Channel number (SSB ARFCN)
640992

SCS
30 KHz

Reference Signal Received Power (SS-RSRP)
-92 dBm

Reference Signal Received Quality (SS-RSRQ)
-11 dB

Signal to Interference plus Noise Ratio (SS-SINR)
30 dB

NR CQI
15

Synchronisation Signal Block (SSB) Index
0

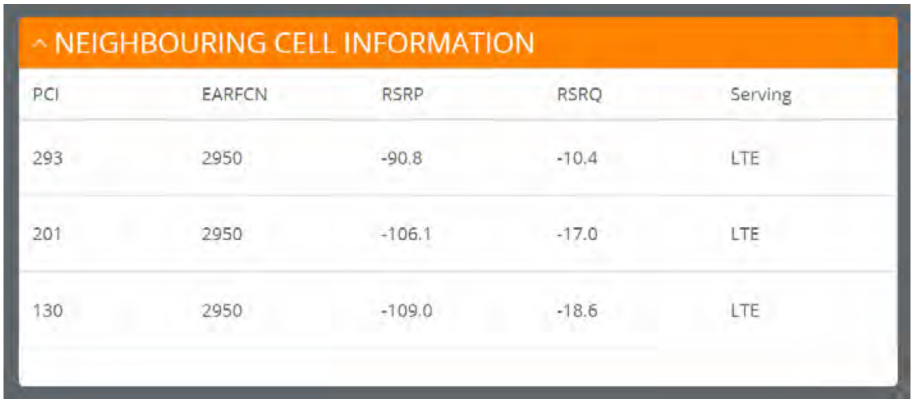
Figure 34 - Advanced Status

Advanced status	
Mobile country code	The Mobile Country Code (MCC) of the AurusPRO.
Mobile network code	The Mobile Network Code (MNC) of the AurusPRO.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the AurusPRO, a unique number up to 19 digits in length.
IMSI	The International Mobile Subscriber Identity is a unique identifier of the user of a cellular network.
Packet service status	Displays whether the packet service is attached or detached. When APN or username/password is changed, the device detaches and reattaches to the network.
Non-NR5G	
ECGI	E-UTRAN Cell Global Identifier. The globally unique identity of a cell in E-UTRA. The ECGI concatenates the PLMN-Id and the ECI (E-UTRAN Cell Identifier). The ECI concatenates the eNodeB ID and the Cell ID
eNodeB	Also known as the Evolved Node B, this is the hardware element in the LTE network that communicates directly with mobile devices.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile LTE network signal.
PCI	Physical Cell ID of the LTE Cell.
Channel number (EARFCN)	The channel number of the current cellular connection.
Reference Signal Received Power (RSRP)	A cell-specific reference signal used to determine RSRP.
Reference Signal Received Quality (RSRQ)	RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by N x RSRP / RSSI where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.
CQI	Channel Quality Indicator. This is a value between 1 and 15 with 15 being the highest rating.
Scell band	The frequency band of the Scell.
Scell PCI	The Physical Layer Cell Identity (PCI) of the Scell.
Scell channel number (EARFCN)	The E-UTRA Absolute Radio Frequency Channel Number (EARFCN) will uniquely identify the LTE band and carrier frequency.
NR5G	
NCGI	NR Cell Global Identifier. This concatenates the PLMN-Id (PLMN Identifier) and the 36bit NCI (NR Cell Identity). This information is not available when the device is operating in LTE or 5G Non-Standalone mode.

gNodeB	The gNodeB (gNB) is the term given to network equipment that transmits and receives wireless communications between UE and a mobile network
gNB CellID	A unique code that identifies the base station from within the location area of the current mobile 5G network signal. This is not available when the device is operating in LTE or 5G Non-Standalone mode.
gNB PCI	Physical Cell ID of the 5G NR Cell.
Channel number NR ARFCN)	The channel number of the current 5G cellular connection.
Reference Signal Received Power (SS-RSRP)	Synchronisation Signal Reference Signal Received Power (SS-RSRP). The linear average over the power contributions (in Watts) of the resource elements that carry Secondary Synchronisation Signal (SSS).
Reference Signal Received Quality (SS-RSRQ)	Secondary Synchronisation Signal Reference Signal Received Quality. SS-RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by N x SS-RSRP / NR carrier RSSI where N is the number of Physical Resources Blocks (PRBs) over which the NR RSSI is measured.
NR CQI	The 5G NR Channel Quality Indicator (CQI).
Synchronisation Signal Block (SSB) Index	This is a key part of beam management. It is a value comprised of Primary Synchronisation Signal (PSS), Secondary Synchronisation Signal (SSS) and the Physical Broadcast Channel (PBCH).

Table 7 - Advanced Status fields

6.1.5 Neighbouring cell information



NEIGHBOURING CELL INFORMATION

PCI	EARFCN	RSRP	RSRQ	Serving
293	2950	-90.8	-10.4	LTE
201	2950	-106.1	-17.0	LTE
130	2950	-109.0	-18.6	LTE

Figure 35 - Cell Information

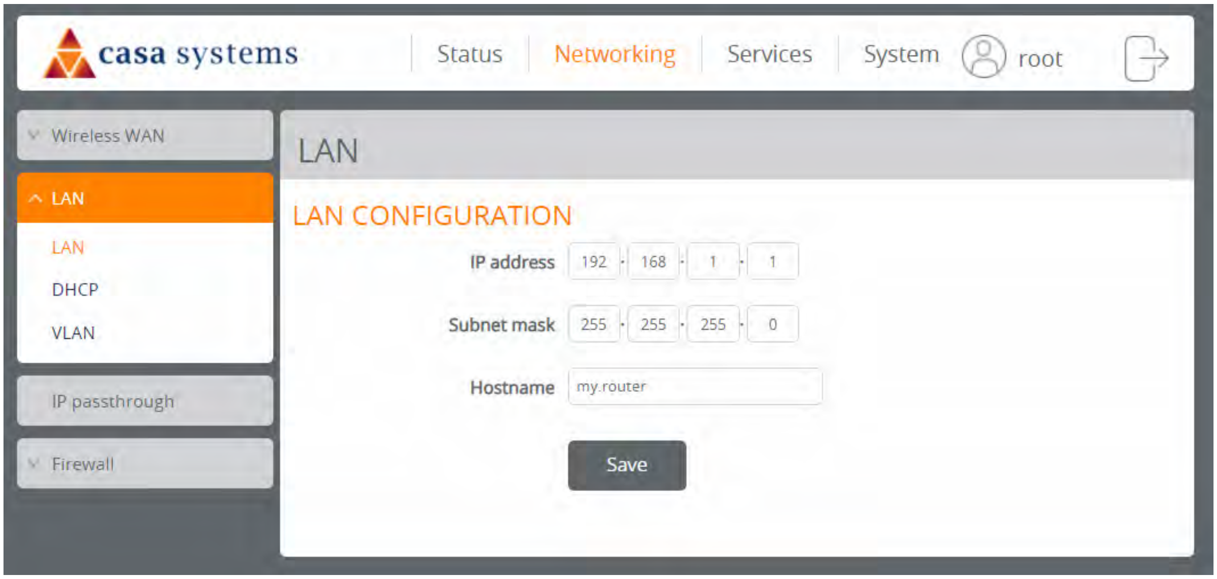
Neighbouring cell Information

PCI	The Physical Cell ID.
EARFCN	E-UTRA Absolute Radio Frequency Channel Number. Uniquely identifies the LTE Band and carrier frequency.

RSRP	Reference Signal Received Power (RSRP).
RSRQ	Reference Signal Received Quality (RSRQ).
Serving	The radio signal being served e.g. 5G NR, LTE.

Table 8 - Cell Information fields

LAN



LAN CONFIGURATION

IP address 192 . 168 . 1 . 1

Subnet mask 255 . 255 . 255 . 0

Hostname my.router

Figure 36 - LAN Information

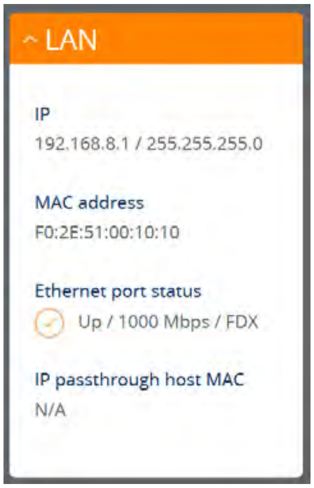
LAN configuration

IP	The IP address of the AurusPRO.
Subnet mask	The subnet mask of the AurusPRO.
Hostname	The label used to identify the device.

Table 9 - LAN Information fields

6.1.6 LAN

Click the LAN submenu under LAN to view the LAN connection information.



^ LAN

IP
192.168.8.1 / 255.255.255.0

MAC address
F0:2E:51:00:10:10

Ethernet port status
✓ Up / 1000 Mbps / FDX

IP passthrough host MAC
N/A

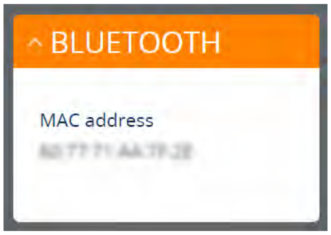
Figure 37 - LAN Information

LAN

IP	The IP address and subnet mask of the AurusPRO.
MAC address	The MAC address of the AurusPRO.
Ethernet port status	Displays the current status of the Ethernet port and its operating speed.
IP passthrough host MAC	The MAC address of the connected gateway.

Table 10 - LAN Information fields

6.1.7 Bluetooth



^ BLUETOOTH

MAC address
[redacted]

Figure 38 - Bluetooth Information

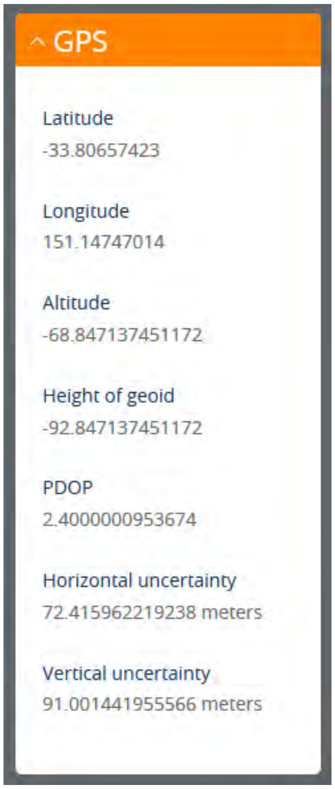
Bluetooth

MAC address	The MAC address of the Bluetooth module.

Table 11 - Bluetooth Information fields

6.1.8 GPS

When a Global Positioning System signal is accessed, its details will display in the GPS page.



^ GPS

Latitude
-33.80657423

Longitude
151.14747014

Altitude
-68.847137451172

Height of geoid
-92.847137451172

PDOP
2.4000000953674

Horizontal uncertainty
72.415962219238 meters

Vertical uncertainty
91.001441955566 meters

Figure 39 - GPS signal Information

GPS	
Latitude	The angular distance of a place north or south of the earth's equator, usually expressed in degrees and minutes
Longitude	The angular distance of a place east or west of the Greenwich meridian, usually expressed in degrees and minutes.
Altitude	The height of an object or point in relation to sea level or ground level.
Height of geoid	The height of an object from sea level if the Earth was under the influence of gravity and its own rotation alone.
PDOP	Position Dilution of Precision. Possible error in location due to GPS satellite location.
Horizontal uncertainty	Possible error in horizontal (latitude/longitude) location due to GPS satellite location.
Vertical uncertainty	Possible error in altitude location due to GPS satellite location.

Table 12 - GPS signal Information fields

6.1.9 NIT

Click the **NIT** to view the antenna's **Azimuth** and **Downtilt** values as measured by the Smart Antenna Tool.

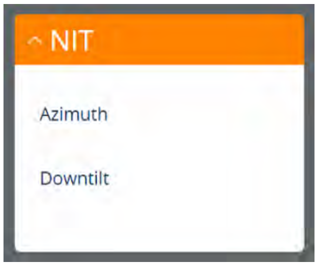


Figure 40 – NIT Information

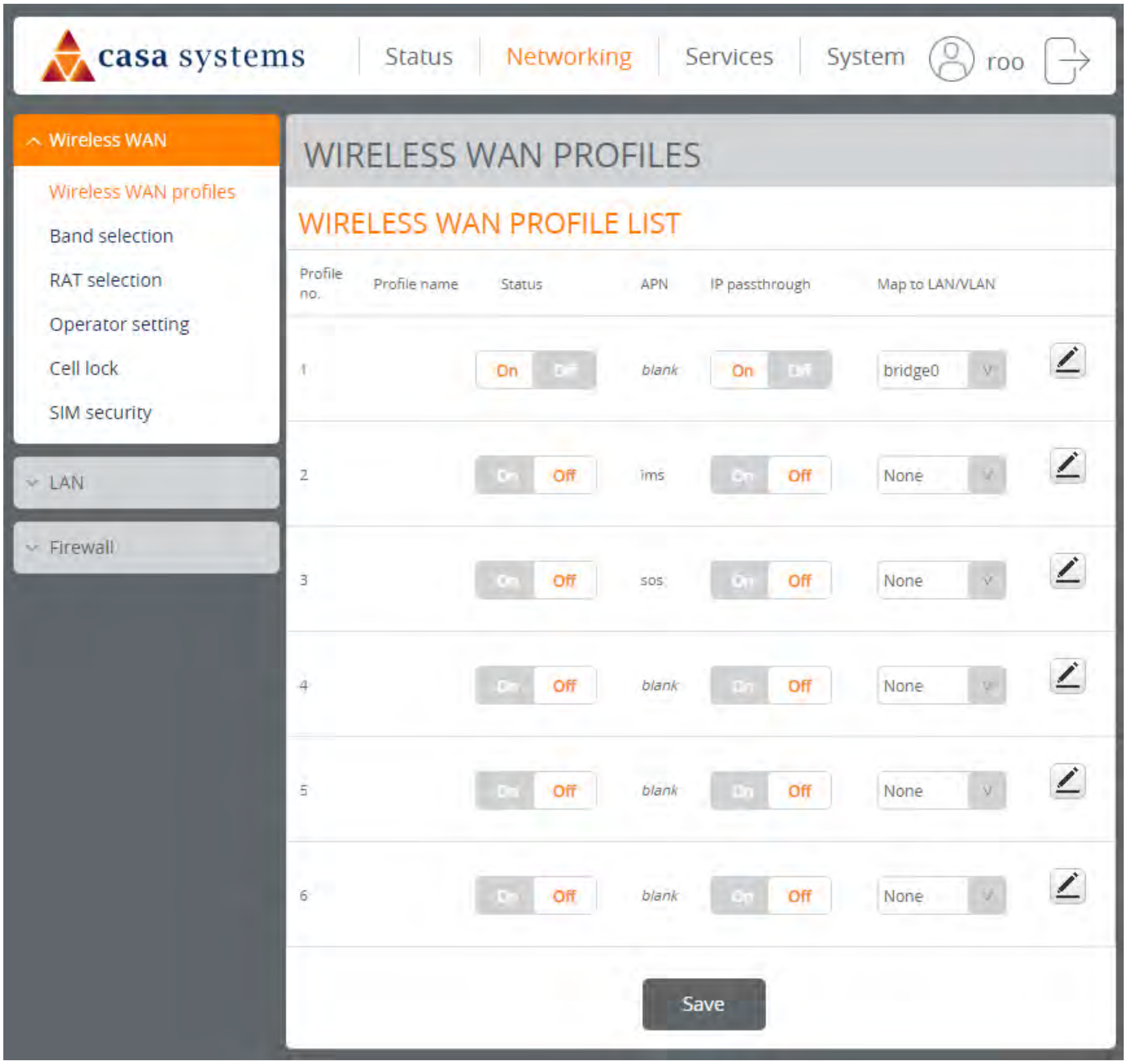
6.2 Networking

6.2.1 Wireless WAN

6.2.1.1 Wireless WAN profiles

⚠ Important – Changing any of these settings can cause the AurusPRO to lose Internet connectivity. Please do not change any of these settings unless instructed to do so.

The **Wireless WAN profiles** page allows you to configure and enable/disable connection profiles. To access this page, click the **Networking** menu, and then select **Wireless WAN profiles** from the menu on the left.



WIRELESS WAN PROFILES

WIRELESS WAN PROFILE LIST

Profile no.	Profile name	Status	APN	IP passthrough	Map to LAN/VLAN
1		On	*blank*	On	bridge0
2		Off	ims	Off	None
3		Off	sos	Off	None
4		Off	*blank*	Off	None
5		Off	*blank*	Off	None
6		Off	*blank*	Off	None

Table 13 - Wireless WAN Profiles page

Each profile refers to a set of configuration items which are used by the AurusPRO to activate a Packet Data (PDP) context. Under normal scenarios, you may have a single profile enabled.

Multiple profiles can be used for simple fast switching of PDP settings such as APN, or for advanced networking configuration where multiple simultaneous PDP contexts may be required. Use the **Status On/Off** button to select the profile to use.

Use the **IP Passthrough On/Off** button to allow or restrict IP Passthrough when the respective profile is in use.

Specify the path to map from LAN to VLAN in the **Map to LAN/VLAN** drop down menu. The options are: **None, bridge0** or a **VLAN**

ⓘ Note – When mapping a profile to the LAN, "**Bridge0**" should be chosen.

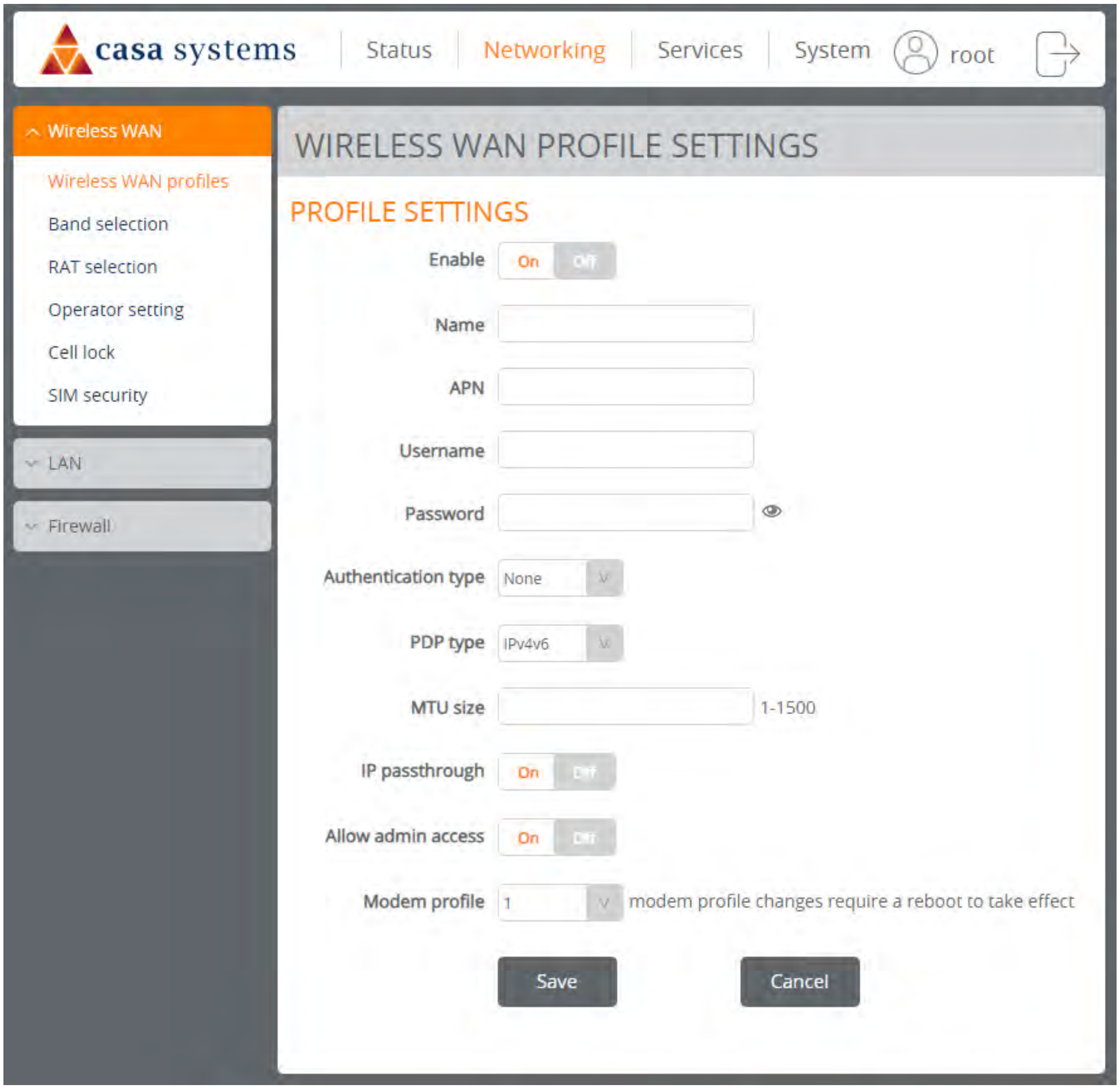
⚠ Important – The **same VLAN MUST NOT be used in multiple profiles**, even if the other profile or profiles are not enabled.

The **Profilename** and **APN** are defined when the Wireless WAN profile settings are configured, see next section.

Configuring a Wireless WAN profile

1 Click the edit ✎ button corresponding to the **Profile** that you wish to create or modify.

2 The **Wireless WAN Profile settings** page is displayed.



WIRELESS WAN PROFILE SETTINGS

PROFILE SETTINGS

Enable: On Off

Name:

APN:

Username:

Password:

Authentication type: None

PDP type: IPv4v6

MTU size: 1-1500

IP passthrough: On Off

Allow admin access: On Off

Modem profile: 1 modem profile changes require a reboot to take effect

Figure 41 - Wireless WAN Profile Settings

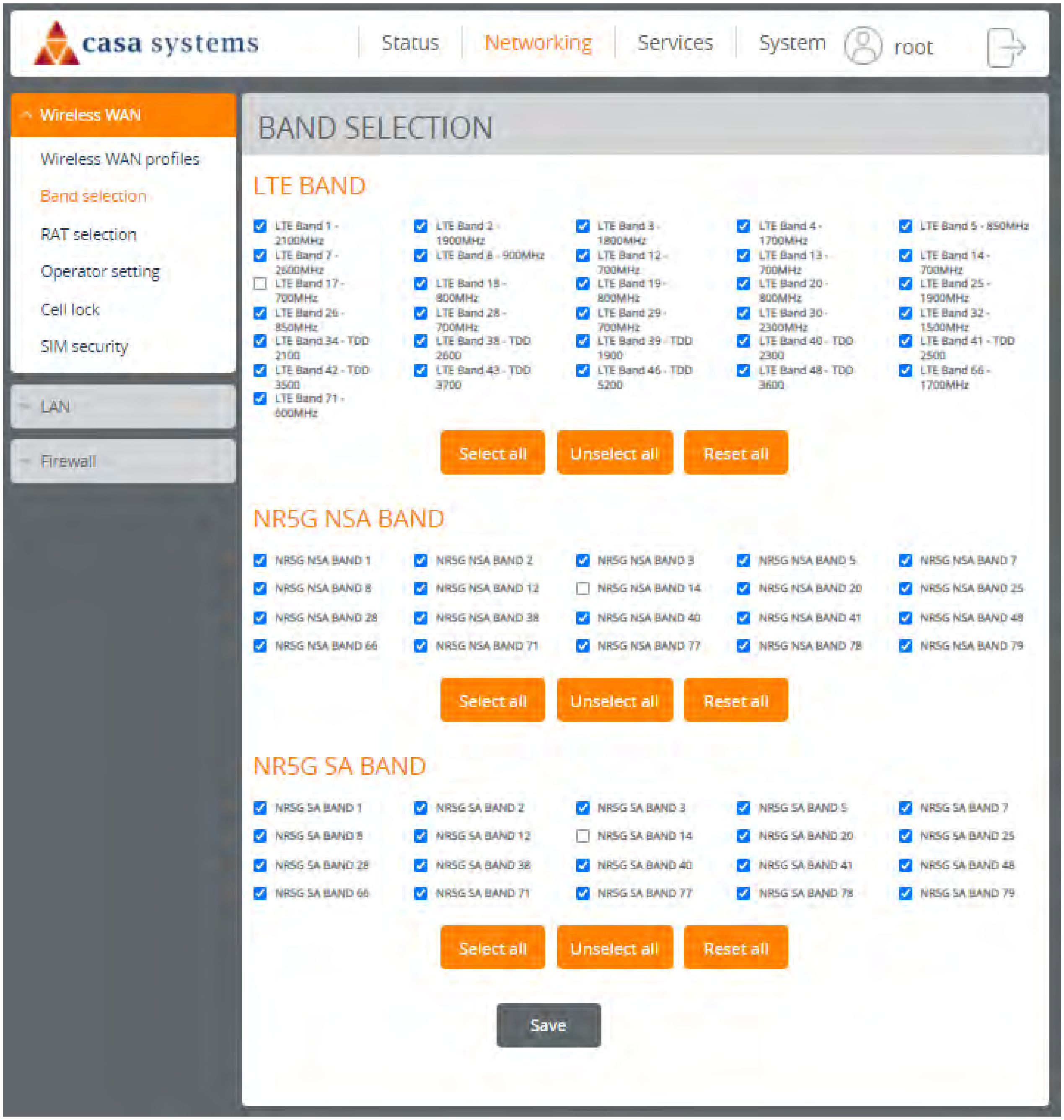
Item	Definition
Enable	Toggle the enable button to On or Off, as desired.
Name	The name of the APN for easy identification on the Wireless WAN profile page. This name is only used to identify the profile on the AurusPRO.
APN	Enter the APN (Access Point Name) configured for the corresponding profile.
Username	The username used to log on to the corresponding APN (if required)..
Password	The password used to log on to the corresponding APN (if required)..
Authentication type	The authentication type required by your provider. This can be set to: None, PAP or CHAP

Item	Definition
PDP Type	Select the **PDP type** (IP protocol) to use for the connection. a ⦿ **IPv4** – Sets a single stack IPv4 connection through which the AurusPRO receives only IPV4 network and DNS addresses. b ⦿ **IPv6** – Sets a single stack IPv6 connection through which the AurusPRO receives only IPV6 network and DNS addresses. Note – Before selecting this PDP type, check with your carrier to confirm that single stack IPV6 connectivity is supported. c ⦿ **IPv4v6** – Sets a dual stack connection allowing simultaneous IPV4 and IPV6 network connectivity. The AurusPRO receives both IPv4 and IPV6 network and DNS addresses. This is the default **PDP type**
Allow Admin Access	Select enable if remote SSH, TR-069 or WebGUI access to the device should be possible via this Wireless WAN Profile. Note – SSH/HTTP/HTTPS can be individually restricted in the **Access Control** menu. Note also that this will automatically be enabled if the profile is selected in the **TR-069 settings** menu.
MTU size	Sets the Maximum Transmission Unit size. This may be from 1 to 1500 bytes.
IP passthrough	Allows a downstream device, such as a router, to manage the connection. The downstream device connects to the Internet and receives a WAN IP address so that all Internet traffic is passed to the downstream device. Internet traffic is still terminated at the gateway (AurusPRO) and passed through to a downstream device, so the carrier is still able to connect to the gateway.
Save button	Click the **Save** button to apply the changes.

Table 14 - Wireless WAN Profile Settings page

6.2.1.2 Band selection

Select individual bands from the following band groupings: LTE, NR5G NSA or NR5G SA



BAND SELECTION

LTE BAND

☑ LTE Band 1 - 2100MHz	☑ LTE Band 2 - 1900MHz	☑ LTE Band 3 - 1800MHz	☑ LTE Band 4 - 1700MHz	☑ LTE Band 5 - 850MHz
☑ LTE Band 7 - 2600MHz	☑ LTE Band 8 - 900MHz	☑ LTE Band 12 - 700MHz	☑ LTE Band 13 - 700MHz	☑ LTE Band 14 - 700MHz
□ LTE Band 17 - 700MHz	☑ LTE Band 18 - 800MHz	☑ LTE Band 19 - 800MHz	☑ LTE Band 20 - 800MHz	☑ LTE Band 25 - 1900MHz
☑ LTE Band 26 - 850MHz	☑ LTE Band 28 - 700MHz	☑ LTE Band 29 - 700MHz	☑ LTE Band 30 - 2300MHz	☑ LTE Band 32 - 1500MHz
☑ LTE Band 34 - TDD 2100	☑ LTE Band 38 - TDD 2600	☑ LTE Band 39 - TDD 1900	☑ LTE Band 40 - TDD 2300	☑ LTE Band 41 - TDD 2500
☑ LTE Band 42 - TDD 3500	☑ LTE Band 43 - TDD 3700	☑ LTE Band 46 - TDD 5200	☑ LTE Band 48 - TDD 3600	☑ LTE Band 66 - 1700MHz
☑ LTE Band 71 - 600MHz				

NR5G NSA BAND

☑ NR5G NSA BAND 1	☑ NR5G NSA BAND 2	☑ NR5G NSA BAND 3	☑ NR5G NSA BAND 5	☑ NR5G NSA BAND 7
☑ NR5G NSA BAND 8	☑ NR5G NSA BAND 12	□ NR5G NSA BAND 14	☑ NR5G NSA BAND 20	☑ NR5G NSA BAND 25
☑ NR5G NSA BAND 28	☑ NR5G NSA BAND 38	☑ NR5G NSA BAND 40	☑ NR5G NSA BAND 41	☑ NR5G NSA BAND 48
☑ NR5G NSA BAND 66	☑ NR5G NSA BAND 71	☑ NR5G NSA BAND 77	☑ NR5G NSA BAND 78	☑ NR5G NSA BAND 79

NR5G SA BAND

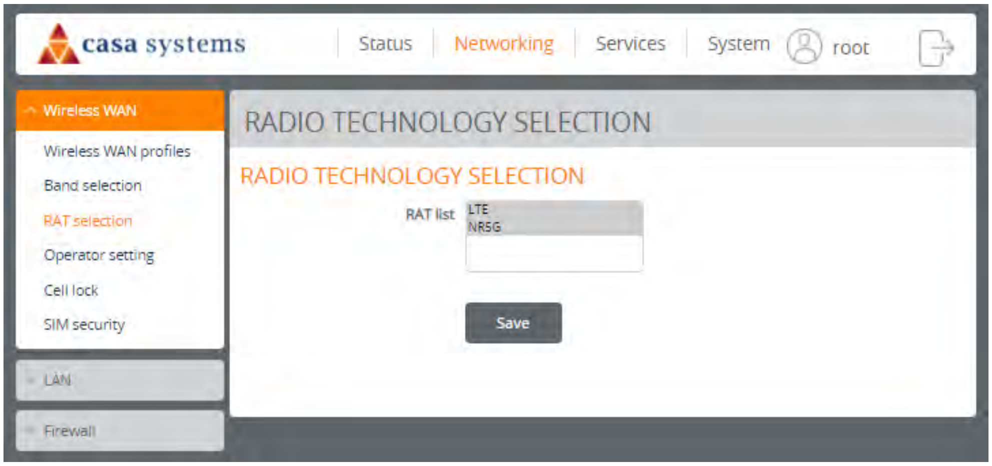
☑ NR5G SA BAND 1	☑ NR5G SA BAND 2	☑ NR5G SA BAND 3	☑ NR5G SA BAND 5	☑ NR5G SA BAND 7
☑ NR5G SA BAND 8	☑ NR5G SA BAND 12	□ NR5G SA BAND 14	☑ NR5G SA BAND 20	☑ NR5G SA BAND 25
☑ NR5G SA BAND 28	☑ NR5G SA BAND 38	☑ NR5G SA BAND 40	☑ NR5G SA BAND 41	☑ NR5G SA BAND 48
☑ NR5G SA BAND 66	☑ NR5G SA BAND 71	☑ NR5G SA BAND 77	☑ NR5G SA BAND 78	☑ NR5G SA BAND 79

Figure 42 - Wireless WAN – Band selection page

To set a device up for different LTE, 5G Non-Standalone (NR5G NSA) and 5G Standalone (NR5G NSA) modes, refer to: *Appendix B – Configuring Radio Access Technologies*

6.2.1.3 RAT selection

Select the preferred RAT (Radio Access Technology) from the following: LTE or NR5G



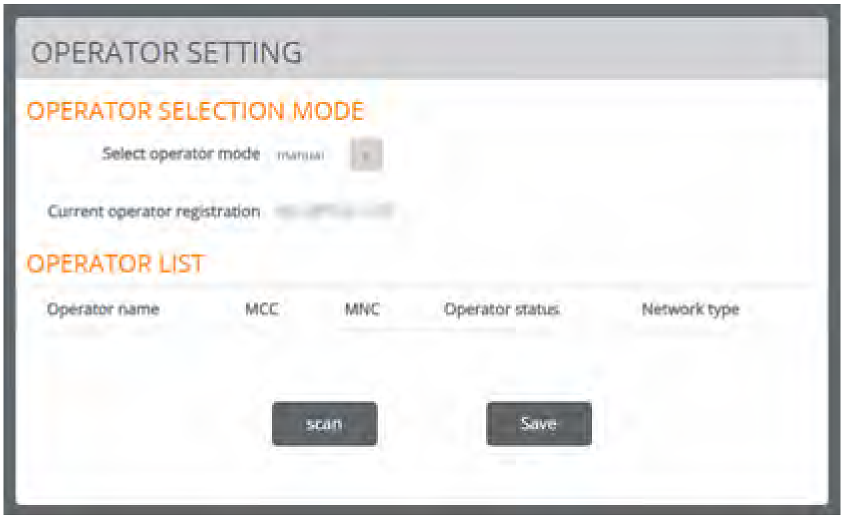
RAT list: LTE, NR5G

Figure 43 - Wireless WAN – Radio Technology selection page

To set a device up for different LTE, 5G Non-Standalone (NR5G NSA) and 5G Standalone (NR5G NSA) modes, refer to: *Appendix B – Configuring Radio Access Technologies*

6.2.1.4 Operator settings

The Operator setting screen lets you select whether to have the AurusPRO automatically select the most appropriate operator and access technology, or if you set it to Manual, you can override and lock it to a particular carrier or access technology.



Select operator mode: manual

Current operator registration

Figure 44 - Wireless WAN – Operator Settings

6.2.1.5 Roaming control

Select On to enable Roaming Control.

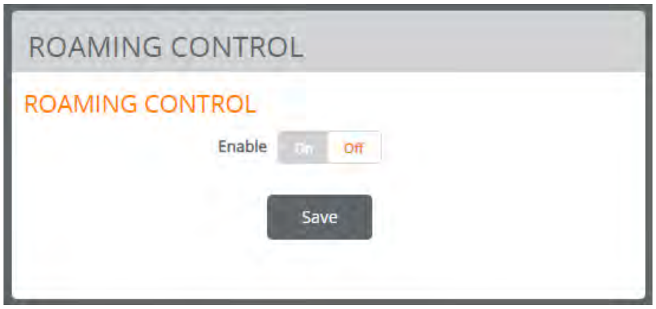


Figure 45 - Roaming control page

6.2.1.6 Cell lock

The Cell lock function allows you to specify a list of cells that the AurusPRO will not deviate from.

Two types of cells can be locked: LTE and NR5G

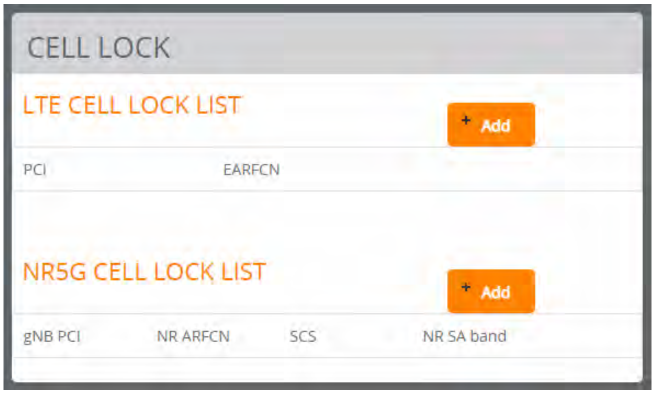


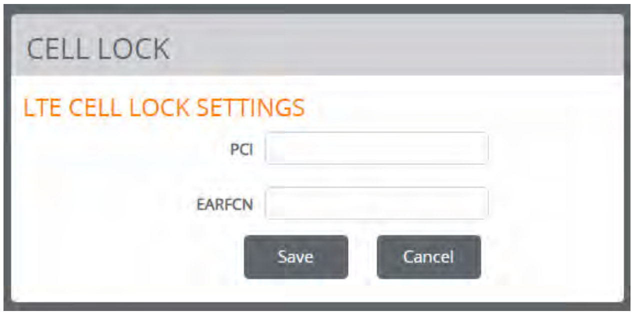
Figure 46 – Cell Lock page

Adding an LTE cell lock

To add an LTE cell to the list:

1 Next to LTE Cell Lock List, click on the Add button

2 Enter the PCI and EARFCN values of the cell that you want to lock to.



CELL LOCK

LTE CELL LOCK SETTINGS

PCI

EARFCN

Figure 47 - LTE Cell Lock settings

3 Click on the **Save** button. It will be added to the **LTE Cell Lock List** on the **Cell Lock** page.

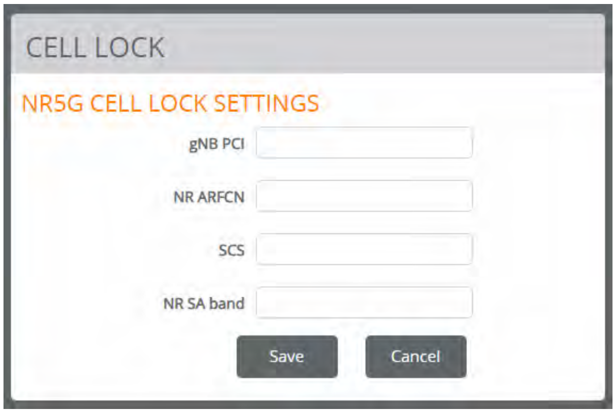
4 Repeat steps 1 to 3 for all the LTE cells that you wish to add.

Adding an NR cell lock

To add an NR5G cell to the list:

1 Next to the **NR5G Cell Lock List**, click on the **Add** button.

2 Enter the gNB, NR ARFCN, Subcarrier Spacing and NR SA band values for the NR5G cell that you want to lock to.



CELL LOCK

NR5G CELL LOCK SETTINGS

gNB PCI

NR ARFCN

SCS

NR SA band

Figure 48 – NR5G Cell Lock settings

3 Click on the **Save** button. It will be added to the **NR5G Cell Lock List** on the **Cell Lock** page.

4 Repeat steps 1 to 3 for all the NR5G cells that you wish to add.

6.2.1.7 SIM security

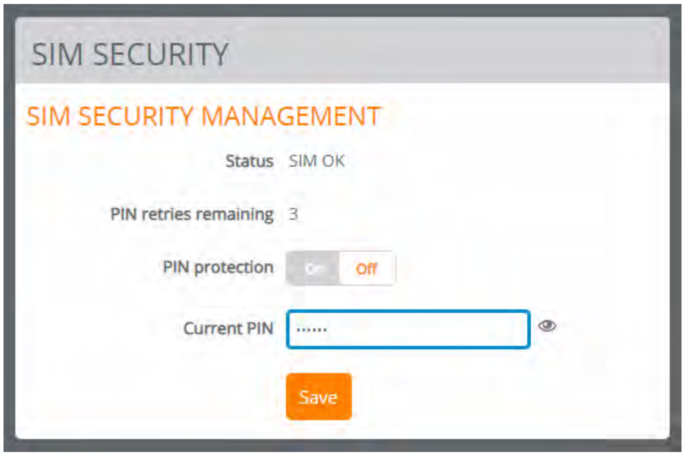
The SIM security settings page can be used for authenticating SIM cards that have been configured with a security PIN.

Unlocking a PIN locked SIM

If the SIM card is locked, you will receive a notice when you access the Status page after which you will be directed to the PIN settings page to enter the PIN. The PIN settings page lists the status of the SIM at the top of the page.

If you are not redirected to the PIN settings page, to unlock the SIM:

1. Click on the **Networking** menu from the top menu bar, and then click **SIM security settings**.



SIM SECURITY

SIM SECURITY MANAGEMENT

Status SIM OK

PIN retries remaining 3

PIN protection On Off

Current PIN ••••••

Figure 49 - Wireless WAN – SIM Security settings page

1. Enter the PIN in the **Current PIN** field (enter numbers only).
2. Click on the **Save** button to save the PIN and unlock access.
3. Once unlocked, you may toggle the **PIN protection** switch to the **Off** position if you no longer wish to have access locked by a PIN.

6.2.2 LAN

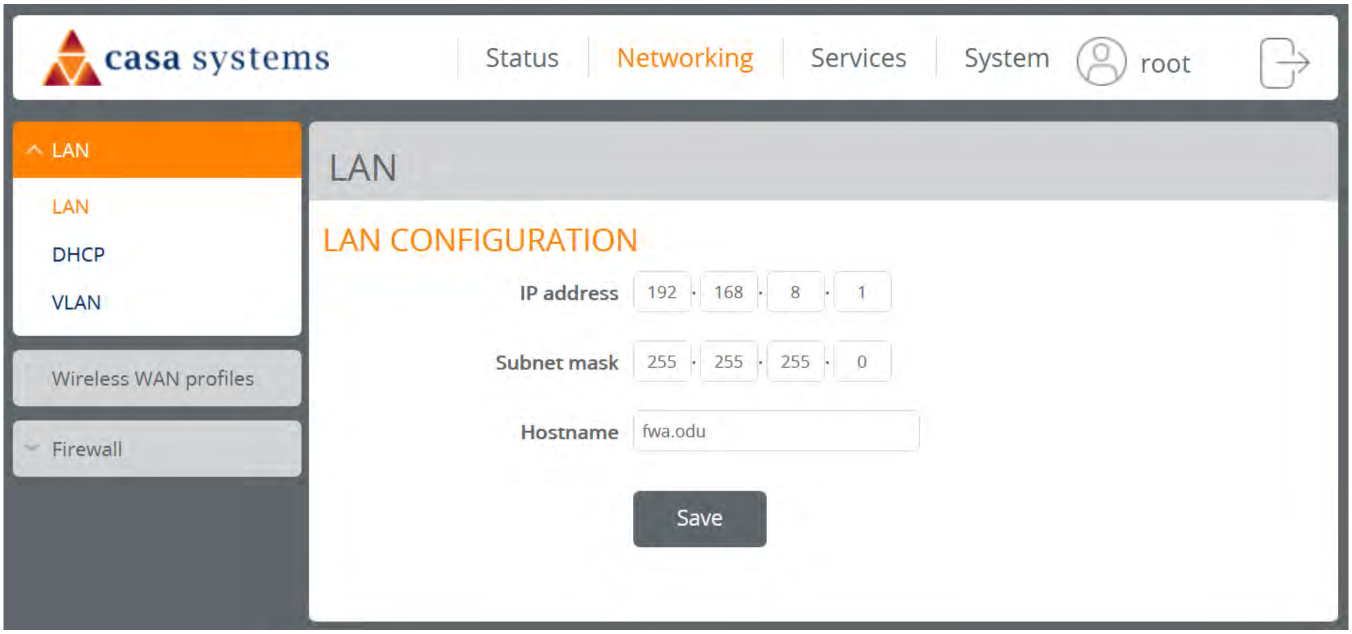
6.2.2.1 LAN Configuration

The LAN configuration page is used to configure the LAN settings of the AurusPRO. To access the LAN configuration page, click the Networking menu at the top of the screen, then click the LAN menu on the left.

The default IP of the LAN port is: 192.168.1.1 with subnet mask: 255.255.255.0

To change the IP address or Subnet mask, enter the new IP Address and/or Subnet mask and click the Save button.

Note – If you change the IP address, remember to refresh the Ethernet interface of your device, or set an appropriate IP address range, then enter the new IP address into your browser address bar to access the AurusPRO.



IP address 192 . 168 . 8 . 1

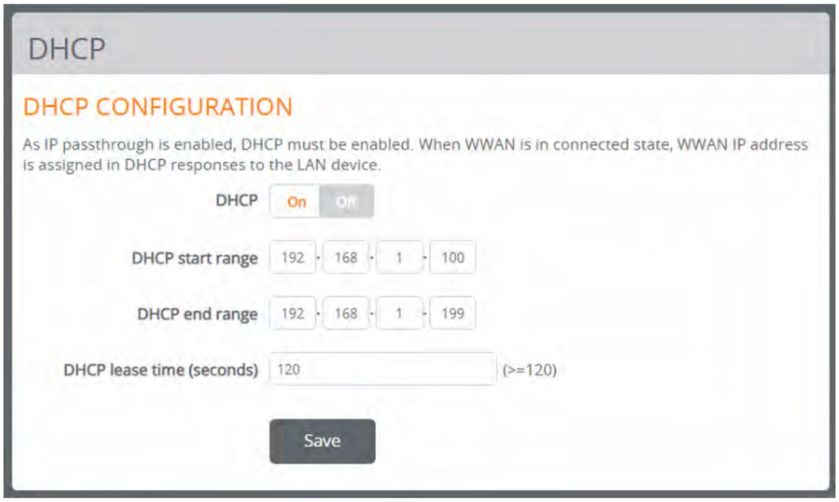
Subnet mask 255 . 255 . 255 . 0

Hostname fwa.odu

Figure 50 - LAN Configuration page

6.2.2.2 DHCP configuration

You can manually set the start and end address range to be used to automatically assign to DHCP clients when they are connected and the lease time of the assigned addresses.



DHCP

DHCP CONFIGURATION

As IP passthrough is enabled, DHCP must be enabled. When WWAN is in connected state, WWAN IP address is assigned in DHCP responses to the LAN device.

DHCP [✓ On] Off

DHCP start range 192 . 168 . 1 . 100

DHCP end range 192 . 168 . 1 . 199

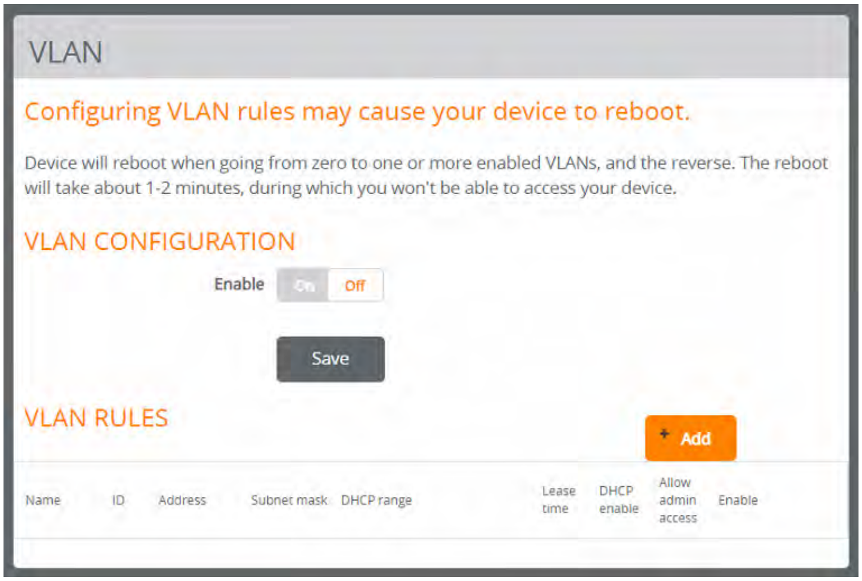
DHCP lease time (seconds) 120 (>=120)

Figure 51 - DHCP Configuration page

Enter the desired DHCP options and click the **Save** button.

6.2.2.3 VLAN

A Virtual Local Area Network (VLAN) is a subnetwork used to group devices located on separate physical networks. This useful feature allows you to partition your network without the need for additional cabling or wireless access.



VLAN

Configuring VLAN rules may cause your device to reboot.

Device will reboot when going from zero to one or more enabled VLANs, and the reverse. The reboot will take about 1-2 minutes, during which you won't be able to access your device.

VLAN CONFIGURATION

Enable On [✓ Off]

VLAN RULES

Name	ID	Address	Subnet mask	DHCP range	Lease time	DHCP enable	Allow admin access	Enable

Figure 52 - VLAN Rules list page

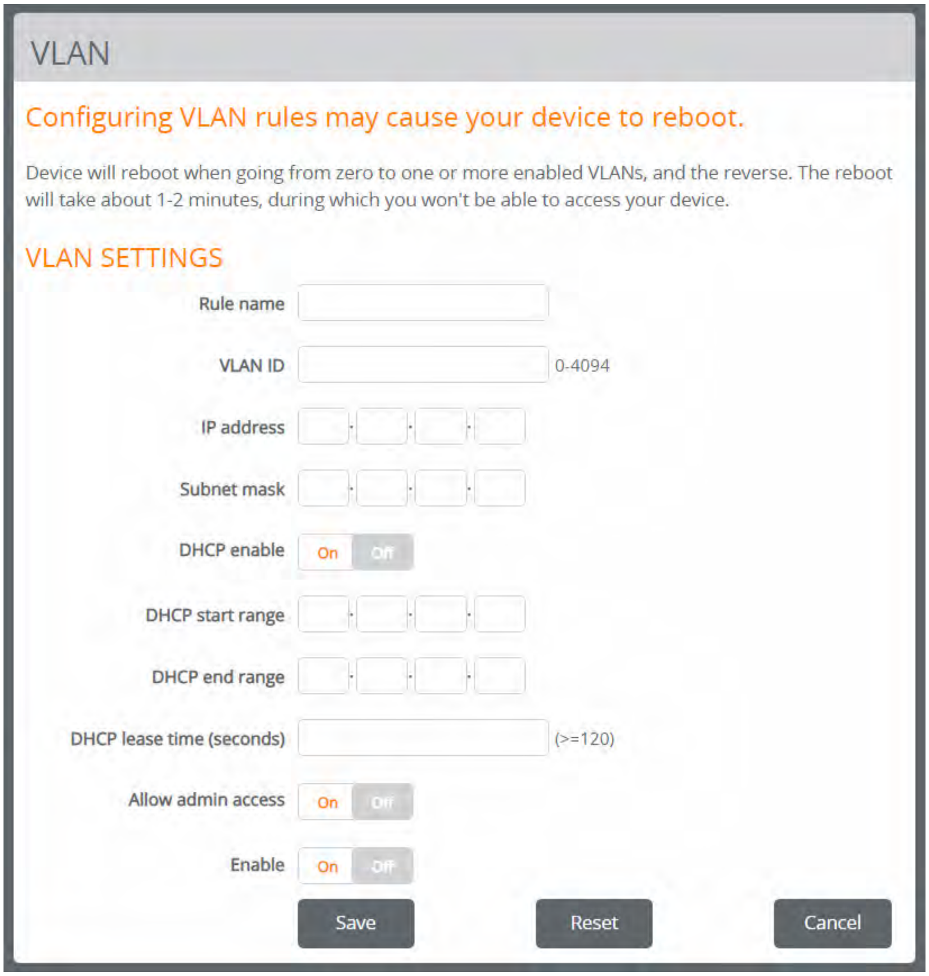
VLAN Settings

Note – VLANs can only be assigned to APN Profiles 2-6.

Click the **Add** button in the **VLAN RULES** section to create a VLAN rule:

1 Click the **+Add** button on the VLAN Configuration page.

The **VLAN Settings** page will open:



VLAN

Configuring VLAN rules may cause your device to reboot.

Device will reboot when going from zero to one or more enabled VLANs, and the reverse. The reboot will take about 1-2 minutes, during which you won't be able to access your device.

VLAN SETTINGS

Rule name	
VLAN ID	0-4094
IP address	. . .
Subnet mask	. . .
DHCP enable	On Off
DHCP start range	. . .
DHCP end range	. . .
DHCP lease time (seconds)	(>=120)
Allow admin access	On Off
Enable	On Off

Figure 53 - VLAN Settings page

2 In the **Rule name** field, enter a name for the VLAN rule. This is a name that allows you to easily identify the VLAN.

3 In the **VLAN ID** field, enter a number between 0 and 4094 which will be used by the network to identify the VLAN uniquely.

Note – The values 253, 254 and 255 are reserved and cannot be assigned to VLANs as **VLAN IDs**.

4 In the **IP address** field, enter the IP address for this device on the VLAN.

5 In the **Subnet mask** field, enter the Subnet mask for the device on the VLAN.

6 In the **DHCP start range** and **DHCP end range** fields, enter the IP address range for the VLAN. Addresses within this range will be assigned automatically to devices connecting to this VLAN.

7 In the **DHCP lease time (seconds)** field, enter the number of seconds that the DHCP lease will be valid for. This value must be 120 or higher.

8 In the **Allow Admin Access** field, select **Enable ON** if local SSH or WebGUI access to the device should be possible via this VLAN.

ⓘ Note – SSH/HTTP/HTTPS can be individually restricted in the **Access Control** menu.

9 Set the **Enable** toggle to the **ON** position.

10 Click the **Save** button to apply the settings.

6.2.3 Firewall

6.2.3.1 NAT

The Port forwarding list is used to configure the Network Address Translation (NAT) rules currently in effect on the AurusPRO. To access the Port forwarding page, click the **Networking** menu at the top of the screen, click the **Firewall** menu on the left.

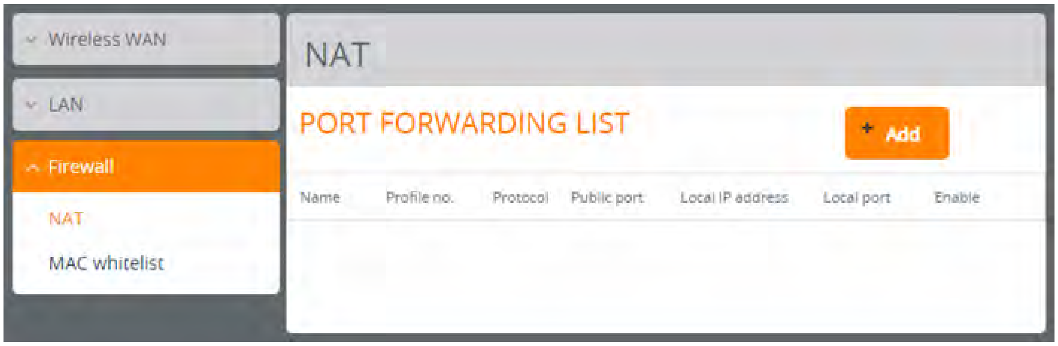


Figure 54 – NAT Port forwarding list

The purpose of the port forwarding feature is to allow mapping of inbound requests to a specific port on the WAN IP address to any connected device.

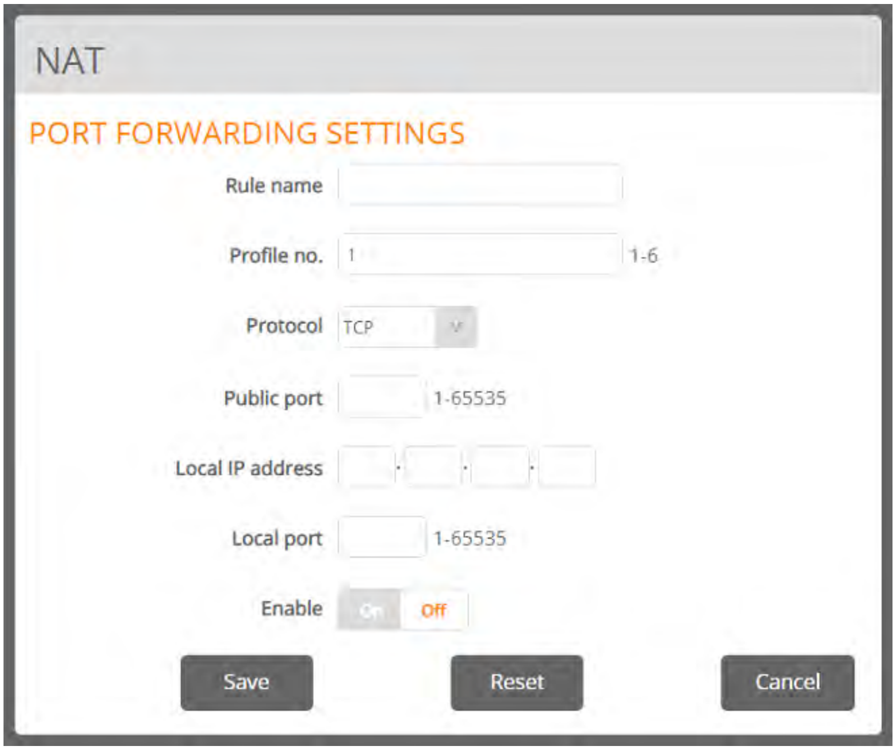
ⓘ Note – Some carriers block inbound connections, or require a public IP address in order to get inbound requests.

Adding a port forwarding rule

To create a new port forwarding rule:

1 Next to the protocol you wish to create a rule for (IPv4 or IPv6), click the **+Add** button.

The port forwarding settings screen is displayed.



NAT

PORT FORWARDING SETTINGS

Rule name	
Profile no.	1 1-6
Protocol	TCP
Public port	1-65535
Local IP address	. . .
Local port	1-65535
Enable	On Off

Figure 55 - Port Forwarding Settings

2 In the **Rule name** field, enter a name for the rule so that it can be easily identified.

3 In the **Profile No.** field, enter a number that corresponds to the Wireless WAN Profile that you want to use for the rule.

4 Use the **Protocol** drop-down list to select the type of protocol you want to use for the rule. The protocols selections available are **TCP**, **UDP** and **TCP/UDP**.

5 In the **Public port** field, enter a number between 1 and 65535 to use for the communication port from the AurusPRO out to the mobile network.

6 In the **Local IP Address / Local IPv6 Address** field, enter the IP address of LAN equipment to which traffic should be routed or a wildcard IP address (0.0.0.0) that allows all IP addresses to access the traffic.

7 In the **Local port** field, enter a port number to use for traffic to the local device. This may be an integer between 1 and 65535.

8 Ensure that the **Enable** toggle button is set to the **ON** position.

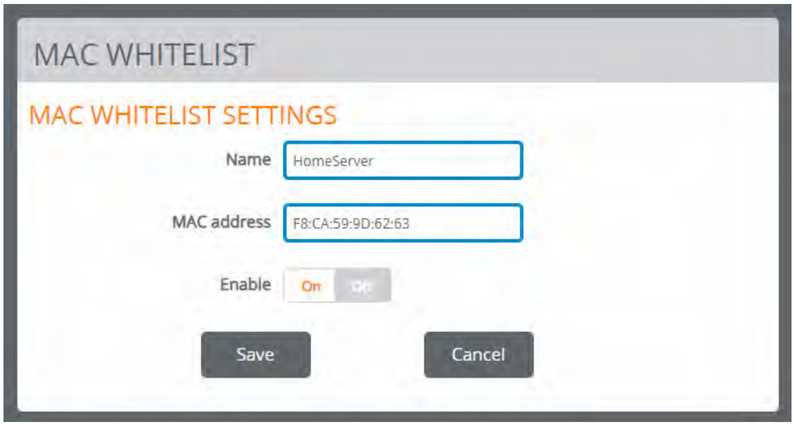
9 Click the **Save** button to confirm your settings.

10 To delete a port forwarding rule, click the × button on the **Port forwarding list** for the corresponding rule that you would like to delete. To edit an existing rule, click the ✎ button.

6.2.3.2 MAC whitelist

The MAC filter feature allows you to apply a policy to the traffic that passes through the router, both inbound and outbound, so that network access can be controlled based on the MAC address of the device seeking to make a connection.

To access the MAC filtering page, click the **Networking** menu at the top of the screen, click the **Firewall** menu on the left, then click the **MAC whitelist** menu item.



MAC WHITELIST

MAC WHITELIST SETTINGS

Name: HomeServer

MAC address: F8:CA:59:9D:62:63

Enable: On

Figure 56 – MAC whitelist page

To filter access based on MAC address:

1 Enter a **Name** to reference the whitelisted device with.

2 Enter the **MAC address** you want to allow access to

3 Click the **Enable** toggle key so that it is in the **On** position.

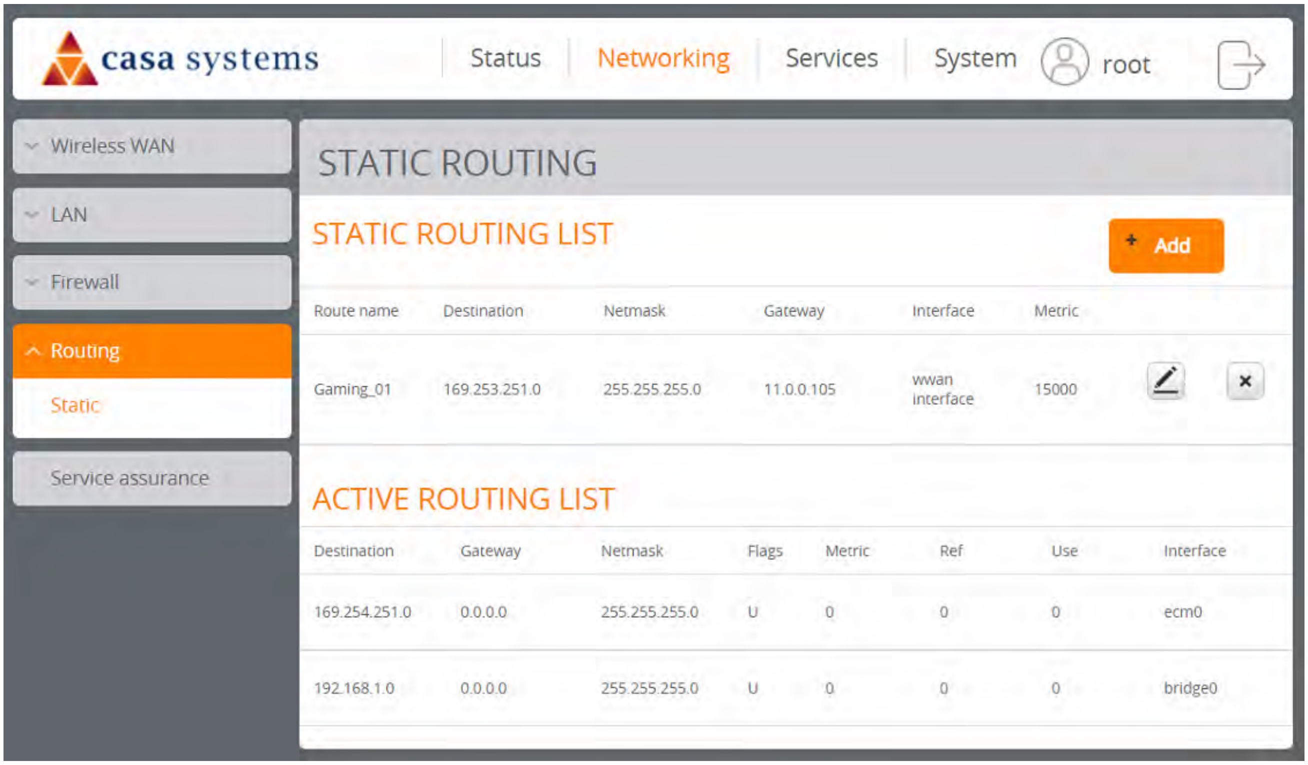
4 Click the **Save** button.

6.2.4 Routing

6.2.4.1 Static Routing

To view the Static Routing settings, click **Networking** then **Routing > Static** menu on the left.

The **Static Routing** page contains details of defined **Static Routing Lists** and well as the **Active Routing list**.



STATIC ROUTING

STATIC ROUTING LIST

Route name	Destination	Netmask	Gateway	Interface	Metric
Gaming_01	169.253.251.0	255.255.255.0	11.0.0.105	wwan interface	15000

ACTIVE ROUTING LIST

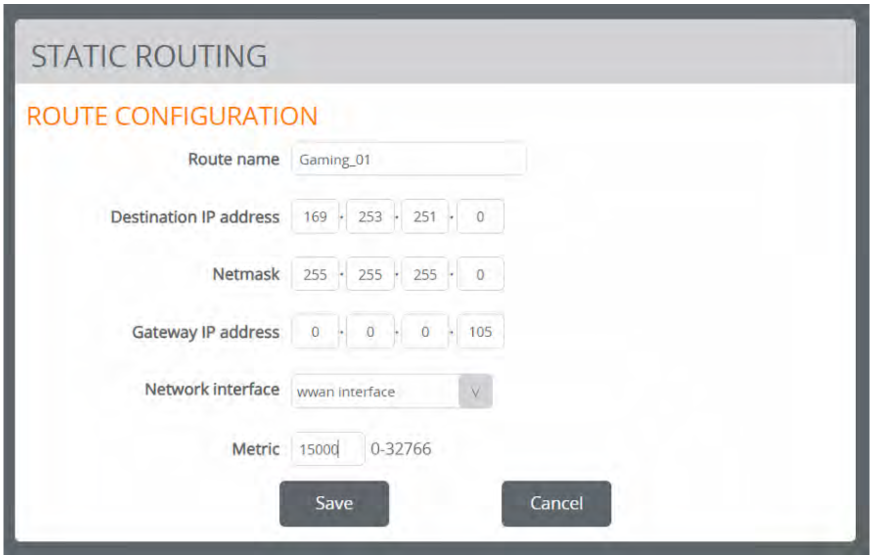
Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
169.254.251.0	0.0.0.0	255.255.255.0	U	0	0	0	ecm0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	bridge0

Figure 57 – Static/Active routing list

Click the **Add** button to define a new **Static Routing List**.

Static Route Configuration

Click the **Add** button to open the ROUTE CONFIGURATION page:



STATIC ROUTING

ROUTE CONFIGURATION

Route name: Gaming_01

Destination IP address: 169 . 253 . 251 . 0

Netmask: 255 . 255 . 255 . 0

Gateway IP address: 0 . 0 . 0 . 105

Network interface: wwan interface

Metric: 15000 0-32766

Figure 58 – Route configuration page

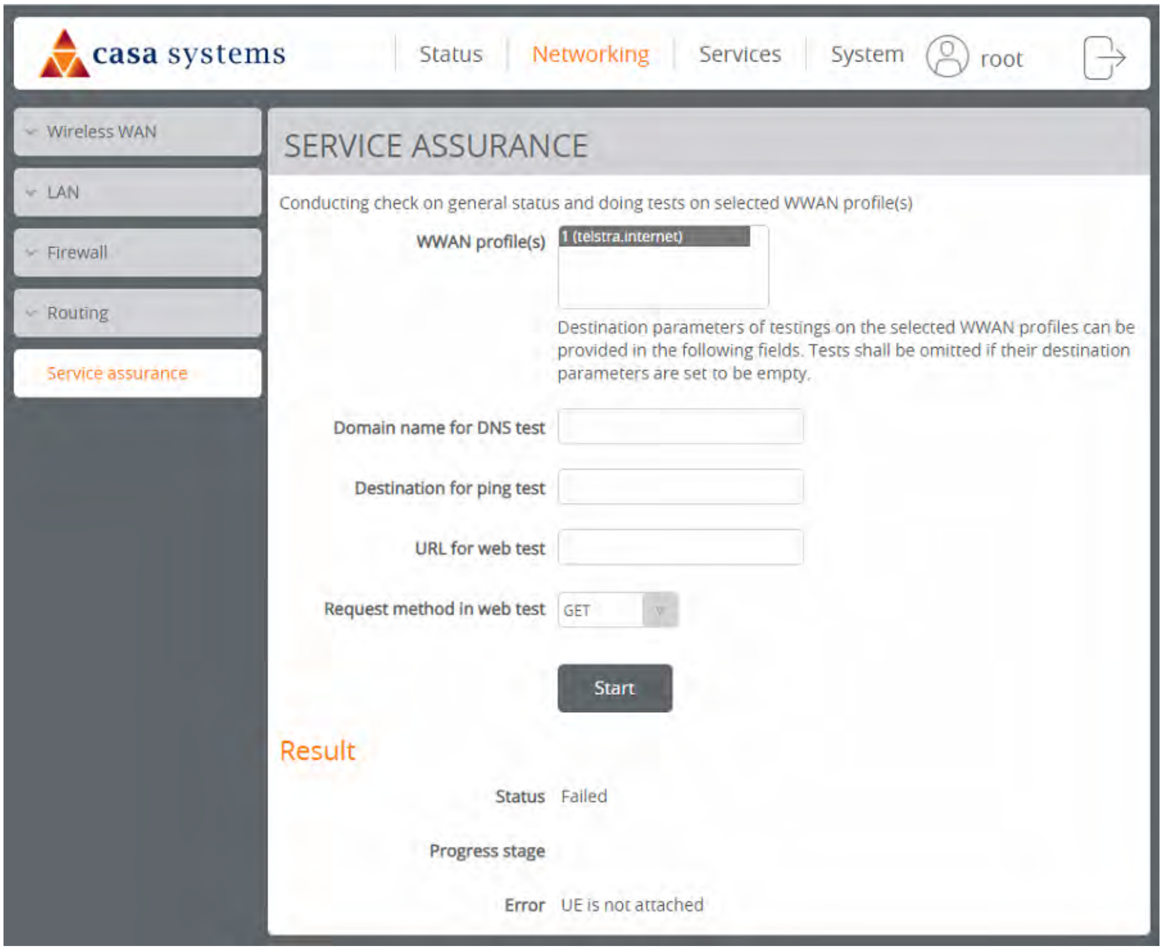
Route configuration

Route name	Enter a meaningful name.
Destination IP address	Enter the destination IP address of the route.
Netmask	Enter a netmask specification.
Gateway IP address	Enter the gateway's IP address
Network interface	Select the Network interface.
Metric	Enter a metric in the range of 0 through 32766
Save button	Click to save the changes and add the configuration to the **Static Routing List.**
Cancel button	Close the window and discard the current entries. Note – if you want to delete an existing Static Route, click the ✖ delete button on the **Static Routing List** to remove it permanently from the system.

Table 15 – Route configuration fields

6.2.5 Service assurance

To conduct a check on general status of selected WWAN profiles and other tests click the **Networking** menu at the top of the screen, then click the **Service assurance** menu item on the left.



SERVICE ASSURANCE

Conducting check on general status and doing tests on selected WWAN profile(s)

WWAN profile(s): 1 (telstra.internet)

Destination parameters of testings on the selected WWAN profiles can be provided in the following fields. Tests shall be omitted if their destination parameters are set to be empty.

Domain name for DNS test:

Destination for ping test:

URL for web test:

Request method in web test: GET

Result

Status: Failed

Progress stage:

Error: UE is not attached

Figure 59 – Service assurance page

From the **WWAN profiles** list select the service you want to monitor.

When the settings are complete, click the Start button to commence the test.

6.2.5.1 Result

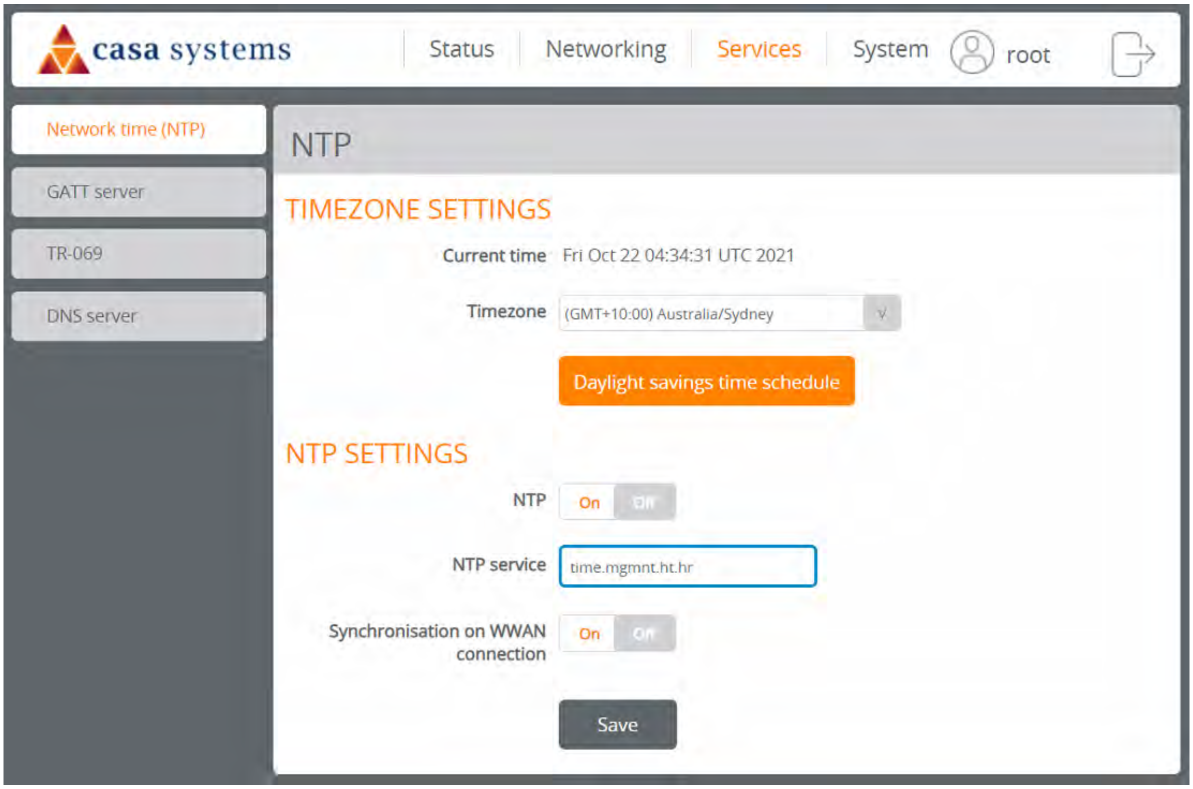
In this section the **Status**, **Progress stage** and any **Error** message will be displayed.

6.3 Services

6.3.1 Network Time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the AurusPRO to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the device. This provides an accurate timekeeping function for features such as System Log entries and Firewall settings where the current system time is displayed and recorded. Any NTP server available publicly on the internet may be used. The default NTP server is time.nrc.ca.

To access the Network time (NTP) page, click the **Services** menu at the top of the screen then click the **Network time (NTP)** menu item on the left.



Current time Fri Oct 22 04:34:31 UTC 2021

Timezone (GMT+10:00) Australia/Sydney

NTP On Off

NTP service time.mgmnt.ht.hr

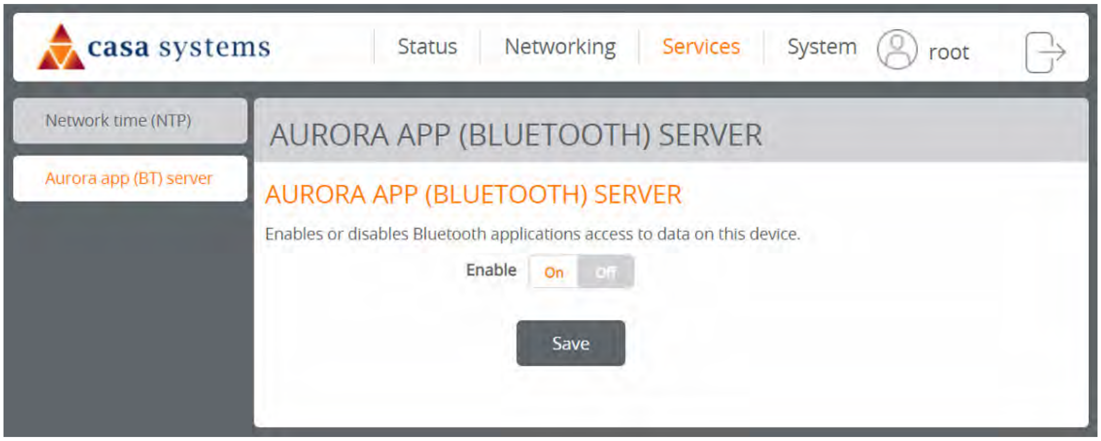
Synchronisation on WWAN connection On Off

Figure 60 - Network Time (NTP) page

6.3.2 Aurora App (Bluetooth) Server

The **Aurora App (Bluetooth) Server** is used to facilitate communication with the Aurora smartphone installation app.

Switch **Enable** to **On** before starting the Aurora installation app on an Android device.



AURORA APP (BLUETOOTH) SERVER

AURORA APP (BLUETOOTH) SERVER

Enables or disables Bluetooth applications access to data on this device.

Enable [✓ On] Off

Figure 61 - Aurora App (Bluetooth) server page

When an installation has been completed, you have the option to disable the Aurora App server, but be aware that next time you try to find the antenna via the app, it will not be able to discover the antenna until the Aurora App server has been re-enabled.

6.3.3 TR-069

The TR-069 (Technical Report 069) protocol is a technical specification also known as CPE WAN Management Protocol (CWMP). It is a framework for remote management and auto-configuration of end-user devices such as customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It is particularly efficient in applying configuration updates across networks to multiple CPEs.

TR-069 uses a bi-directional SOAP/HTTP-based protocol based on the application layer protocol and provides several benefits for the maintenance of a field of CPEs:

- Simplifies the initial configuration of a device during installation
- Enables easy restoration of service after a factory reset or replacement of a faulty device
- Firmware and software version management
- Diagnostics and monitoring

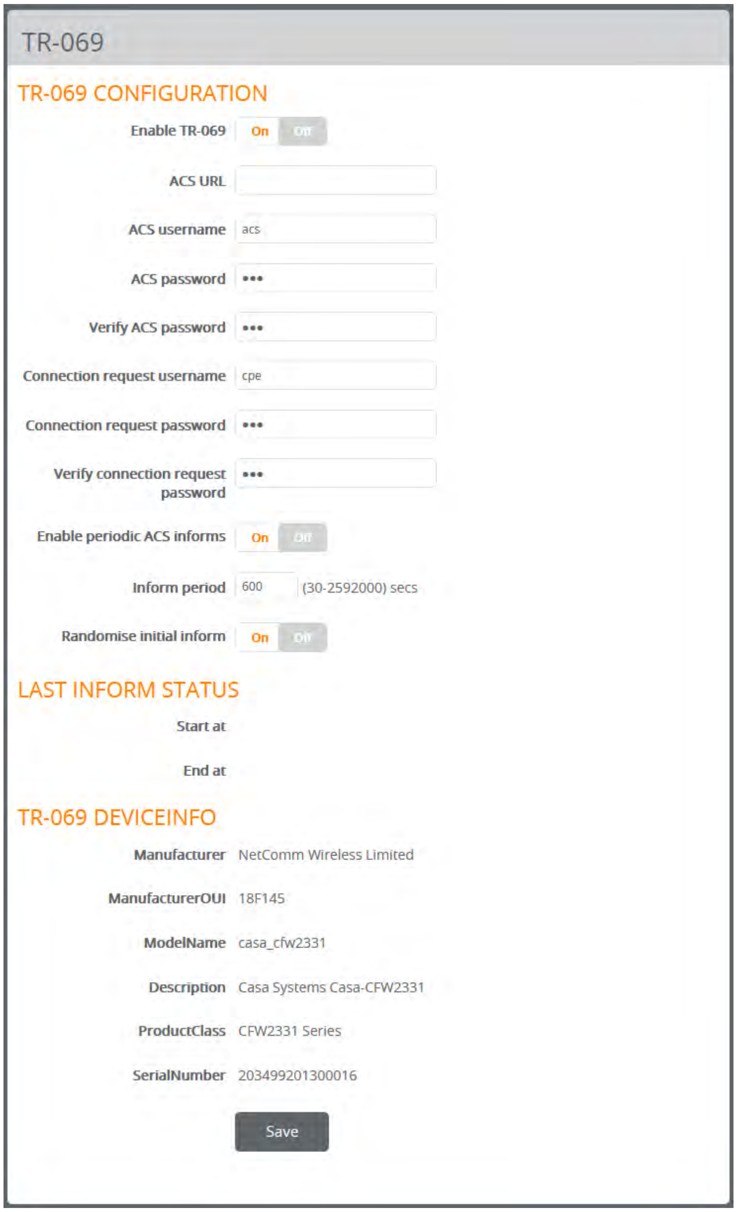
Note – You must have your own compatible ACS infrastructure to use TR-069. To access and configure the TR-069 settings, you must be logged into the router with the root account.
When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

The CPE sends “inform” messages periodically to alert the ACS server that it is ready. These inform messages can also be configured to accept a connection request from the ACS server. When a connection is established, any tasks queued on the ACS server are executed. These tasks may be value retrieval or changes and firmware upgrades.

6.3.3.1 TR-069 configuration

To configure TR-069:

1 Click the **Enable TR-069** toggle key to switch it to the **ON** position.



TR-069

TR-069 CONFIGURATION

Enable TR-069	On Off
ACS URL	
ACS username	acs
ACS password	•••
Verify ACS password	•••
Connection request username	cpe
Connection request password	•••
Verify connection request password	•••
Enable periodic ACS informs	On Off
Inform period	600 (30-2592000) secs
Randomise initial inform	On Off

LAST INFORM STATUS

Start at	
End at	

TR-069 DEVICEINFO

Manufacturer	NetComm Wireless Limited
ManufacturerOUI	18F145
ModelName	casa_cfw2331
Description	Casa Systems Casa-CFW2331
ProductClass	CFW2331 Series
SerialNumber	203499201300016

Figure 62 - TR-069 Configuration

2 In the **ACS URL** field, enter the Auto Configuration Server's full domain name or IP address.

3 Use the **ACS** username field to specify the username used by the server to authenticate the CPE when it sends an "inform" message.

4 In the **ACS password** and **Verify ACS password** fields, enter the password used by the server to authenticate the CPE when it sends an "inform" message.

5 In the **Connection request** username field, enter the username that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.

6 In the **Connection request password** and **Verify password** fields, enter the password that the CPE uses to authenticate the Auto Configuration Server during a connection request to the CPE.

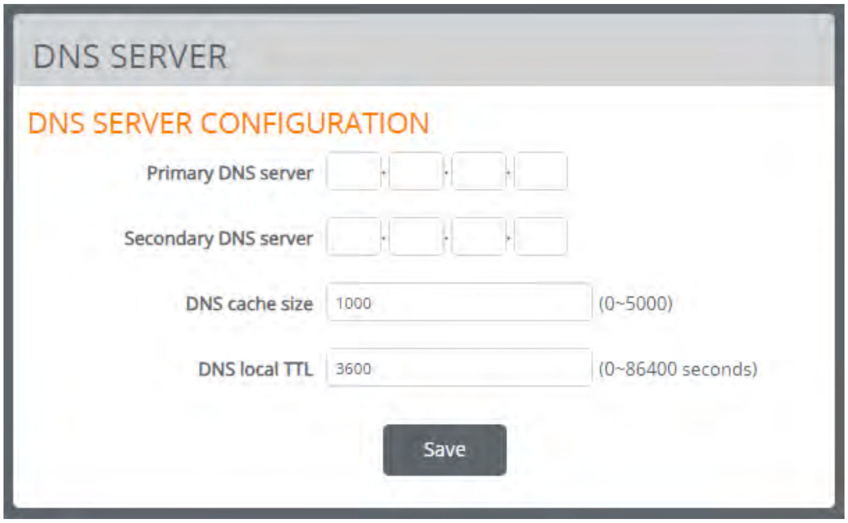
7 The inform message acts as a beacon to inform the ACS of the existence of the router. Select **Enable periodic ACS informs** toggle key to **ON** in order to turn on the periodic ACS inform messages.

8 In the **Inform Period** field, enter the number of seconds between the inform messages.

9 Click the **Save** button to save the settings.

6.3.4 DNS Server

Enter the IP addresses of the **Primary DNS server** and **Secondary DNS server.**



DNS SERVER

DNS SERVER CONFIGURATION

Primary DNS server . . .

Secondary DNS server . . .

DNS cache size 1000 (0~5000)

DNS local TTL 3600 (0~86400 seconds)

Figure 63 - DNS Server page

Set a **DNS cache size** of between 0 and 5000.

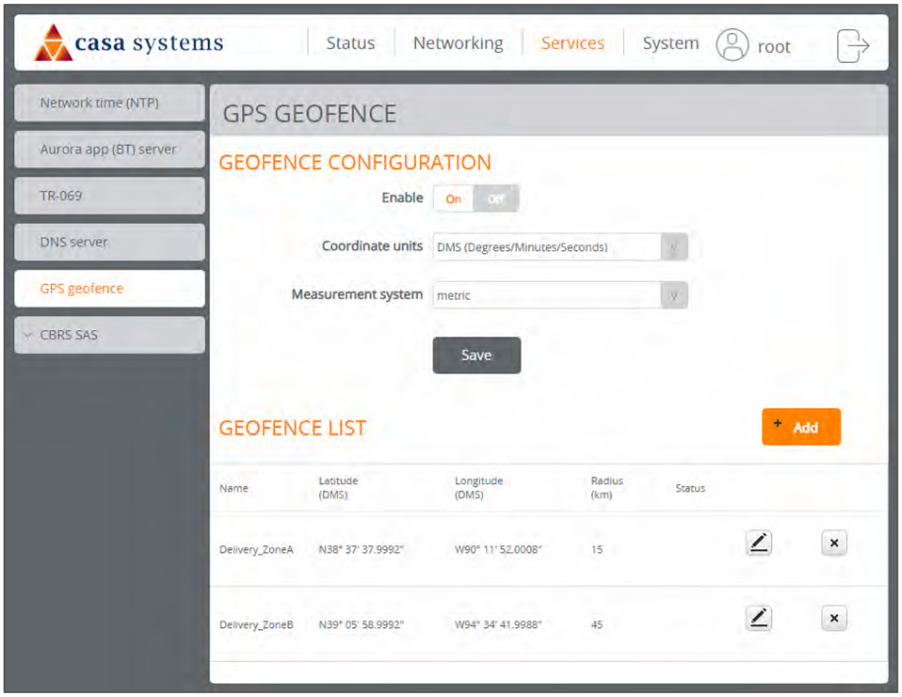
Set the **DNS local TTL (Time-To-Live)** time between 0 and 86,400 seconds.

Click the **Save** button to apply the settings to the DNS server.

6.3.5 Geofence

To access the Geofence screen, select the **Services** item from the top menu bar then select the **Geofence** menu item.

Geofence allows you to designate a circular area and then uses the router's GPS position to monitor when the gateway moves out of or in to that area.



GPS GEOFENCE

GEOFENCE CONFIGURATION

Enable: On

Coordinate units: DMS (Degrees/Minutes/Seconds)

Measurement system: metric

GEOFENCE LIST

Name	Latitude (DMS)	Longitude (DMS)	Radius (km)	Status
Delivery_ZoneA	N38° 37' 37.9992"	W90° 11' 52.0008"	15	
Delivery_ZoneB	N39° 05' 58.9992"	W94° 34' 41.9988"	45	

Figure 64 – Geofence options

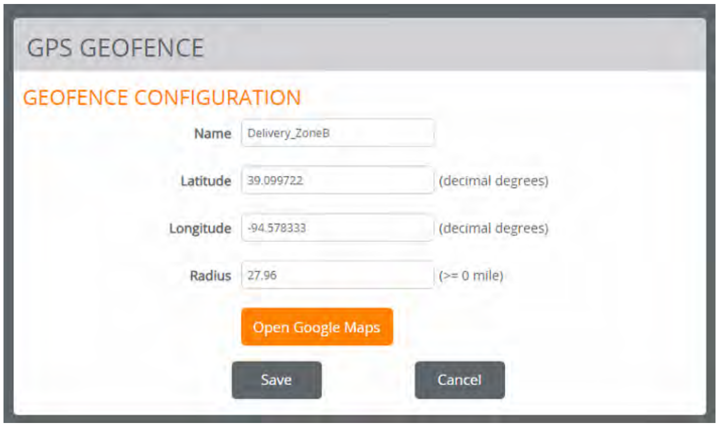
Item	Description
GEOFENCE CONFIGURATION	
Enable button	Toggles Geofence operation On or Off. When on your currently defined Geofences appear in the Geofence list, see below.
Coordinate units	Select either: ● DMS (Degrees/Minutes/Seconds), or ● Decimal degrees Changing this will change the display in the **GEOFENCE LIST** lower on the page, and the **GEOFENCE CONFIGURATION** page, see below.
Measurement system	Select either: ● metric, or ● imperial

	Changing this will change the display in the **GEOFENCE LIST** lower on the page, and the **GEOFENCE CONFIGURATION** page, see below.
Save button	Saves any changes made on this page
Add button	Click to add a new Geofence definition. The add Geofence configuration screen will open, see next section below.
GEOFENCE LIST	This table contains all your currently defined Geofences.
Name	A user defined reference name.
Latitude / Longitude	The Latitude and Longitude coordinates defined in the **GEOFENCE CONFIGURATION** page display. The **Coordinate units** selection will determine which system displays: DMS or decimal degrees
Radius	Set a radius from the centre of the geofence point. The **Measurement system** selection will determine which system displays: Kilometres or miles
Status	**In** if the router is inside the radius. **Out** if the router is outside the radius.
Edit button	Click this to edit an existing Geofence in the list. The user interface is the same as the add Geofence configuration screen, see next section below.
Delete button	Click to remove the geofence from the list.

Table 16 – Geofence user interface

6.3.5.1 Add Geofence

Click the **+Add** button to create a new Geofence (note that editing an existing Geofence uses the same configuration page).



GPS GEOFENCE

GEOFENCE CONFIGURATION

Name: Delivery_ZoneB

Latitude: 39.099722 (decimal degrees)

Longitude: -94.578333 (decimal degrees)

Radius: 27.96 (>= 0 mile)

Figure 65 – Configure Geofences

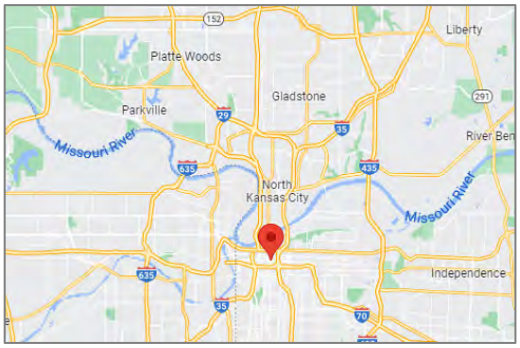
Item	Description
Name	When you Add a new Geofence you will be prompted to enter a meaningful name. This will be its reference in the Geofence list page.
Latitude / Longitude	Enter the Latitude and Longitude coordinates of the centre of the geofence. The **Coordinate units** selection will determine which system displays: DMS or decimal degrees
Radius	Set a radius from the centre of the geofence point for the fence line. The **Measurement system** selection will determine which system displays: Kilometres or miles
Open Google Maps button	When coordinates have been entered, click the **Google maps** button to show where you expect the centre of the geofence to be. For example:  152 Liberty Platte Woods Gladstone 291 Parkville 29 35 River Ben Missouri River 635 435 North Kansas City Missouri River 635 Independence 35 70
Save button	Saves the new Geofence (Add) or saves the changes to an existing Geofence (Edit).
Cancel button	Closes the **Add/Edit** page and returns to the Geofence list without saving any changes.

Table 17 – Geofence configuration options

6.3.6 CBRS SAS

CBRS (Citizens Broadband Radio Service) was introduced in the USA in 2016 to prioritise use of 3.5 GHz band spectrum (3550–3700 MHz) so that access to the spectrum could be prioritised into three levels to prevent harmful interference to higher priority users. The highest priority is reserved for government/military purposes and then the next level for Priority Access Licensed (PAL) users. Other users (General Authorized Access users) must request access to use the spectrum via the SAS (Spectrum Access Server).

Currently this functionality only applies to devices in service in USA.

The Spectrum Access System (SAS) is a cloud-based service that manages devices transmitting in the CBRS band. A CBRS device (CBSD) needs authorization from the SAS before it starts to transmit in the CBRS band.

The authorization process must be performed by a Certified Professional Installer (CPI) using the Aurora Pro installation app on an Android mobile phone or other device.

Never attempt to alter any CBRS Setting, including the URL, or else the CPE device will stop working.

⚠ Warning – Before considering or making any changes to these settings consult with your authorized Certified Professional Installer (CPI).

Any changes will require the CPE device to be submitted to a new CBRS SAS installation and registration process.

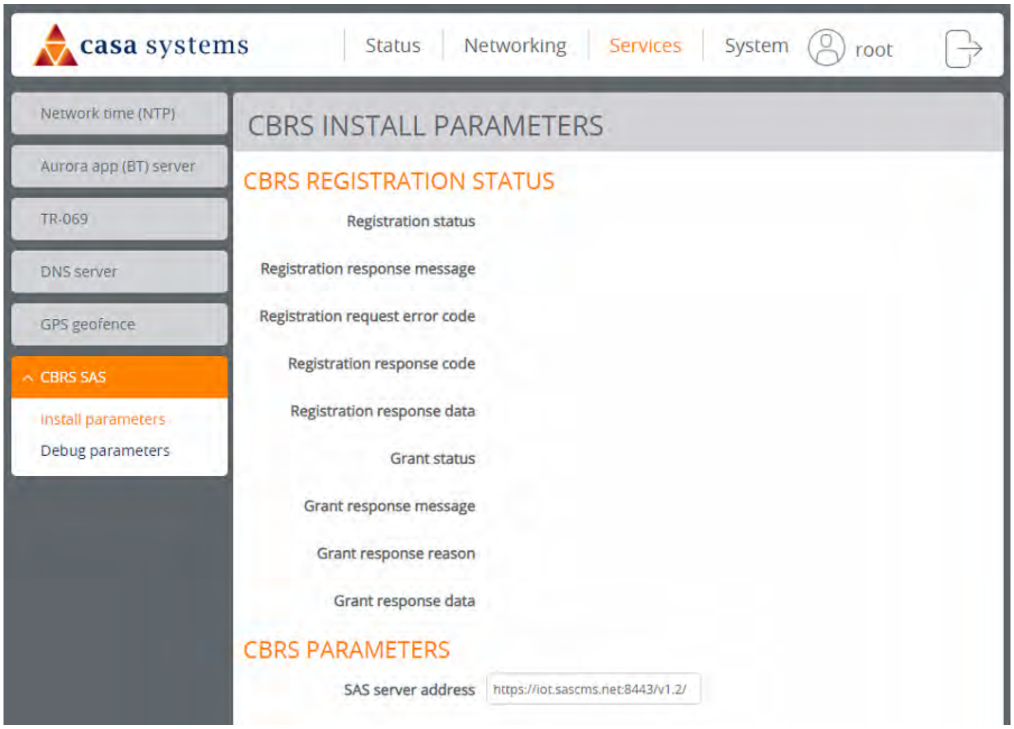
For more information on the Aurora Pro installation app and its interaction with the CBRS system, refer to the Aurora ODU Installation App (CBRS) User Guide.

6.3.6.1 Install parameters

This page is typically used for troubleshooting purposes. Consult with authorized Certified Professional Installer (CPI) and the debug or troubleshooting guide prior to troubleshooting installation issues.

To access the CBRS SAS screens, select the **Services** item from the top menu bar then open the **CBRS SAS** menu item.

From the **CBRS SAS** submenu select the **Install parameters** item on to view the status of the installation and parameters entered by the CPI and as registered with the CBRS.



CBRS INSTALL PARAMETERS

CBRS REGISTRATION STATUS

Registration status

Registration response message

Registration request error code

Registration response code

Registration response data

Grant status

Grant response message

Grant response reason

Grant response data

CBRS PARAMETERS

SAS server address https://iot.sascms.net:8443/v1.2/

Figure 66 – CBRS install parameters page [truncated]

6.3.6.2 Debug parameters

This page is typically used for troubleshooting purposes. Consult with authorized Certified Professional Installer (CPI) and the debug or troubleshooting guide prior to troubleshooting installation issues.

To view the current parameters, select **Services** and then from the **CBRS SAS** submenu select the **Debug parameters**.

6.4 System

6.4.1 Log – System log

The System Log enables you to troubleshoot any issues you may be experiencing with the AurusPRO. To access the System Log page, click the **System** menu. A page containing the **System Logs** buttons are displayed.

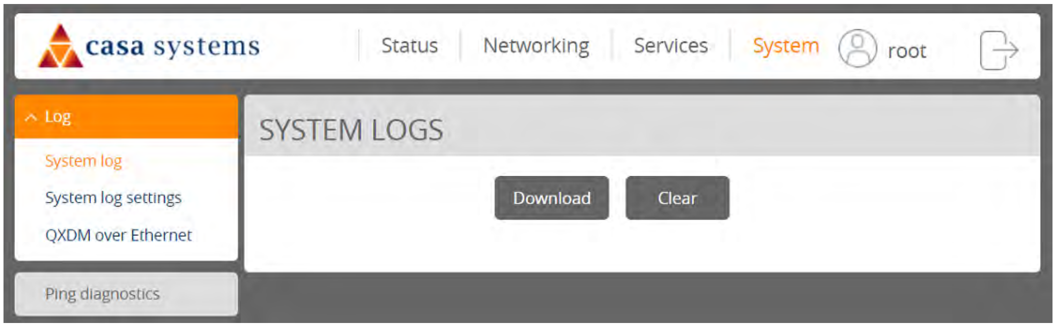


Figure 67 - System Log page

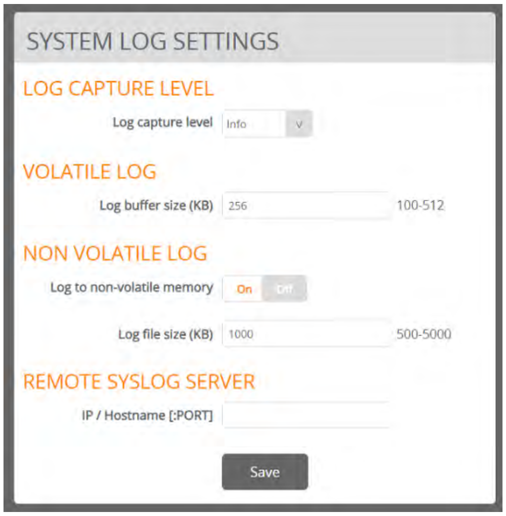
You can download the log file to your local computer by clicking on the **Download** button.

A .txt log file will be downloaded to your browser's Download folder.

The **Clear** button clears the log file when logging to non-volatile memory is enabled (refer to the System log settings section). It does not clear the log/message buffer.

6.4.1.1 Log – System log settings

To access the System log settings page, click the **System** menu item then select the **Log** menu on the left and then select **System log settings** from the drop-down menu.



SYSTEM LOG SETTINGS

LOG CAPTURE LEVEL

Log capture level: Info

VOLATILE LOG

Log buffer size (KB): 256 (100-512)

NON VOLATILE LOG

Log to non-volatile memory: On / Off

Log file size (KB): 1000 (500-5000)

REMOTE SYSLOG SERVER

IP / Hostname [:PORT]:

Save

Figure 68 - System Log Settings

Log capture level

The log capture level defines the amount of detail that the system log stores. This setting also affects the Display level setting on the System log page. The system will capture and display events for the selected level and all the events at levels below it. For example, setting it to “Notice” will show “Notice”, “Warning” and “Error” events.

Item	Definition
Debug	Show extended system log messages with full debugging level details.
Info	Show informational messages.
Notice	Show normal system logging information.
Warning	Show warning messages.
Error	Show error condition messages only.

Table 18 – System log detail levels

Volatile log

Contents of Volatile memory is stored temporarily.

1 Specify the maximum **Log buffer size** (100-512 kilobytes).

2 Click the **Save** button.

A drawback of log data saved in volatile memory is that the log data is stored in RAM and therefore when the unit loses power, or is rebooted, the device will lose any log information stored in the RAM.

Non-volatile memory is the type of memory in which data remains stored even if it is powered-off. To ensure that log information is accessible between reboots of the AurusPRO there are two options:

- Click On to enable the **Log to non-volatile memory** option.
- Use a **Remote Syslog Server**.

Non-volatile log

When the AurusPRO is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the device. Up to 512kb of log data will be stored before it is overwritten by new log data. Non-volatile logging can lead to Flash memory wear. This facility is intended for debugging only.

1 Click On to enable the **Log to non-volatile memory** option.

2 Specify the maximum **Log file size** (500-5000 kilobytes).

3 Click the **Save** button.

Remote syslog server

The AurusPRO can be configured to output log data to a remote syslog server. This is an application running on a remote computer which accepts and displays the log data. Most syslog servers can also save the log data to a file on the computer on which it is running allowing you to ensure that no log data is lost between reboots.

To configure the AurusPRO to output log data to a remote syslog server:

1 Click the **System** menu from the top menu bar. The **System log** item is displayed.

2 Under the **Remote syslog server** section, enter the IP address or hostname of the syslog server in the **IP / Hostname [:PORT]** field.

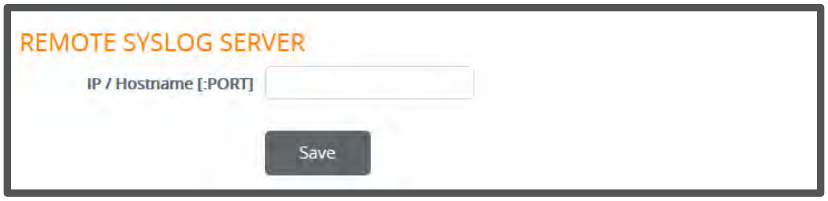


Figure 69 – Remote syslog server configuration

You can also specify the port number after the IP or hostname by entering a semi-colon and then the port number e.g. 192.168.1.102:514.

If you do not specify a port number, the AurusPRO will use the default UDP port 514.

3 Click the **Save** button to save the configuration.

6.4.1.2 QXDM over Ethernet

For debugging, you can use QXDM over Ethernet. QXDM is a Qualcomm tool used for capture and analysis of mobile signalling data.

To use QXDM over Ethernet:

1 Click on the **Enable** toggle key to set it to the **On** position.

2 Enter the **Server IP address**.

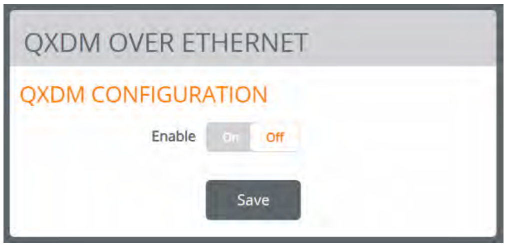
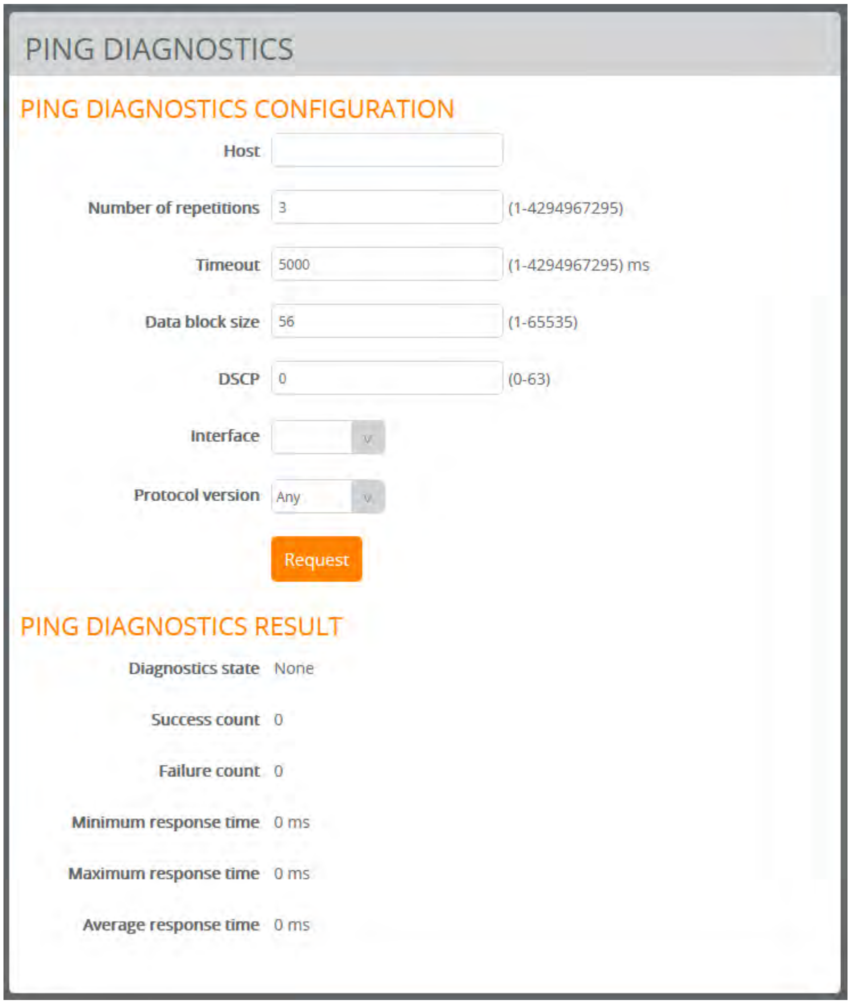


Figure 70 - QXDM over Ethernet page

3 Click the **Save** button to begin the capture and analysis of mobile signalling data.

6.4.2 Ping diagnostics

Ping Diagnostics are used to send controlled ping packets to determine the status of the link. These are small packets of data that the AurusPRO sends to a remote address and if the connection is up, a reply is received.



PING DIAGNOSTICS

PING DIAGNOSTICS CONFIGURATION

Host		
Number of repetitions	3	(1-4294967295)
Timeout	5000	(1-4294967295) ms
Data block size	56	(1-65535)
DSCP	0	(0-63)
Interface		
Protocol version	Any	

PING DIAGNOSTICS RESULT

Diagnostics state	None
Success count	0
Failure count	0
Minimum response time	0 ms
Maximum response time	0 ms
Average response time	0 ms

Figure 71 - Ping Diagnostics page

Use Ping Diagnostics to test the status of the network connection:

1. In the Host field, enter the domain name or IP address that you want to send a ping request to for the test.
2. In the Number of repetitions field, enter the number of times you want the AurusPRO to continue the ping requests.
3. In the Timeout field, enter the number of milliseconds to wait before the ping request times out if there is no response.
4. In the Data block size field, enter the number of bytes that the ping packet is made up of.

5 In the **DSCP** field, enter an integer between 0 and 63 which acts as a classification code according to the Differentiated Services Code Point (DSCP) definition.

6 In the **Interface** drop-down list, select the interface that the ping test is to be performed on. If no interface is selected, the default interface rmnet_data0 is used.

7 In the **Protocol** drop-down list, select the IP protocol to use for the test.

8 Click on the **Request** button. The **PING DIAGNOSTIC RESULT** section updates with the results of the ping request.

6.4.3 System configuration

6.4.3.1 Restore factory defaults

Restoring factory defaults will reset the AurusPRO to its factory default configuration. You may encounter a situation where you need to restore the factory defaults on your AurusPRO, such as:

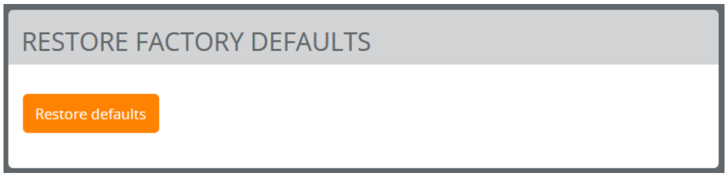
- You have lost your User name and User password and are unable to login to the web configuration page.
- You are asked to perform a factory reset by support staff.

To restore the AurusPRO to its factory default settings, please follow these steps:

1 Open a browser window and navigate to the IP address of the AurusPRO (default address is http://192.168.1.1). Login to the AurusPRO using **root** as the User Name and **admin** as the password.

2 Click the **System** item from the top menu bar, then **System configuration** on the left menu and then click the **Restore default**. Button.

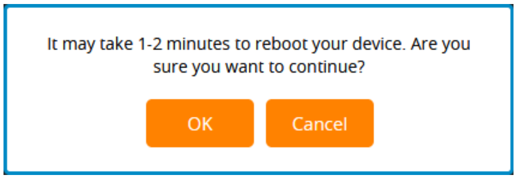
3 Under the Restore factory defaults section, click the **Restore defaults** button.



RESTORE FACTORY DEFAULTS

Figure 72 - Restore Factory Defaults page

4 A warning message will display.



It may take 1-2 minutes to reboot your device. Are you sure you want to continue?

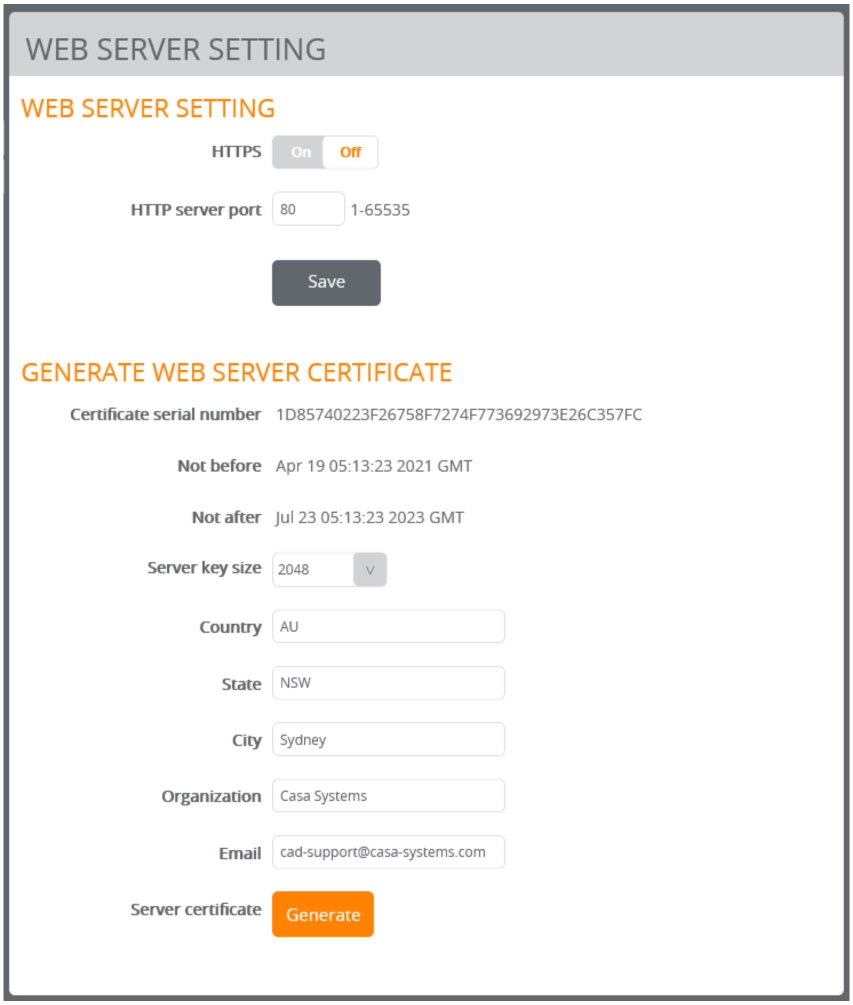
Figure 73 - Restore Factory Defaults Confirmation Message

5 Click **OK** to reboot the AurusPRO.

6 The AurusPRO reboots with the default settings applied.

6.4.3.2 Web server settings

You can configure whether the AurusPRO's web server uses HTTP or HTTPS and the server port. Additionally, you can generate a web server certificate by entering data in all the fields under the **Generate web server certificate** section.



WEB SERVER SETTING

WEB SERVER SETTING

HTTPS: On [✓ Off]

HTTP server port: 80 1-65535

GENERATE WEB SERVER CERTIFICATE

Certificate serial number: 1D85740223F26758F7274F773692973E26C357FC

Not before: Apr 19 05:13:23 2021 GMT

Not after: Jul 23 05:13:23 2023 GMT

Server key size: 2048

Country: AU

State: NSW

City: Sydney

Organization: Casa Systems

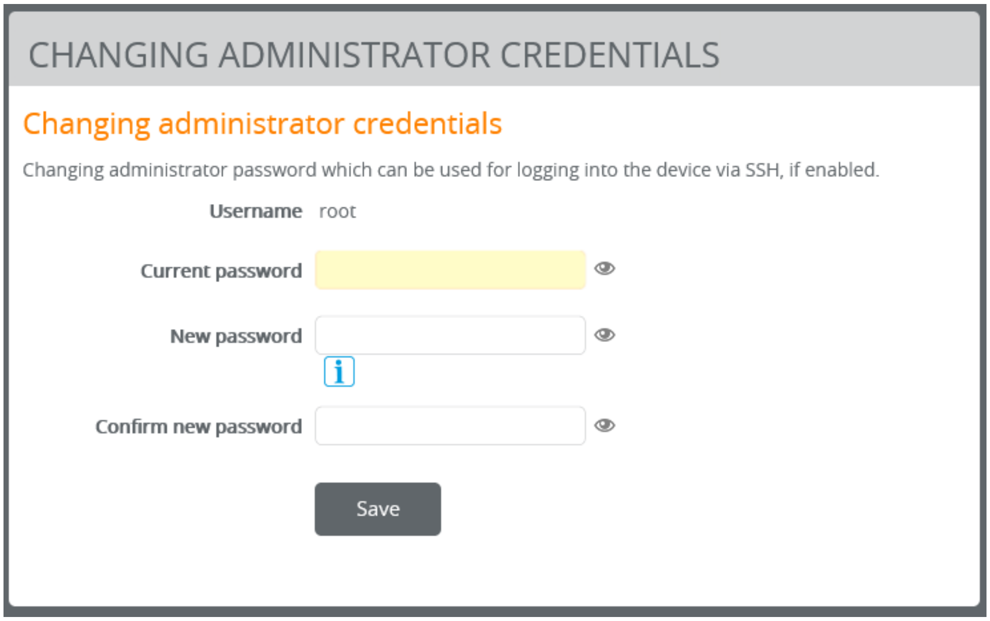
Email: cad-support@casa-systems.com

Server certificate:

Figure 74 - Web server settings

6.4.3.3 Administrator credentials

Use this page to change the **Password** used to access the AurusPRO via SSH.



CHANGING ADMINISTRATOR CREDENTIALS

Changing administrator credentials

Changing administrator password which can be used for logging into the device via SSH, if enabled.

Username root

Figure 75 - Changing administrator credentials

The default **User Name** and **User Password** for SSH access are as follows:

Administrator account access via SSH

Username	root
Password	oelinux123

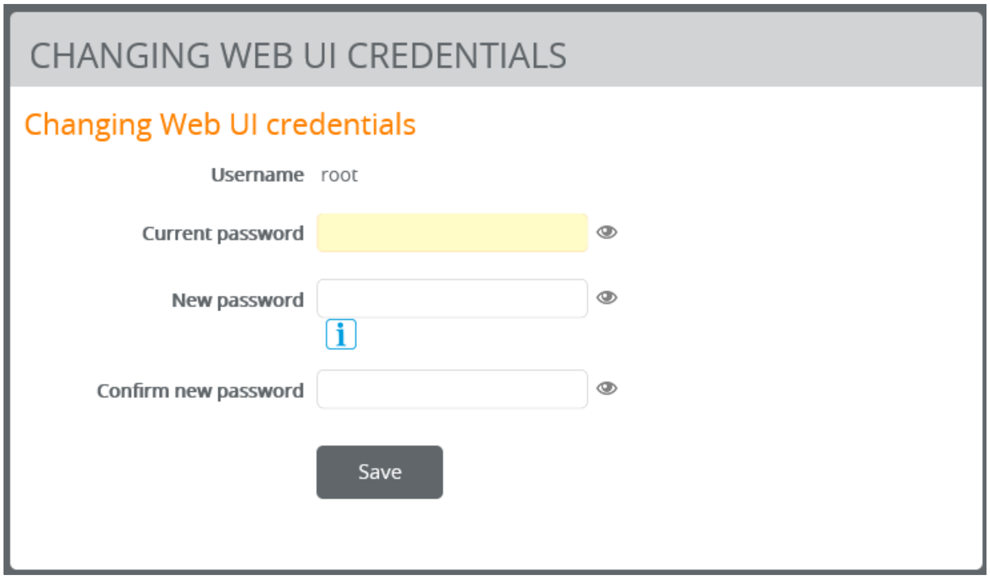
Table 19 - Login details – Administrator account via SSH

Enter the **Password** in the table to into the **Current password** field if you have not previously created a new SSH access Password.

If you have created a new SSH access Password but have forgotten it, you will have to **Restore factory default** settings, see section *6.4.3.1*, above.

6.4.3.4 Web UI credentials

Use this page to change the default **Password** that you initially used to log in via the Web User Interface (refer to section *5.1 Log in as Administrator via Web UI* on page 12).



CHANGING WEB UI CREDENTIALS

Changing Web UI credentials

Username root

Current password

New password

Confirm new password

Figure 76 - Changing web interface credentials

The default **User Name** and **User Password** for Web UI access are as follows:

Administrator account access via Web UI

Username	root
Password	admin

Table 20 - Login details – Administrator account via Web UI

Enter the **Password** in the table to into the **Current password** field if you have not previously created a new Web UI access Password.

If you have created a new Web UI access password but have forgotten it, you will have to **Restore factory default** settings, see section *6.4.3.1*, above.

6.4.3.5 Settings backup/restore

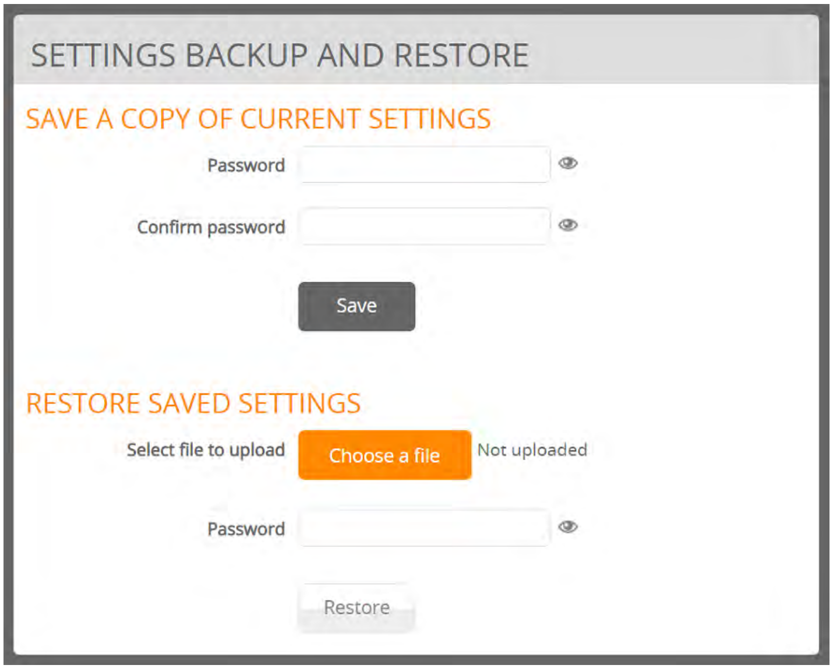
Use this page to save your current settings in a backup file and then to retrieve the backup file to restore your previous settings should this be necessary.

To **SAVE A COPY OF CURRENT SETTINGS**:

1 Enter a **Password** for the new backup file.

2 Enter the same password into the **Confirm password** field

3 Click the Save button.



SETTINGS BACKUP AND RESTORE

SAVE A COPY OF CURRENT SETTINGS

Password

Confirm password

RESTORE SAVED SETTINGS

Select file to upload

Not uploaded

Password

Figure 77 - Setting backup/restore page

A .zip folder will be downloaded to the download folder of your browser. We suggest that you move this to a secure folder.

To RESTORE SAVED SETTINGS:

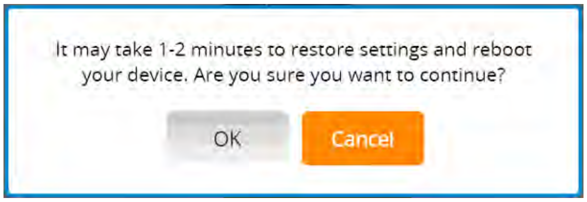
1 Click the Choose a file button and navigate to the backup file.

2 Select the file and the word Uploaded will appear after the button

3 Enter the Password you created when making the backup file.

4 Click the Restore button.

5 The following warning message will appear:



It may take 1-2 minutes to restore settings and reboot your device. Are you sure you want to continue?

Figure 78 – Confirmation of restore message

6 Click the OK button to proceed with the restoration of your previous settings.

6.4.3.6 Runtime Configuration

Runtime Configuration can be used to load a configuration file containing carrier-specific settings such as MBN changes which are not available via the web user interface. It is used for late binding of carrier configurations at the time of installation.

Runtime Configuration files can only be created by Casa Systems engineers. Please speak to your Casa Systems representative for more information.

To access the Runtime Configuration page, select System > System configuration > Runtime configuration

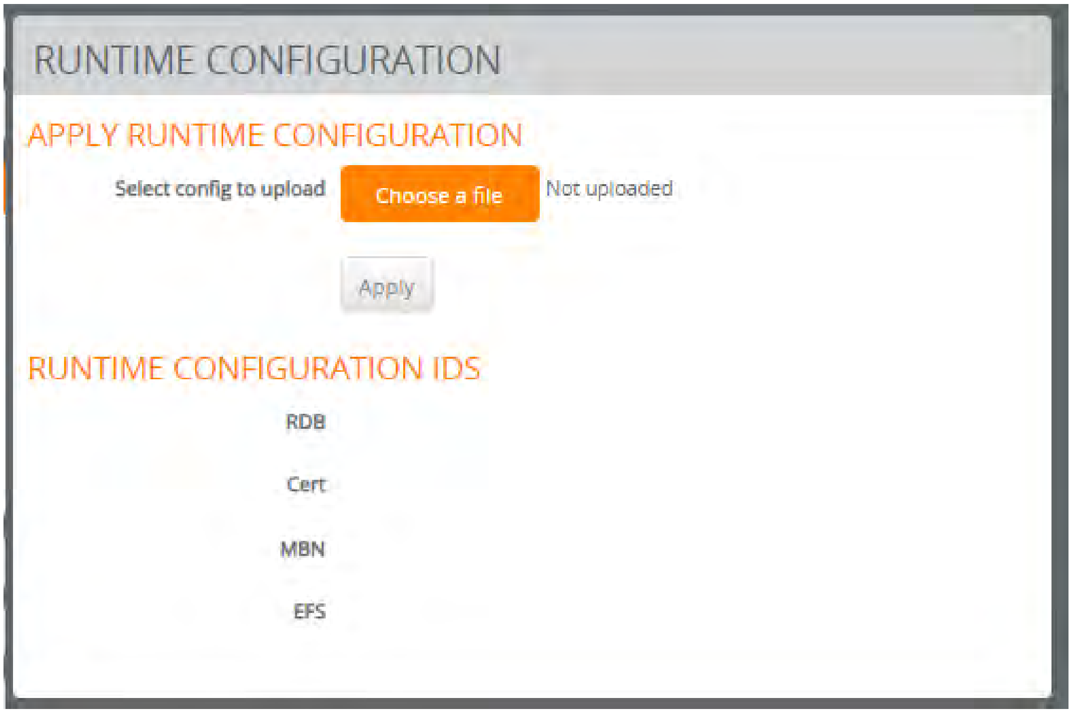


Figure 79 - Runtime configuration page

To apply runtime configuration:

1 Select the Choose a file button and locate the configuration file.

2 Select the file. The word Uploaded appears next to the button.

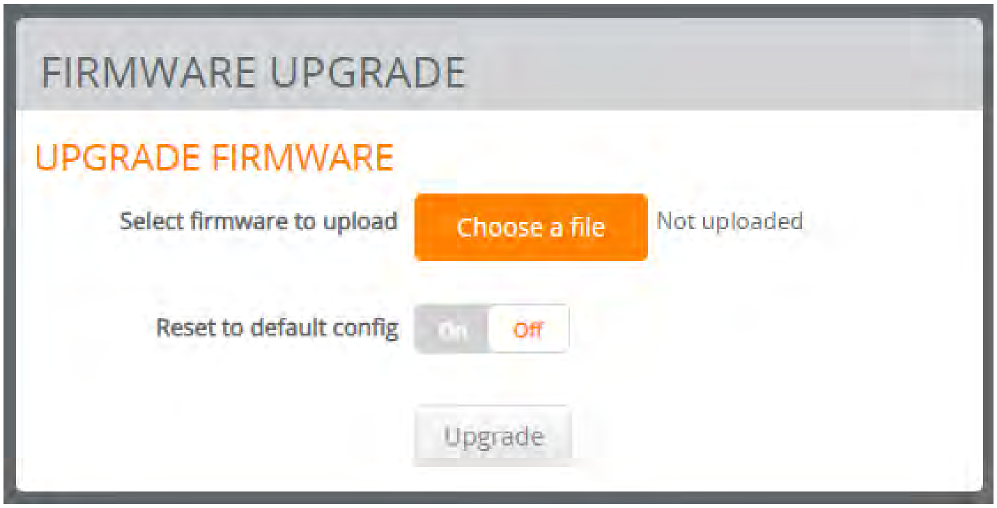
3 Select the Apply button to install the configuration file.

4 The device automatically reboots after successful upload of the configuration file.

The following runtime configuration IDs will be read and displayed on this page. They are 15-digit configuration IDs that uniquely identify the configuration file.

6.4.4 Firmware upgrade

To access the Firmware upgrade page, navigate to System, then click Firmware Upgrade on the left side menu.



FIRMWARE UPGRADE

UPGRADE FIRMWARE

Select firmware to upload Not uploaded

Reset to default config On Off

Figure 80 - Firmware Upgrade page

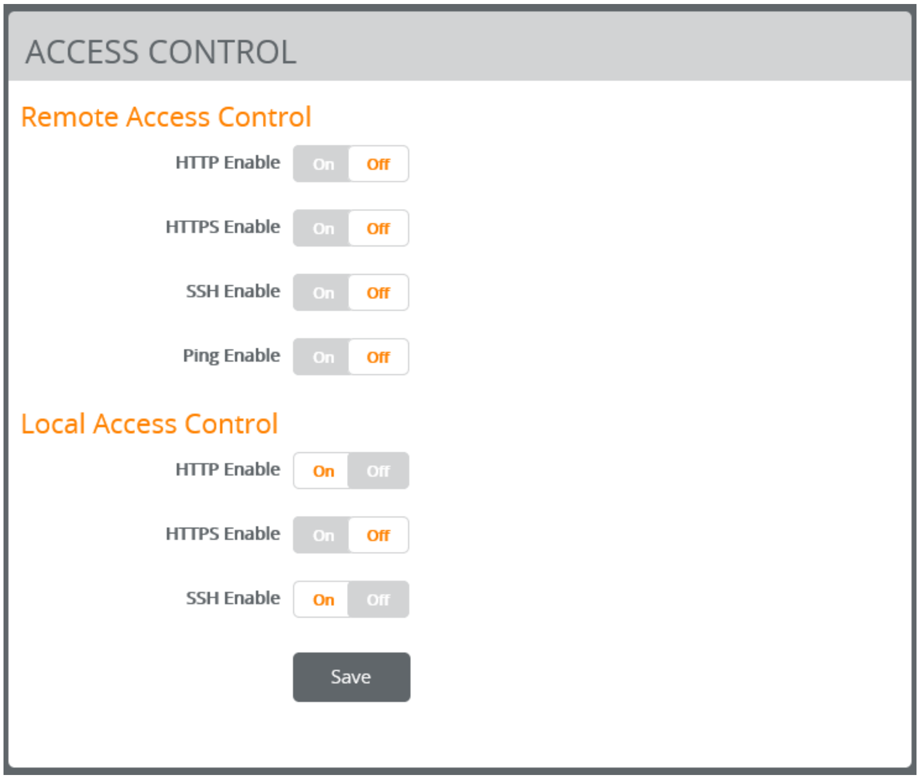
To upgrade the firmware of the AurusPRO:

1. Click the Choose a file button, then locate the firmware file on your computer.
2. To remove all current settings select On for Reset to default config.

   Selecting Off for Reset to default config will save all current user defined settings and apply them using the new firmware.
3. Click the Upgrade button.
4. The AurusPRO performs the firmware upgrade and then reboots.

6.4.5 Access control

The Access Control page turns on or off access to the antenna via different protocols. You can specify certain protocols to have different settings from local or remote connections.



ACCESS CONTROL

Remote Access Control

HTTP Enable On [✓ Off]

HTTPS Enable On [✓ Off]

SSH Enable On [✓ Off]

Ping Enable On [✓ Off]

Local Access Control

HTTP Enable [✓ On] Off

HTTPS Enable On [✓ Off]

SSH Enable [✓ On] Off

Figure 81 - Access Control page

Item	Definition
Remote Access Control	
HTTP Enable	Enables/disables HTTP access to the web interface of the antenna from a remote connection.
HTTPS Enable	Enables/disables HTTPS access to the web interface of the antenna from a remote connection.
SSH Enable	Enables/disables SSH access to the antenna from a remote connection.
Ping Enable	Enables/disables a response to pings from a remote connection.
Local Access Control	
HTTP Enable	Enables/disables HTTP access to the web interface of the antenna from a local connection.
HTTPS Enable	Enables/disables HTTPS access to the web interface of the antenna from a local connection.

Item	Definition
SSH Enable	Enables/disables SSH access to the antenna from a local connection.

Table 21 - Access Control options

Note – It is **not possible** to disable both Local HTTP and HTTPS simultaneously via the WebUI in order to stop accidental lock out of the WebUI.

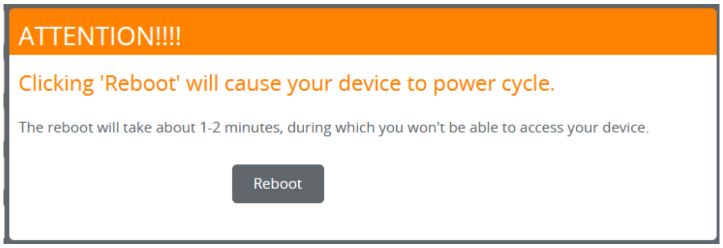
Intentional lock out of the WebUI from local access can be performed by disabling both local HTTP and HTTPS via TR-069.

6.4.6 Reboot

The **Reboot** option in the **System** section performs a soft reboot of the device. This can be useful if you have made configuration changes you want to implement.

To reboot the AurusPRO:

1. Click the **System** menu item from the top menu bar.
2. Click the **Reboot** button from the menu on the left side of the screen.
3. The AurusPRO displays a warning that you are about to perform a reboot.



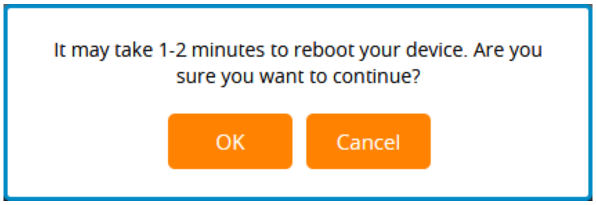
ATTENTION!!!!

Clicking 'Reboot' will cause your device to power cycle.

The reboot will take about 1-2 minutes, during which you won't be able to access your device.

Figure 82 - Reboot message

4. If you wish to proceed, click the **Reboot** button.
5. A warning popup will advise that "*It may take 1-2 minutes to reboot your device. Are you sure you want to continue?*"



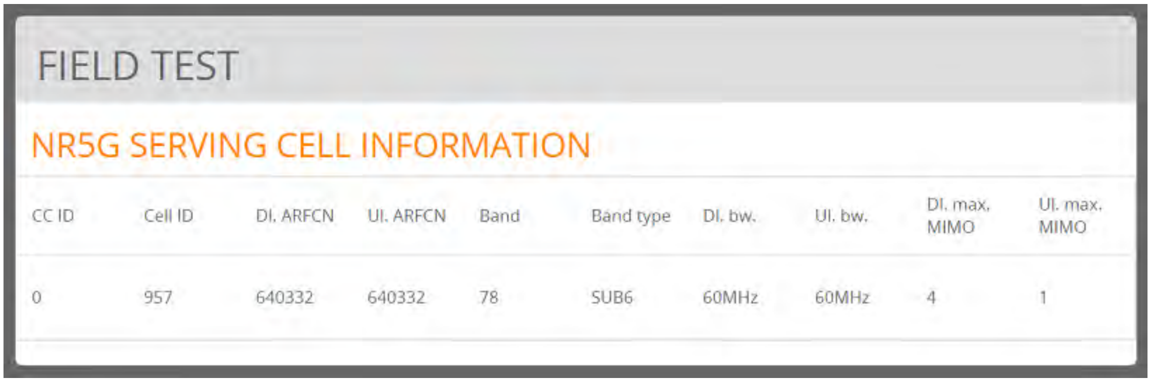
It may take 1-2 minutes to reboot your device. Are you sure you want to continue?

Figure 83 - Reboot confirmation message

6. Click **OK** to continue with the reboot process.

6.4.7 Field test

The Field test page contains NR5G cell information which may be useful when troubleshooting signal strength issues. This screen can be found by navigating to System > Field test.



FIELD TEST

NR5G SERVING CELL INFORMATION

CC ID	Cell ID	Dl. ARFCN	Ul. ARFCN	Band	Band type	Dl. bw.	Ul. bw.	Dl. max. MIMO	Ul. max. MIMO
0	957	640332	640332	78	SUB6	60MHz	60MHz	4	1

Figure 84 - Field test

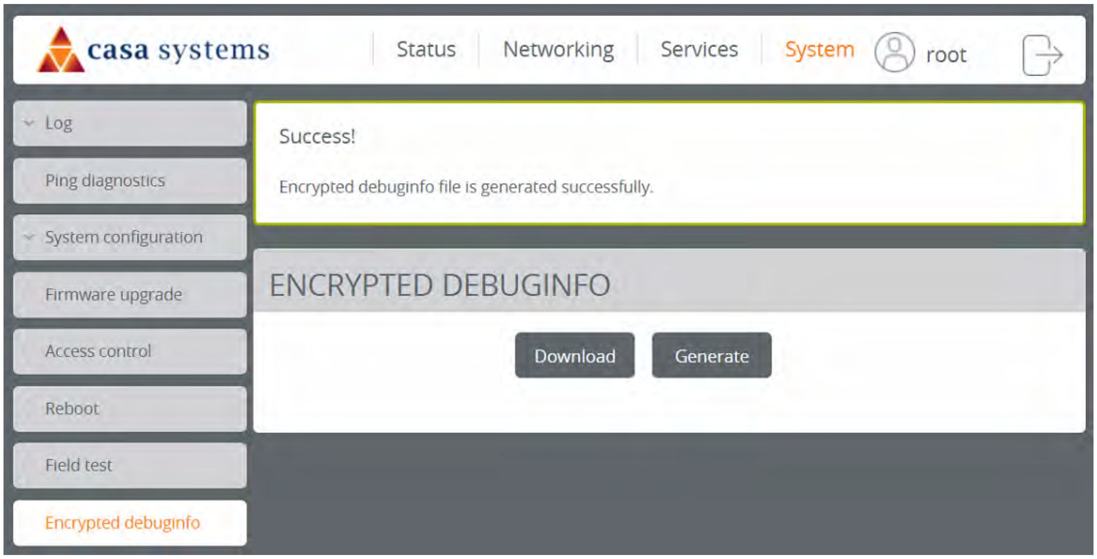
NR5G Serving Cell Information	
CC ID	Component Carrier ID.
Cell ID	The physical cell identifier.
Dl. ARFCN	Downlink Absolute Radio Frequency Channel Number.
Ul. ARFCN	Uplink Absolute Radio Frequency Channel Number.
Band	The NR5G band.
Band Type	The type of the NR5G band, e.g. Sub6 or mmWave.
Dl. bw.	Downlink bandwidth.
Ul. bw.	Uplink bandwidth.
Dl. max MIMO	Downlink maximum Multiple Input Multiple Output.
Ul. max MIMO	Uplink maximum Multiple Input Multiple Output.

Table 22 - NR5G Serving cell information

6.4.8 Encrypted Debug Information

The Encrypted Debug Information page contains additional information which may be useful when troubleshooting an issue.

To create a debug file navigate to **System > Encrypted Debug Information.**



Success!

Encrypted debuginfo file is generated successfully.

ENCRYPTED DEBUGINFO

Figure 85 - Encrypted Debug Information page

6.4.8.1 Generate

Click the **Generate** button to create a debug file.

While the generation process is taking place the browser will be unavailable and the message “*Please wait*” will be displayed.

After a few minutes the generation process will end, the browser will become available and the “*Success – Encrypted debuginfo file is generated successfully*” message will be displayed at the top of the page.

6.4.8.2 Download

Click the **Download** button to download the new file into your browser’s default downloads folder.

The following debug file will be saved in your browser’s default downloads folder: **`debuginfoX.tar.gz`**

Appendix A – Safety and compliance

RF Exposure

Your device contains a transmitter and a receiver. When it is on, it receives and transmits RF energy. When you communicate with your device, the system handling your connection controls the power level at which your device transmits.

This device meets the government’s requirements for exposure to radio waves.

This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

This equipment complies with radio frequency (RF) exposure limits adopted by the Federal Communications Commission for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator and your body.

FCC Statement

This device must be professionally installed.

FCC compliance

Federal Communications Commission Notice (United States): Before a wireless device model is available for sale to the public, it must be tested and certified to the FCC that it does not exceed the limit established by the government-adopted requirement for safe exposure.

FCC regulations

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device 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 in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

Operating temperature

- -40ºC to 55ºC

Company details

Casa Systems, Inc.

100 Old River Road, Andover, Massachusetts 01810 USA

https://www.casa-systems.com/contact-us/

Product details

Product: CBRS 5G Cat B Outdoor CPE

Model No: CFW-2832

Appendix B – Configuring Radio Access Technologies

This device supports the following modes of operations in various combinations

- LTE (3GPP Core Network Option 1)
- 5G Non Standalone (3GPP Core Network Option 3x)
- 5G Standalone (3GPP Core Network Option 2)

Please refer to the following table to understand which modes of operation are possible and how to configure them.

	Allowed RAT				How to Configure	
Mode	LTE	5G NSA	5G SA	Supported	RAT Selection Menu	Band Selection Menu
LTE Only	Yes	No	No	Yes	Select LTE only	Select LTE Frequency Bands
LTE + 5G NSA	Yes	Yes	No	Yes	Select LTE + 5G NR	Select LTE + NSA Frequency Bands
5G NSA Only	No	Yes	No	No	–	–
LTE + 5G NSA + 5G SA	Yes	Yes	Yes	Yes	Select LTE + 5G NR	Select LTE + NSA + SA Frequency Bands
LTE + 5G SA	Yes	No	Yes	No	–	–
5G NSA + 5G SA	No	Yes	Yes	No	–	–
5G SA Only	No	No	Yes	Yes	Select 5G NR	Select SA Frequency Bands

Appendix table 1 – RAT/Band Selection table

Use this table in conjunction with the settings described in sections *6.2.1.3 RAT selection* and *6.2.1.2 Band selection* of this guide.

Note – 5G Standalone Mode is not supported when utilising mmWave frequency bands.