User Guide (Carrier)

AurusLink+ Outdoor CPE

Release 16 Self Install

Model CFW-3211/3212

Doc No. UG01437

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 AurusLINK+ 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

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

Document history

This document applies to the following CPE model:

AurusLink+ Outdoor CPE – CFW-3211/3212

Ver.	Document description	Date
v1.00	Initial document release	23 December, 2022

Table i. – Document revision history

Contents

1 Document overview

1.1 Introduction

This document provides all the information needed to set up, configure and deploy the CFW-3211/3212 Outdoor CPE antenna.

1.1.1 Organisation of this Document

This Carrier User Guide Is designed for use by a carrier's technical support personnel, it includes two sections:

Section 1 – Device description and general overview of end-user installation

This section is designed to give end-users all the information they need to understand their new device and install it using the recommended Smartphone application method.

A separate *User Guide* for end-users is planned to be produced containing only this first section.

Section 2 – Device configuration details

The second section is designed to give technical personnel of the ISP in depth descriptions of all advanced settings available in the CPE.

This allows each ISP to preconfigure their devices to their individual requirements or alternatively allows them to reconfigure units remotely.

The contents of this *User Guide* contains both sections and is meant for use by ISP technicians.

1.2 Target audience

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

Specifically it is for carrier technicians who will pre-configure the Outdoor CPE devices prior to distribution to end users. Also included are the installation instructions which the end user will use to install the device on their own premises.

Note – It is assumed by Casa Systems that end users will not be expected to log in to WebUI at any time, nor will they be provided any of the username / password credentials.

1.2.1 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

The AurusLINK+ Outdoor CPE is a self-Install, Release 16 CPE device that allows easy connection to mobile networks providing access to broadband Internet. The unit itself is specified as an outdoor product in terms of IP rating, environmentals, etc.

The AurusLink+ Outdoor CPE is designed to be affixed by adhesive tape on the exterior of a window. If windows cannot be opened, for example in a high rise building, the CPE can be affixed to the inside of the window.

2.2 Package contents

The in-box contents include:

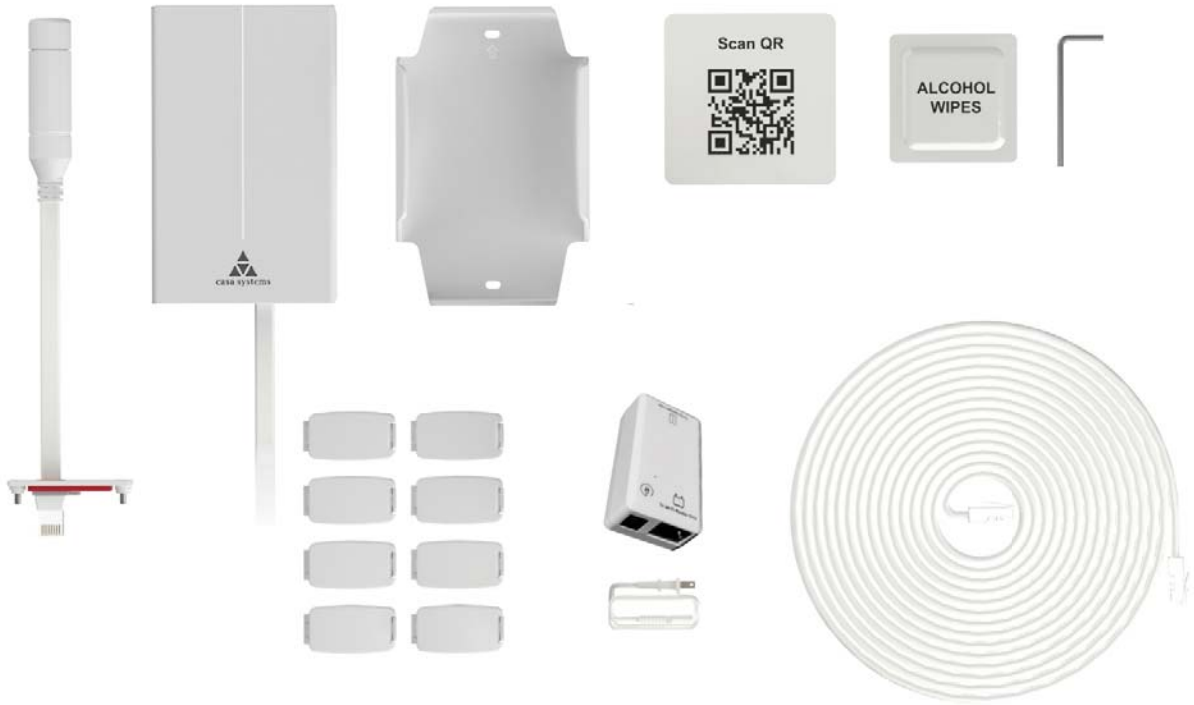


*Figure 1 – Package contents**[images not to scale]***

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

2.2.1 Other tools required

- 1 x Smartphone with the Aurora Installation application installed used during installation.

3 Physical dimensions and interfaces

3.1 Physical dimensions

3.1.1 CFW-3211/3212

Below are details of the layout and physical dimensions of the CFW-3211/3212.

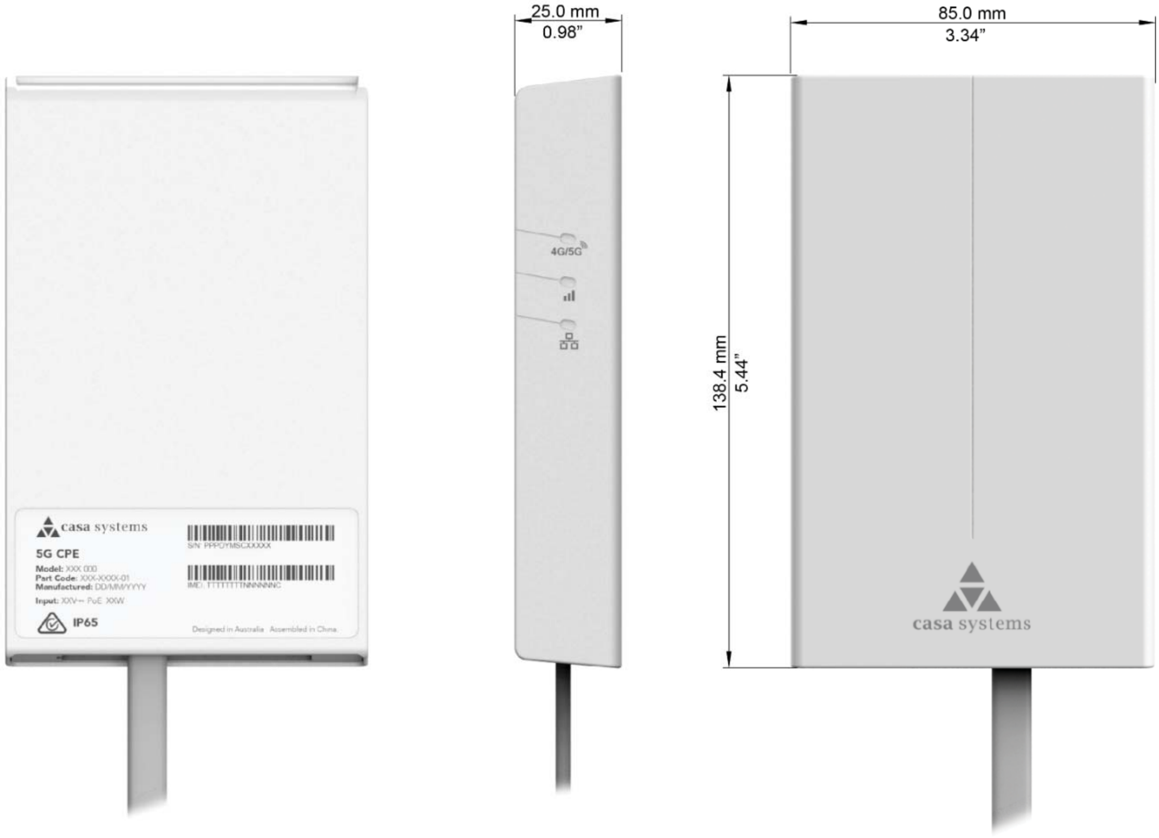


Figure 2 – CFW-2211/3212 Outdoor CPE dimensions

CFW-3211/3212 Dimensions

Height	138.4mm (5.44 in)
Width (excluding mount)	85mm (3.34 in)
Depth (excluding mount)	25mm (.98 in)
Weight (excluding mount)	~240gr (~ 8.5oz)

Table 1 - CFW-3211/3212 device dimensions

3.2 Interface

3.2.1 CFW-3211/3212

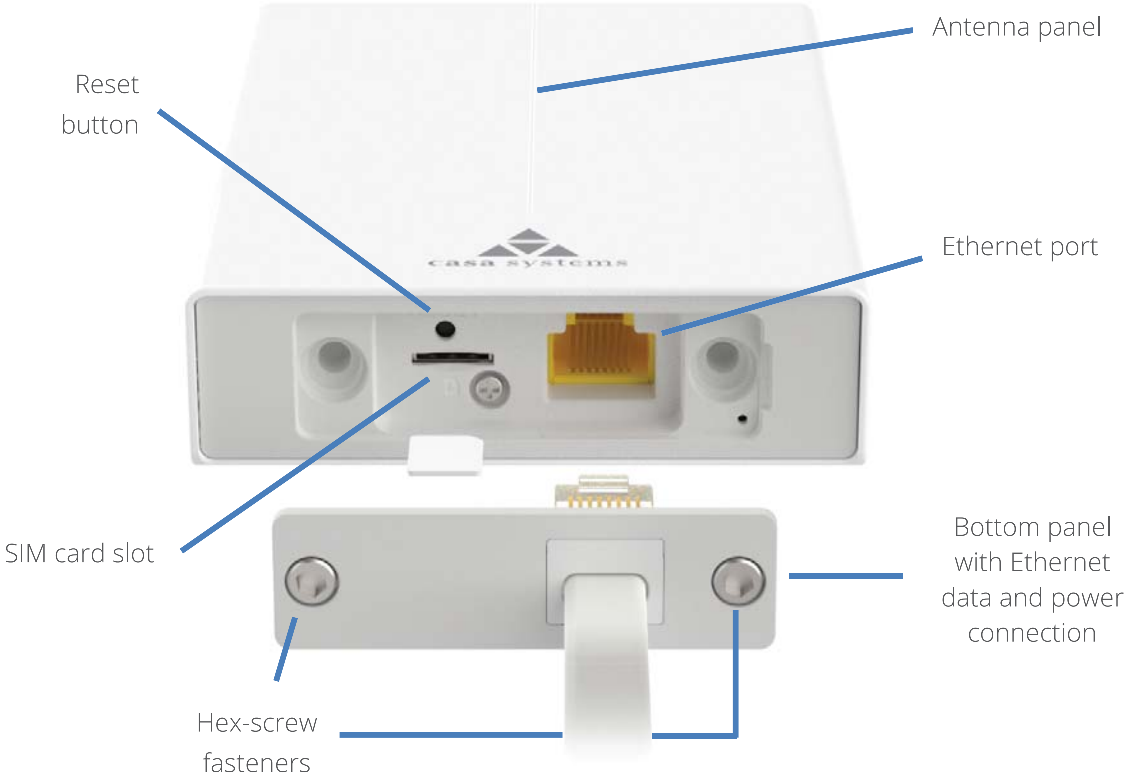


Figure 3 – Interfaces – CFW-3211/3212

Item	Description
Bottom of the CPE	
Antenna panel	Includes an integrated 4x4 MIMO Low-Gain OMNI Directional Antenna
Reset button	Push a thin wire such as a paperclip into this small opening to reset the device. This button provides two options: • Press and hold for less than 5 seconds to reboot to Normal mode. This will restart the unit with the same configuration settings • Press and hold for 5 to 15 seconds to reset the router to its Installer level settings This will restart the unit with the same settings present at installation time.

Item	Description
	Other Reset Options This Installer Reset is the safest reset option and should be the first one attempted when troubleshooting a problem. In addition to Installer Reset two other types of reset are available through the User Interface: Carrier Reset and Full Factory Reset For more information on the differences between these three options, go to section 6.4.3.1 Restore factory defaults of this guide.
SIM slot	Insert the Nano SIM 4FF here, if the correct side is up it will clip into place. If it does not clip into place, remove the SIM and turn it or flip it and try again.
Ethernet Port	Connect the Ethernet connector which passes through the bottom panel into the Ethernet port. The Ethernet provides power and data connectivity to the Power over the Ethernet (PoE) device inside the premises.
Screw holes (2)	Threaded screw holes for the two Hex-screw fasteners on the bottom panel
Bottom Panel	
Bottom cover panel	The bottom cover panel has the Ethernet cable passing through it. Once the Ethernet cable is plugged into the Ethernet port the bottom panel will fit into the recess on the bottom of the antenna box
Hex-screw fasteners	Use the supplied hex wrench to tighten the bottom panel onto the bottom of the antenna box

Table 2 – Interfaces – CFW-3211/3212

3.2.2 PoE injector

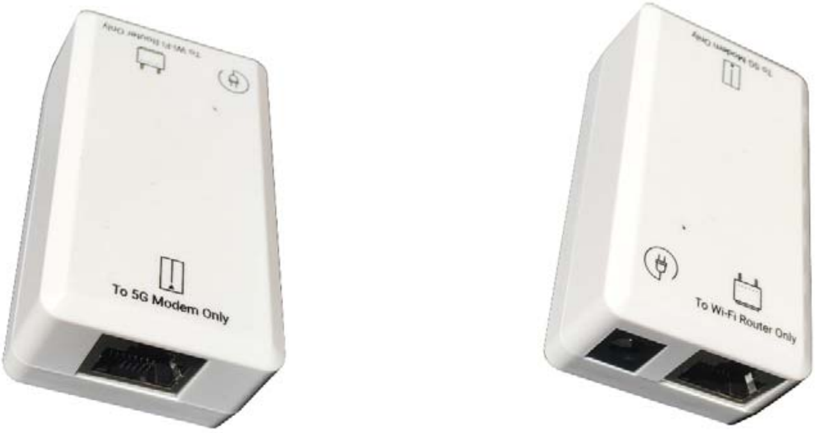


Figure 4 – CFW-2211/3212 PoE injector dimensions

CFW-3211/3212 Dimensions

Length	~68mm (.98 in)
Width	~39mm (3.34 in)
Height	~25mm (~ .98in)
Weight	~35gr (~1.25oz)

Table 3 - CFW-3211/3212 PoE injector dimensions

3.3 LED indicator lights

3.3.1 CFW-3211/3212

Below are details of the colour, actions and meaning of the three LED lights on the side of the CFW-3211/3212.

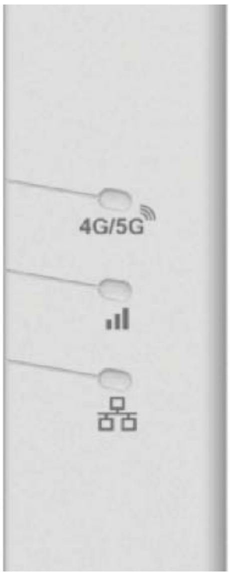


Figure 5 – CFW-2211/3212 LED indicator lights

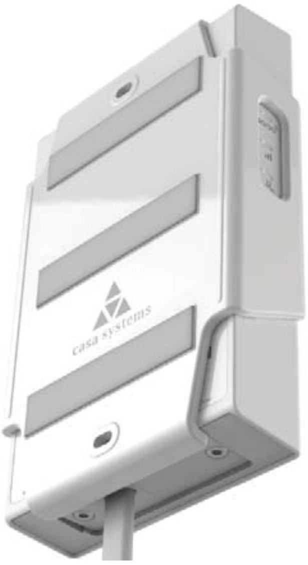


Figure 6 – LED cut out on side of mounting bracket

Icon	LED Color	Action	Indicated status
4G/5G	Blue	Solid	Connected to WWAN
	Red	Solid	SIM PIN/PUK locked / Other connectivity issues related to WWAN (e.g. wrong APN, etc.)
	Blue	Flashing	Device booting
📶	Blue	Solid	Signal strength is good/excellent -105dBm = < RSRP and 10 = < SINR (values could be re-defined by one RD8 for "good RSRP threshold" and one RDB for "good SINR threshold")
	Green	Solid	Signal strength is fair -105dBm > RSRP and 10 > SINR (values could be re-defined by above RD8s)
	None	Off	No service, limited service

Icon	LED Color	Action	Indicated status
🖧	Green	Flashing	Device starting up
	Green	Solid	Ethernet to RG established
	None	Off	Ethernet to RG not established

Table 4 - CFW-3211/3212 LED display

3.3.2 LED Auto-dim functionality

The AurusLINK+ LEDs are programmed by default to switch themselves off 30 minutes after power up to reduce unwanted inside and outside glare of the LEDs through the Window. The user has the option to override this feature during installation via the Aurora Installation APP.

When the Auto LED off feature is enabled, the LEDs will only come back on either:

- when an Error situation (indicated by a RED LED) occurs, or
- when the device is rebooted via the power switch.

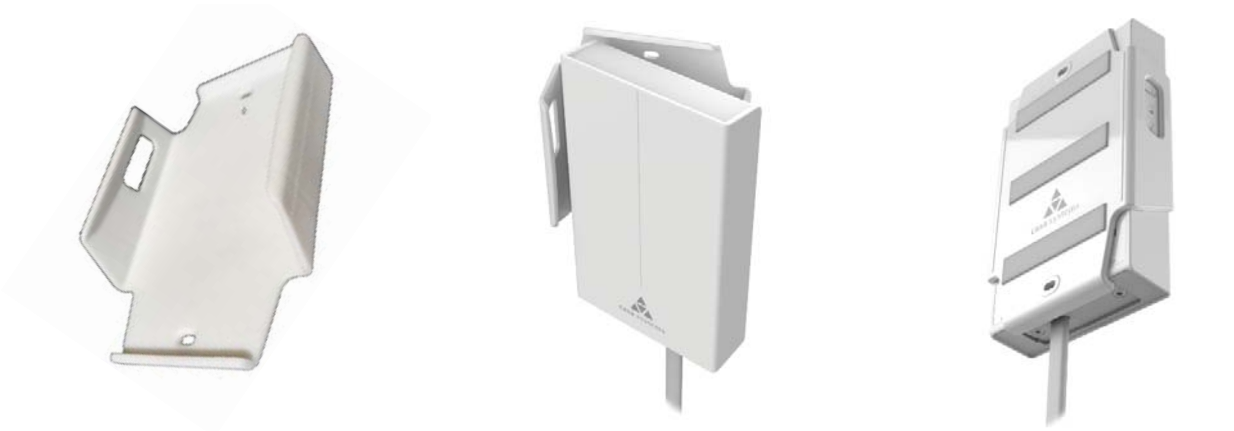
If the LEDs come back on, then once all red LEDs disappear the timer for the "Auto LED Off" feature shall be started again.

The carrier has the option to change the timer value from 30 minutes in the factory.

3.4 Mounting bracket

The AurusLINK+ 5G Outdoor CPE antenna uses a plastic mounting bracket that is stuck with strips of special adhesive tape which will stick to the window but is not sticky to touch.

The mounting bracket can be fixed to either the outside (preferred option) or inside of an external window and may be moved multiple times provided that each window location was thoroughly cleaned with the supplied alcohol wipes prior to fixture.



Empty bracket with LED cutout and up arrow

CPE being snapped into bracket

CPE and Bracket with adhesive strips

Figure 7 – Plastic Mounting bracket

Note – Other types of mounting brackets(wall/pole/rail) are available, contact Casa Systems sales or product support if required.

3.4.1 Mounting bracket assembly instructions

Important – Prior to mounting, you should identify the best location using the Aurora AP, and refer to section 4 of this User Guide.

1 Note the direction of the arrow on the inside of the mounting bracket.

2 Snap the CPE onto the mounting bracket with the top of the casing oriented to the top of the bracket as indicated by its up ⇧ arrow.

The LED lights should be visible through the LED cut out on the side of the mounting bracket.

3 Clean the window where you intend to mount the bracket with the supplied alcohol wipes.

4 Peel off the paper covers on the three adhesive strips on the back of the mounting bracket.

5 Firmly press the mounting bracket and antenna against the glass so that the adhesive sticks.

3.4.2 Overview of completed mounting

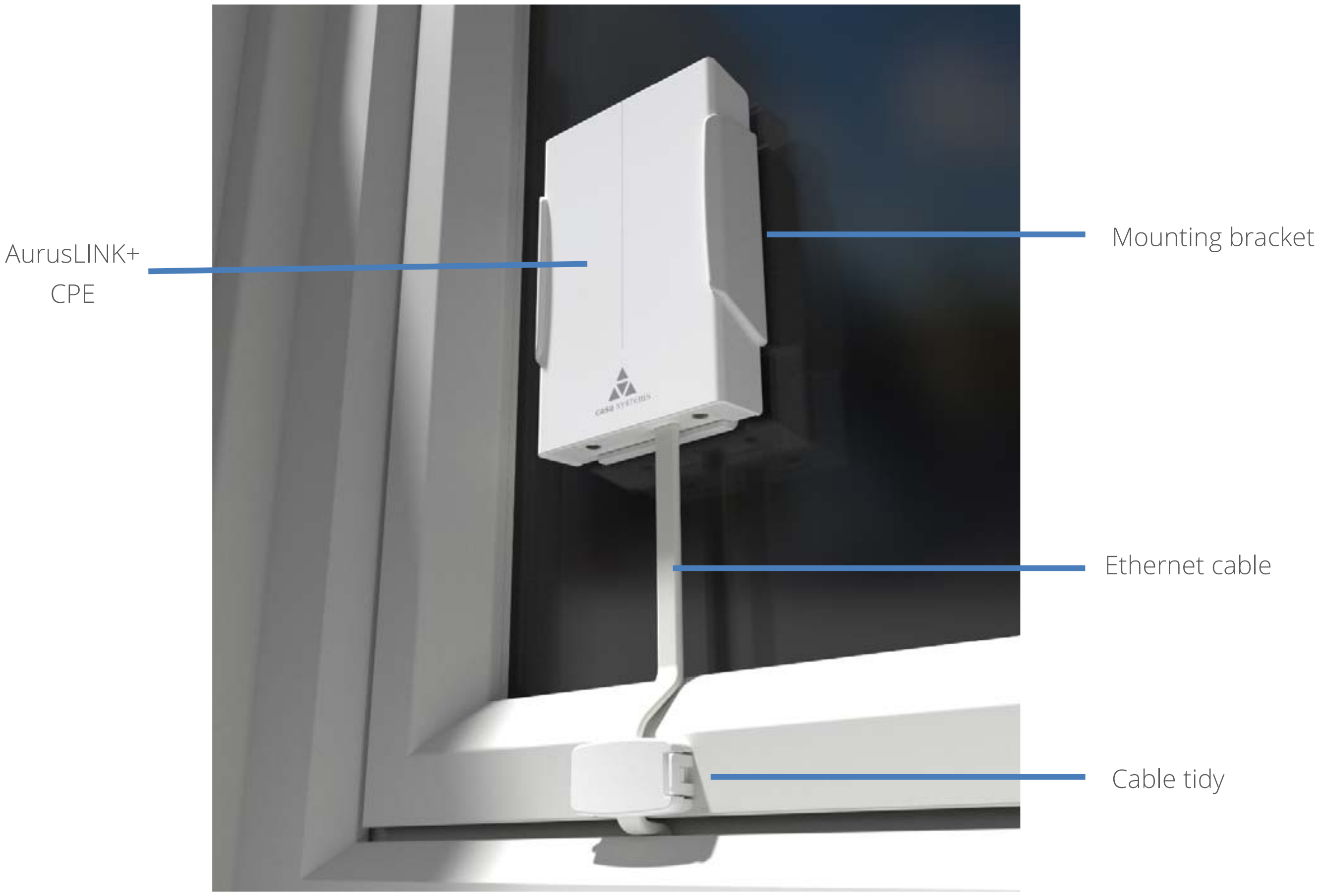


Figure 8 - CFW-3211/3212 with mounting bracket attached to window

4 Aurora Smartphone installation APP overview

The Android and IOS Smartphone application (freely available on appropriate APP stores) is designed to aid the consumer through the installation process.

The Smartphone application provides all the guidance required by the end consumer to set up and start the antenna: from unboxing, through site survey measurements around the home, and then final installation,

Utilising easy to understand terminology and graphics, combined with non technical language and performance indicators, the application is suitable for non technical end-consumers.

ⓘ Note – If you do not have a Smartphone, the installation is possible utilising the LED lights on the side of the device. Contact the Customer Service department of your service provider for more information.;

4.1 Download App

Open a fully charged Android or IOS Smartphone.

4.1.1 Scan QR code

The QR code is located on the side of the box that the CPE came in:

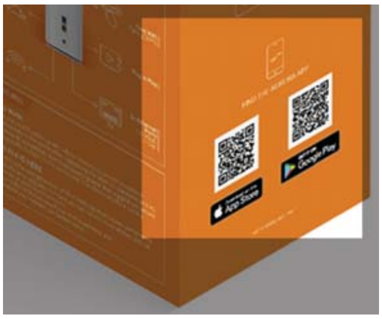


Figure 9 – QR codes on the side of the packing box

Scan the QR code that corresponds to your type of Smartphone.

ⓘ Note – If the QR codes are not present on the box, then the instruction and QR code can be found on the welcome card inside the box

Follow the instructions on your Smartphone to download and install the app.

ⓘ Note – If you cannot download the application using the QR code, you can go to either the

- App store (for iPhones), or
- Goggle Play (for Android phones),

search Aurora Installation Application and download and manually install it.

4.2 Prepare the device

4.2.1 Insert SIM card

There are two options for SIM card provision:

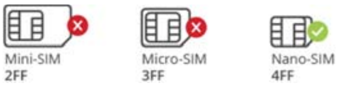
- For some carriers the SIM card will already be pre-inserted, and hence this step (4.2.1) and the next (4.2.2) will not be required.
- For carriers where the SIM card will not be pre-inserted steps 4.2.1 and 4.2.2 will be required.

To insert a SIM card.

1 If the bottom panel with ethernet cable is attached, using the supplied hex key to unscrew the two Hex screws on the bottom panel and lift off the panel to reveal the SIM card slot

2 While holding the SIM card relative to the front of the antenna casing, orient the SIM card so that the metallic circuits are facing upward and the clipped corner is in the top right.

Note – Use *only* the Nano-SIM 4FF supplied by your provider.



3 Push the SIM card into the slot as shown below.

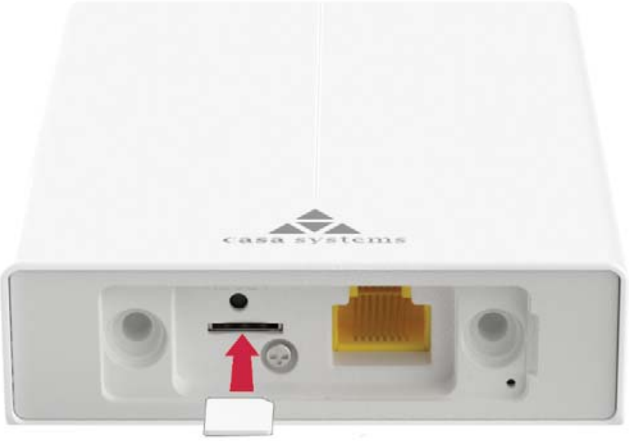


Figure 10 – Placing the SIM card into the SIM card reader

The SIM card slot employs a 'Push Push' system to lock the card in place.

Push the SIM card in once and the spring locking mechanism will click to secure the SIM card in the slot.

When locked in place a small amount (~1mm) of the card will protrude off the face of the bottom panel.

4 To remove the SIM card, rapidly push the SIM card in twice and the spring will eject the card.

4.2.2 Connect Ethernet cable and bottom panel to device

Connect the end of the Ethernet cable on the inside of the weatherproof joiner to the port on the bottom of the CPE.

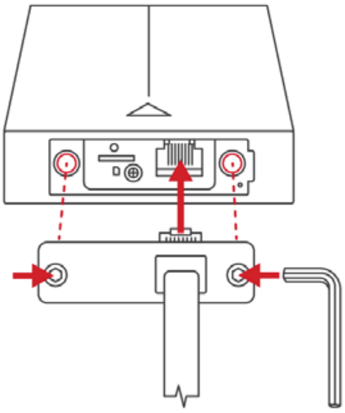


Figure 11 – Fix waterproof panel to bottom of CPE diagram

Place the weather seal over the end of the device and use the Allen key tool to tighten the bolts.

4.2.3 Connect Ethernet cable to PoE injector

Connect the other end of the 5m Ethernet cable to the side of the supplied Power supply marked ”To 5G modem only”.

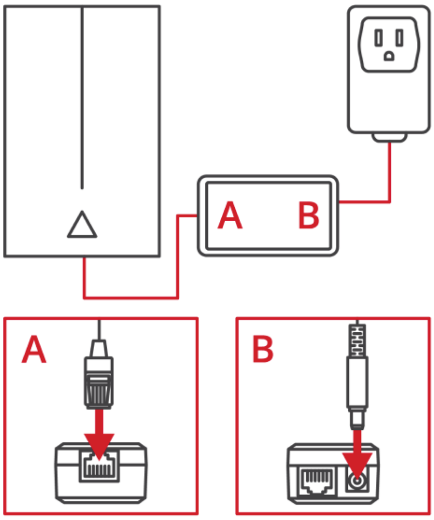


Figure 12 – PoE connection diagram

4.2.4 Power on your device

Connect the power supply to a power outlet.

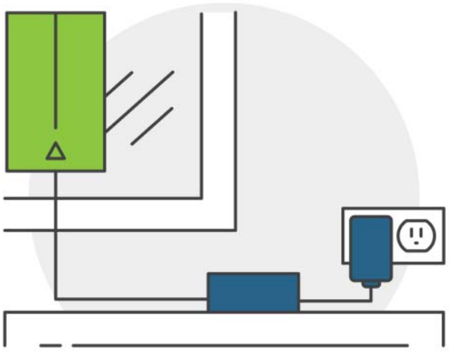


Figure 13 – Power point close to window diagram

The power point must be within 5 meters of the window.

4.2.5 Connect device to Smartphone app

If you do not already have the App on your Smartphone, install the App using the QR code printed on the CPE's label.

Open your smartphone and click the App icon.

The Smartphone App will guide you through how to connect to your CPE.

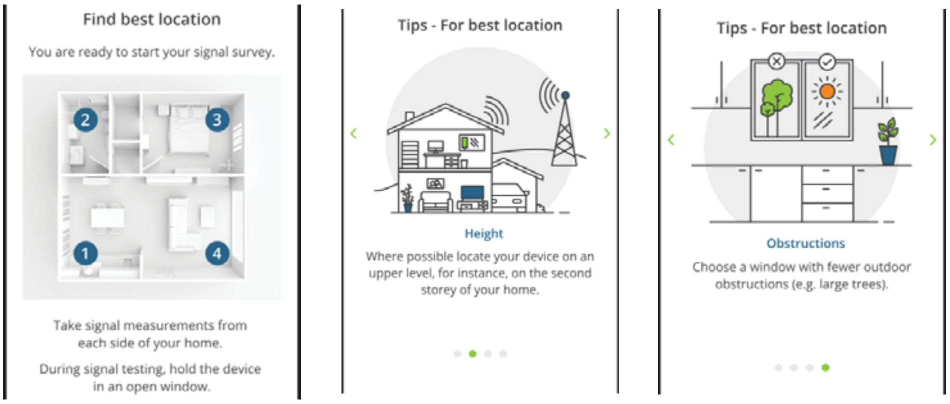
When the app has connected to the device, the app will indicate "Success".

4.3 App Installation

Follow the steps in the App on your Smartphone to complete the installation.

4.3.1 Site survey

Find the best location, the app includes Tips to find the best location”



Find best location

You are ready to start your signal survey.

Take signal measurements from each side of your home.

During signal testing, hold the device in an open window.

Tips - For best location

Height

Where possible locate your device on an upper level, for instance, on the second storey of your home.

Tips - For best location

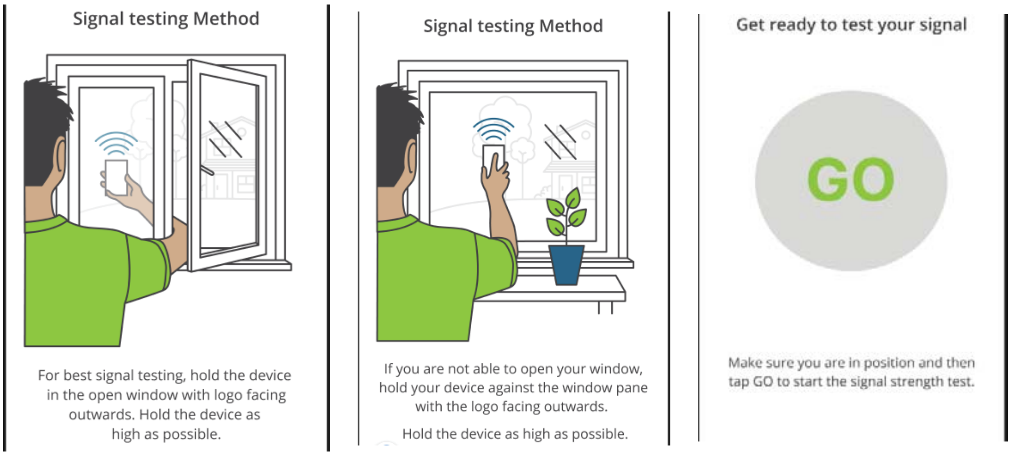
Obstructions

Choose a window with fewer outdoor obstructions (e.g. large trees).

Figure 14 – Plan the site survey

4.3.2 Perform signal reception Tests

For best signal testing, hold the device in the open window with logo facing outwards. Hold the device as high as possible.



Signal testing Method

For best signal testing, hold the device in the open window with logo facing outwards. Hold the device as high as possible.

Signal testing Method

If you are not able to open your window, hold your device against the window pane with the logo facing outwards.

Hold the device as high as possible.

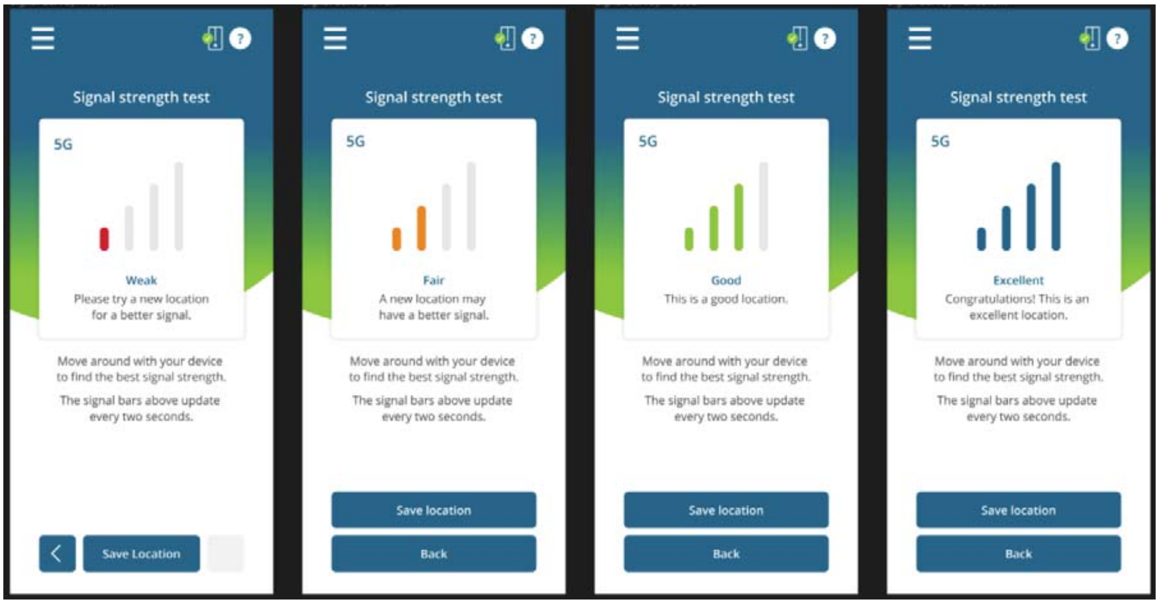
Get ready to test your signal

Make sure you are in position and then tap GO to start the signal strength test.

Figure 15 – Signal testing

4.3.3 Save good or excellent locations

When you get a good or excellent for a location click the Save location button to add it to the app.



Please try a new location for a better signal.

A new location may have a better signal.

This is a good location.

Congratulations! This is an excellent location.

Move around with your device to find the best signal strength.

The signal bars above update every two seconds.

Figure 16 – Test signal strength

4.3.4 Identify each possible location

When saving good or excellent locations, add a meaningful name so that you can identify which window it relates to.

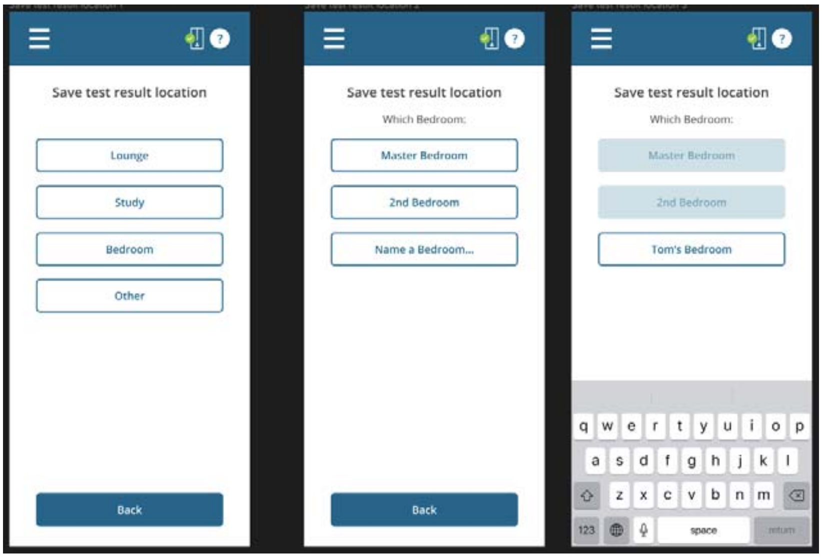
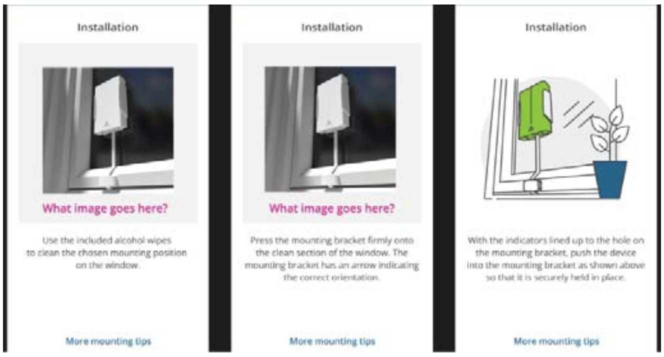


Figure 17 – Record acceptable locations

4.3.5 Install at best location



Use the included alcohol wipes to clean the chosen mounting position on the window.

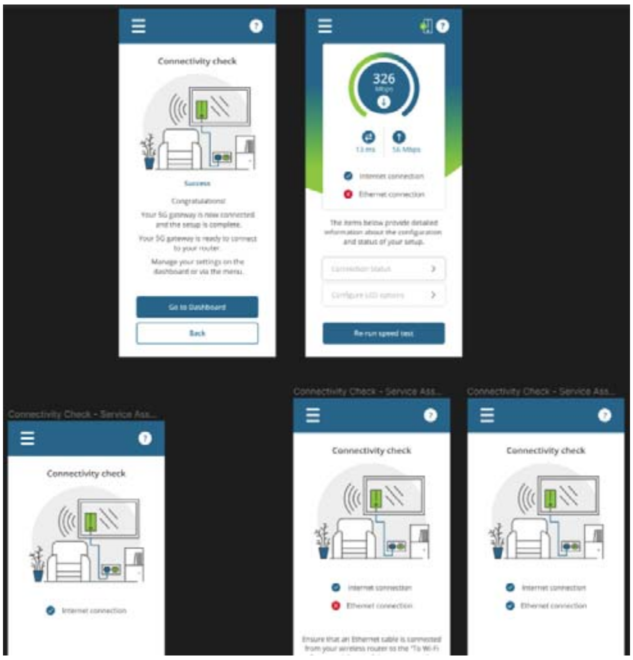
Press the mounting bracket firmly onto the clean section of the window. The mounting bracket has an arrow indicating the correct orientation.

With the indicators lined up to the hole on the mounting bracket, push the device into the mounting bracket as shown above so that it is securely held in place.

Figure 18 – Install the device on window

4.3.6 Perform connection check

Once installed, connect to router and perform a connection check following the instructions in the app.



Success

Congratulations!

Your 5G gateway is now connected and the setup is complete.

Your 5G gateway is ready to connect to your router.

Manage your settings on the dashboard or via the menu.

The items below provide detailed information about the configuration and status of your setup.

Ensure that an Ethernet cable is connected from your wireless router to the "To Wi-Fi

Figure 19 – Perform connection check

4.3.7 Success – enjoy internet access

The AurusLINK+ is now installed. The APP can now be closed.

In the case of Red LEDs appearing in the future, the user should consult the APP for instructions.

5 Advanced set up of the AurusLINK+

The AurusLINK+ 5G Outdoor CPE series of antennas all use the same firmware.

The AurusLINK+ CFW-3211/3212 will be shipped pre-configured for the carrier.

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

⚠ Important – It is NOT INTENDED for End Users (Consumers) to have access to the Web UI of this device.
The configuration tools and settings contained in this section of this Carrier User Guide are only for the information of carrier technicians and should not be made available to the end user.

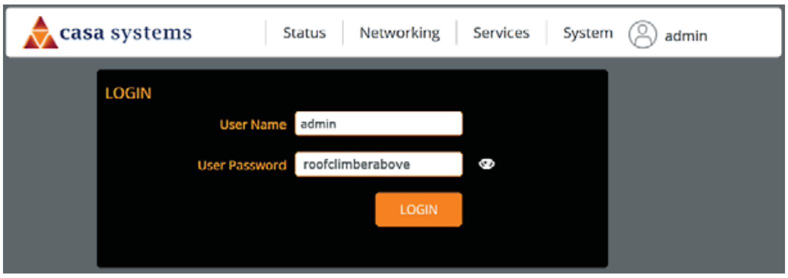
5.1 Log in as Administrator via Web UI

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**.

⚠ Important – Some service providers/carriers have opted to use a different URL to access the Web UI.
If you encounter difficulty logging in, consult the instructions provided by your service providers/carriers or contact your service provider/carrier's technical support.

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



User Name admin

User Password roofclimberabove

Figure 20 – Log in prompt for the web-based user interface

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

Administrator account

User Name	admin
User Password	roofclimberabove

Table 5 - Management account login details – Administrator account

⚠ Important – Please note that manufacturer recommends that the User Password be changed by the mobile carrier at the time of factory production prior to shipping to the end user.
If you do not know the new password, or if the default value "roofclimberabove" does not work on first time installation, please contact your local mobile carrier or Casa Systems representative.

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.

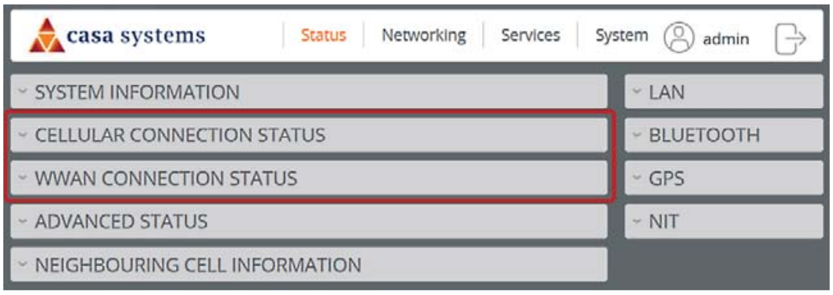
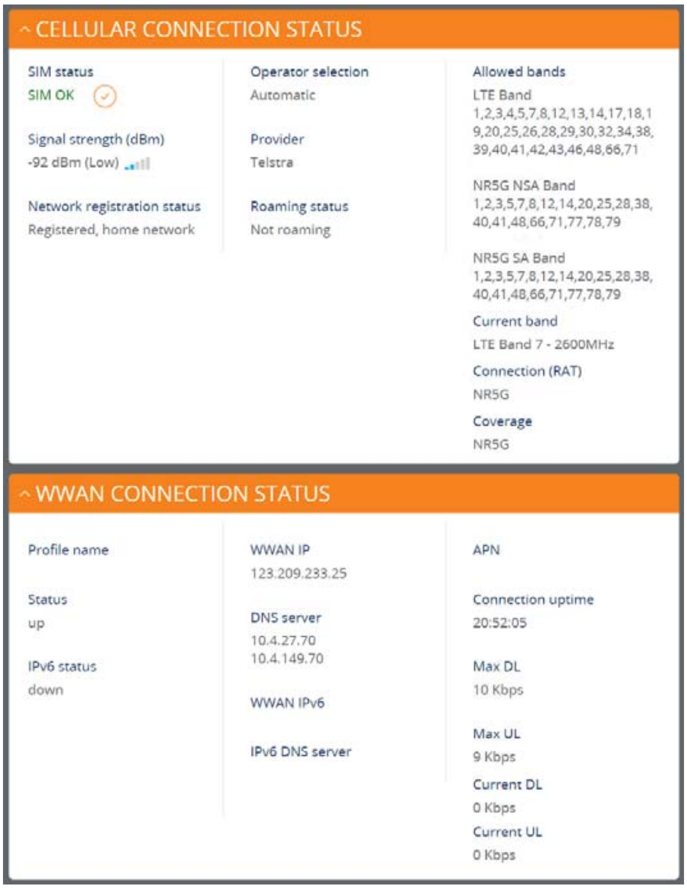


Figure 21 - Main menu items

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 22 - Cellular Connection Status and WWAN Connection Status

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

6 User interface

The AurusLINK+ 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 AurusLINK+ management console.

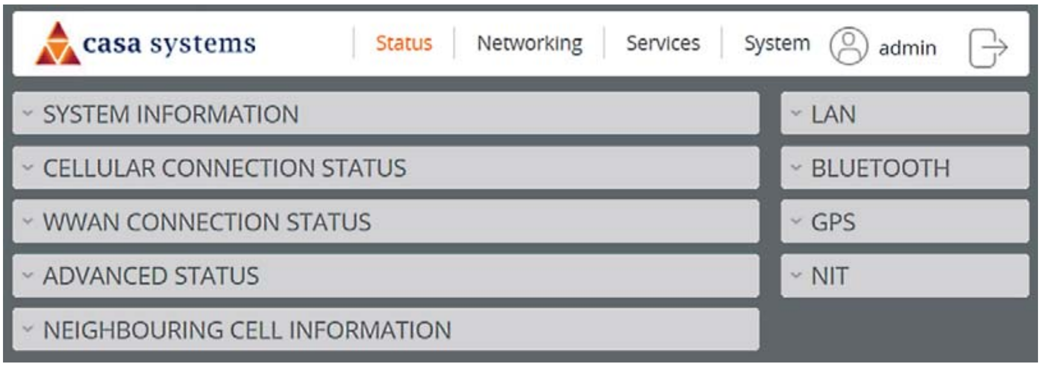


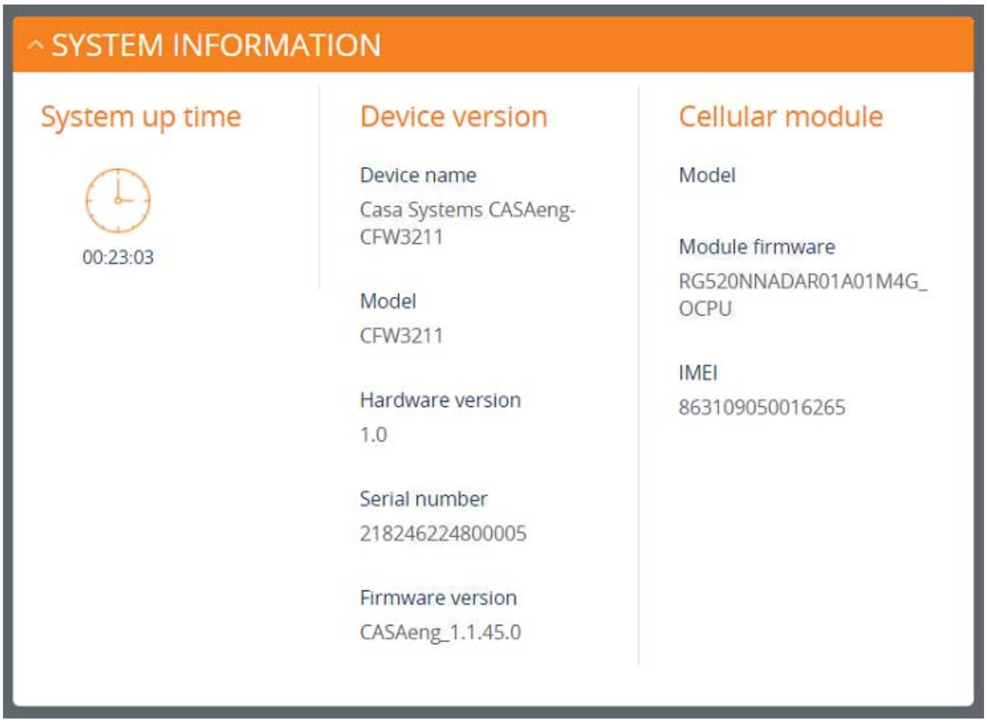
Figure 23 - The Status menu page – first screen after log in

The status page has links to pages displaying

- SYSTEM INFORMATION
- CELLULAR CONNECTION STATUS
- WWAN CONNECTION STATUS
- ADVANCED STATUS
- NEIGHBOURING CELL INFORMATION
- LAN details
- BLUETOOTH MAC address details
- GPS connection details *see 6.1.8*
- NIT Smart Antenna Tool readings *see 6.1.9*

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

00:23:03

Device version

Device name

Casa Systems CASAeng-CFW3211

Model

CFW3211

Hardware version

1.0

Serial number

218246224800005

Firmware version

CASAeng_1.1.45.0

Cellular module

Model

Module firmware

RG520NNADAR01A01M4G_OCPU

IMEI

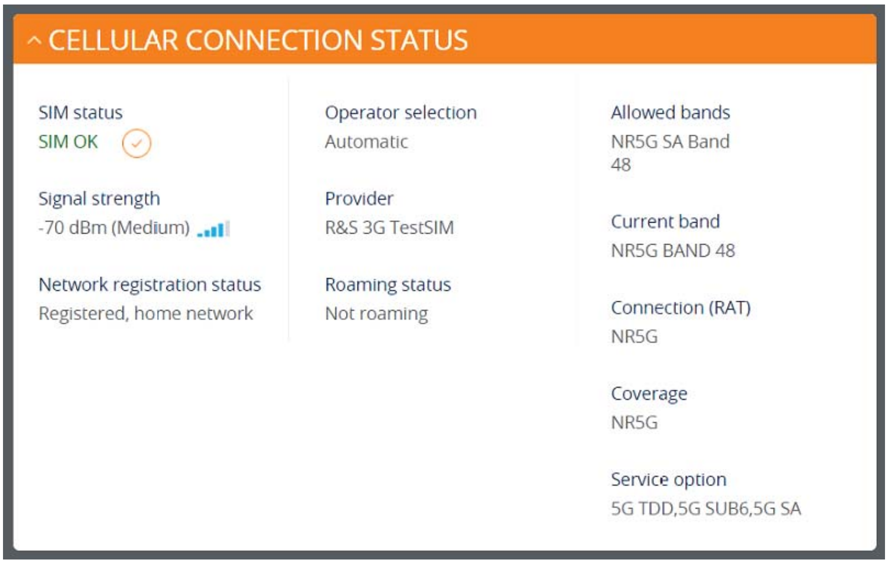
863109050016265

Figure 24 - System Information

System Information	
Device Version	
System up time	The current uptime of the AurusLINK+.
Device name	The manufacturer's name of this device.
Model	The manufacturer's model number.
Hardware version	The hardware version of the AurusLINK+.
Serial Number	The serial number of the AurusLINK+.
Firmware version	The firmware version of the AurusLINK+
Cellular module	
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 6 - 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

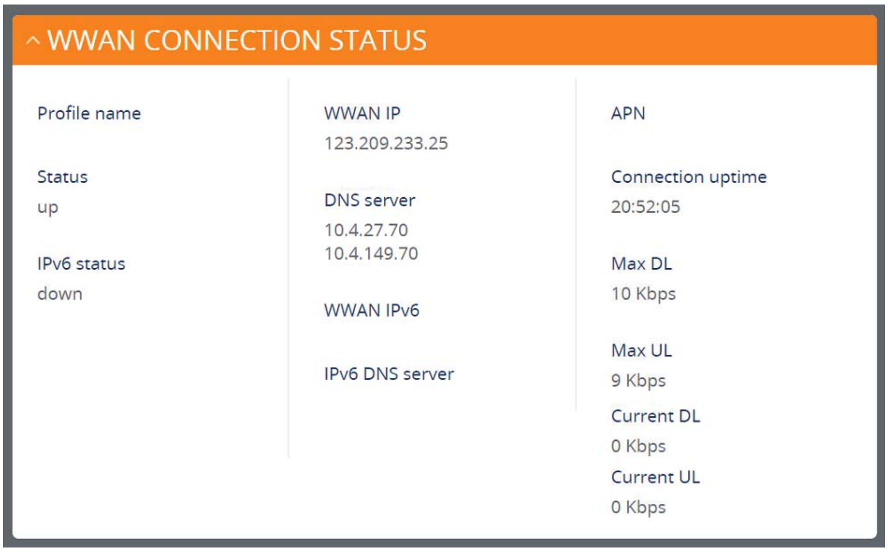
Service option
5G TDD,5G SUB6,5G SA

Figure 25 - Cellular Connection Status

Cellular Connection Status	
SIM status	Displays the activation status of the AurusLINK+ on the carrier network.
Signal strength (dBm)	The current signal strength measured in dBm.
Network registration status	The status of the AurusLINK+'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 AurusLINK+.
Allowed bands	The bands to which the AurusLINK+ may connect.
Current band	The current band being used by the AurusLINK+.
Coverage	The type of mobile coverage being received by the AurusLINK+.

Table 7 - Cellular Connection Status fields

6.1.3 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

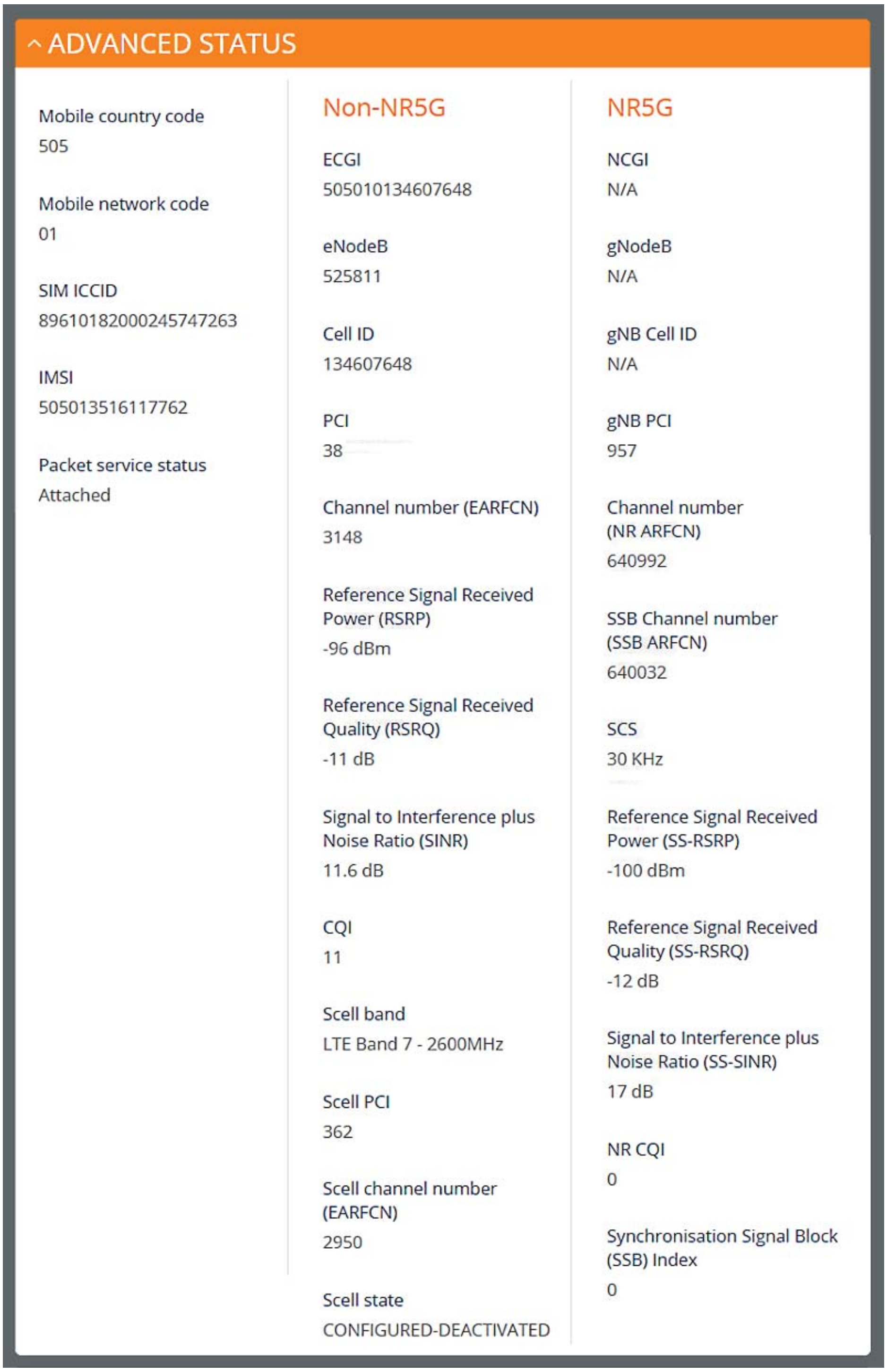
Figure 26 - WWAN Connection Status

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 8 - WWAN Connection Status fields

6.1.4 Advanced status



Mobile country code
505

Mobile network code
01

SIM ICCID
89610182000245747263

IMSI
505013516117762

Packet service status
Attached

Non-NR5G

ECGI
505010134607648

eNodeB
525811

Cell ID
134607648

PCI
38

Channel number (EARFCN)
3148

Reference Signal Received Power (RSRP)
-96 dBm

Reference Signal Received Quality (RSRQ)
-11 dB

Signal to Interference plus Noise Ratio (SINR)
11.6 dB

CQI
11

Scell band
LTE Band 7 - 2600MHz

Scell PCI
362

Scell channel number (EARFCN)
2950

Scell state
CONFIGURED-DEACTIVATED

NR5G

NCGI
N/A

gNodeB
N/A

gNB Cell ID
N/A

gNB PCI
957

Channel number (NR ARFCN)
640992

SSB Channel number (SSB ARFCN)
640032

SCS
30 KHz

Reference Signal Received Power (SS-RSRP)
-100 dBm

Reference Signal Received Quality (SS-RSRQ)
-12 dB

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

NR CQI
0

Synchronisation Signal Block (SSB) Index
0

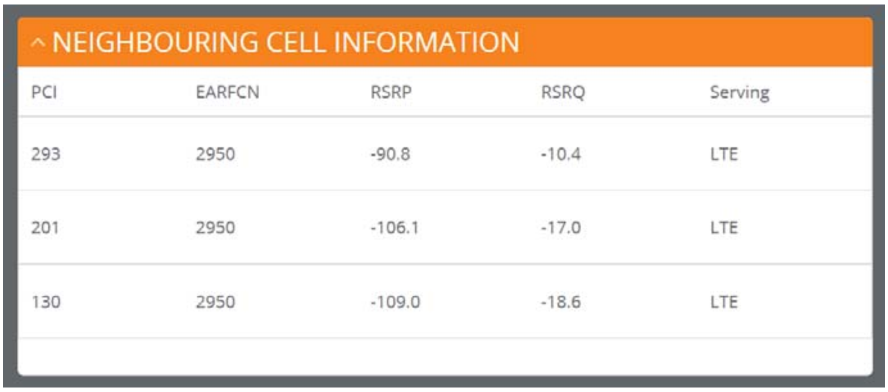
Figure 27 - Advanced Status

Advanced status	
Mobile country code	The Mobile Country Code (MCC) of the AurusLINK+.
Mobile network code	The Mobile Network Code (MNC) of the AurusLINK+.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the AurusLINK+, 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 (SS-RSRP)	A cell-specific reference signal used to determine RSRP.
Reference Signal Received Quality (SS-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.
NR 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 secondary cell (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.
Scell state	The current state of the Scell.

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.
SSB Channel number (SSB ARFCN)	The Synchronisation Signal Block channel number of the current 5G cellular connection.
SCS	The size of current SubCarrier Spacing (SCS) expressed in KHz
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 9 - 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

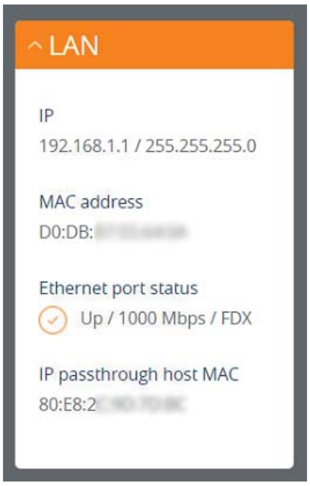
Figure 28 - Cell Information

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 10 - Cell Information fields

6.1.6 LAN

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



^ LAN

IP
192.168.1.1 / 255.255.255.0

MAC address
D0:DB:[redacted]

Ethernet port status
✓ Up / 1000 Mbps / FDX

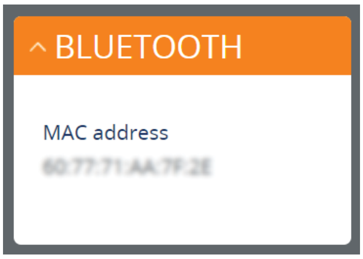
IP passthrough host MAC
80:E8:2[redacted]

Figure 29 - LAN Information

LAN	
IP	The IP address and subnet mask of the AurusLINK+.
MAC address	The MAC address of the AurusLINK+.
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 11 - LAN Information fields

6.1.7 Bluetooth



MAC address

[redacted]

Figure 30 - Bluetooth Information

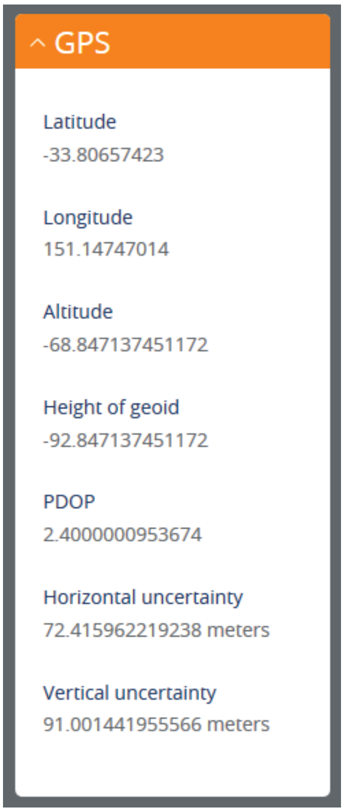
Bluetooth	
MAC address	The MAC address of the Bluetooth module.

Table 12 - Bluetooth Information fields

6.1.8 GPS

ⓘ Note – Please note that not all AurusLINK+ devices support GPS.
In case GPS is not supported on your device, the menu item on the Status page will be disabled and this screen will not be accessible.

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



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 31 - 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 13 - GPS signal Information fields

6.1.9 NIT

Note – Please note that not all AurusLINK+ devices support NIT.
In case NIT is not supported on your device, the menu item on the Status page will be disabled and this screen will not be accessible.

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

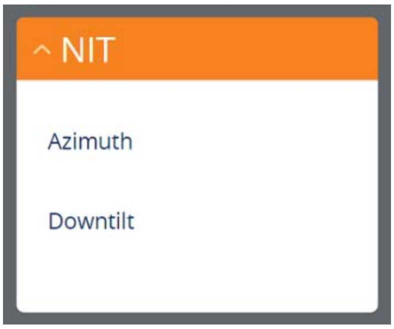


Figure 32 – NIT Information

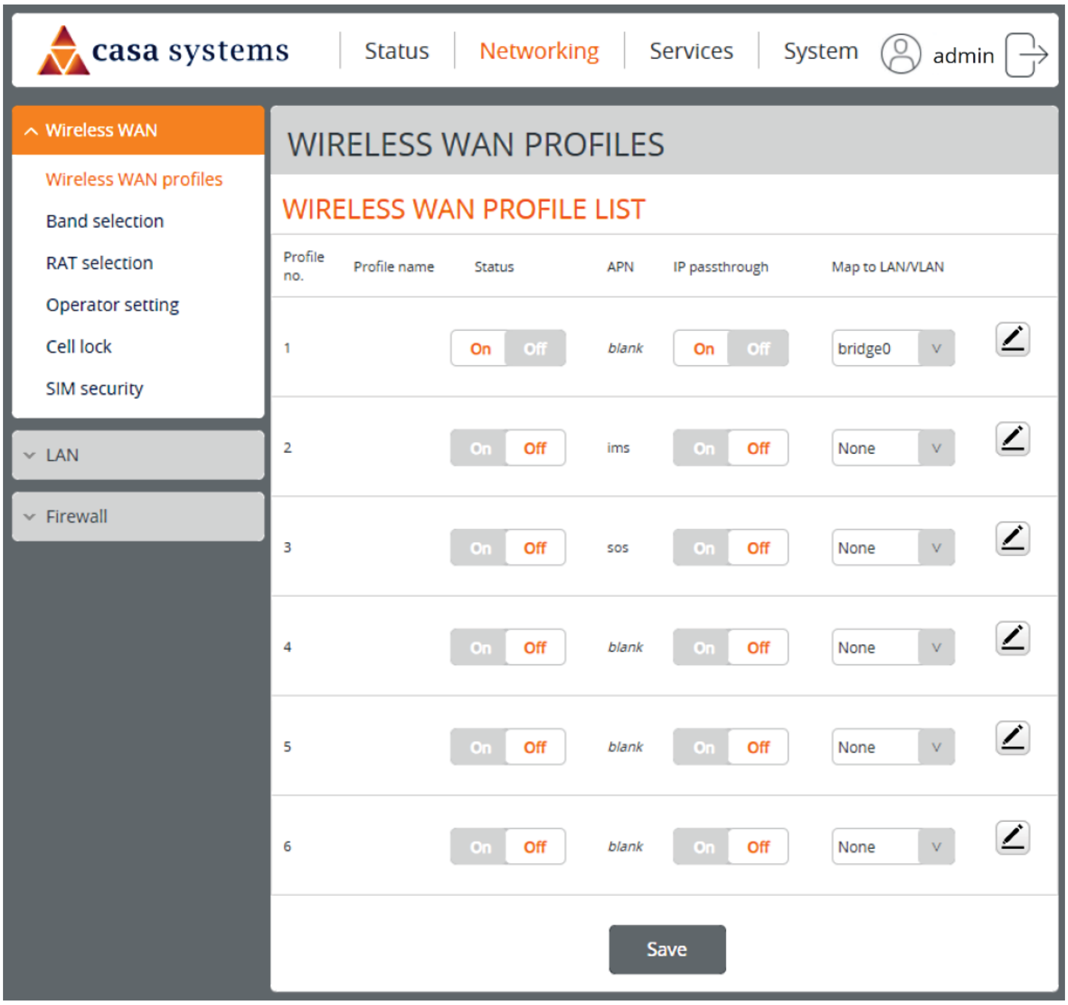
6.2 Networking

6.2.1 Wireless WAN

6.2.1.1 Wireless WAN profiles

Important – Changing any of these settings can cause the AurusLINK+ 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 14 - Wireless WAN Profiles page

Each profile refers to a set of configuration items which are used by the AurusLINK+ 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.

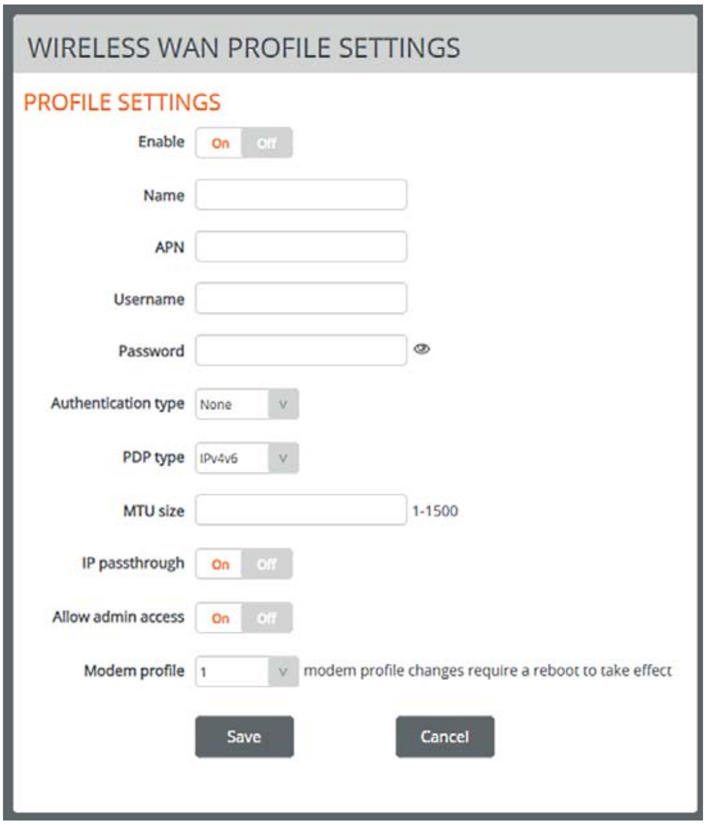
⚠ Important – The **same VLAN** <u>**MUST NOT**</u> **be used in multiple profiles**, even if the other profile or profiles are not enabled.

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

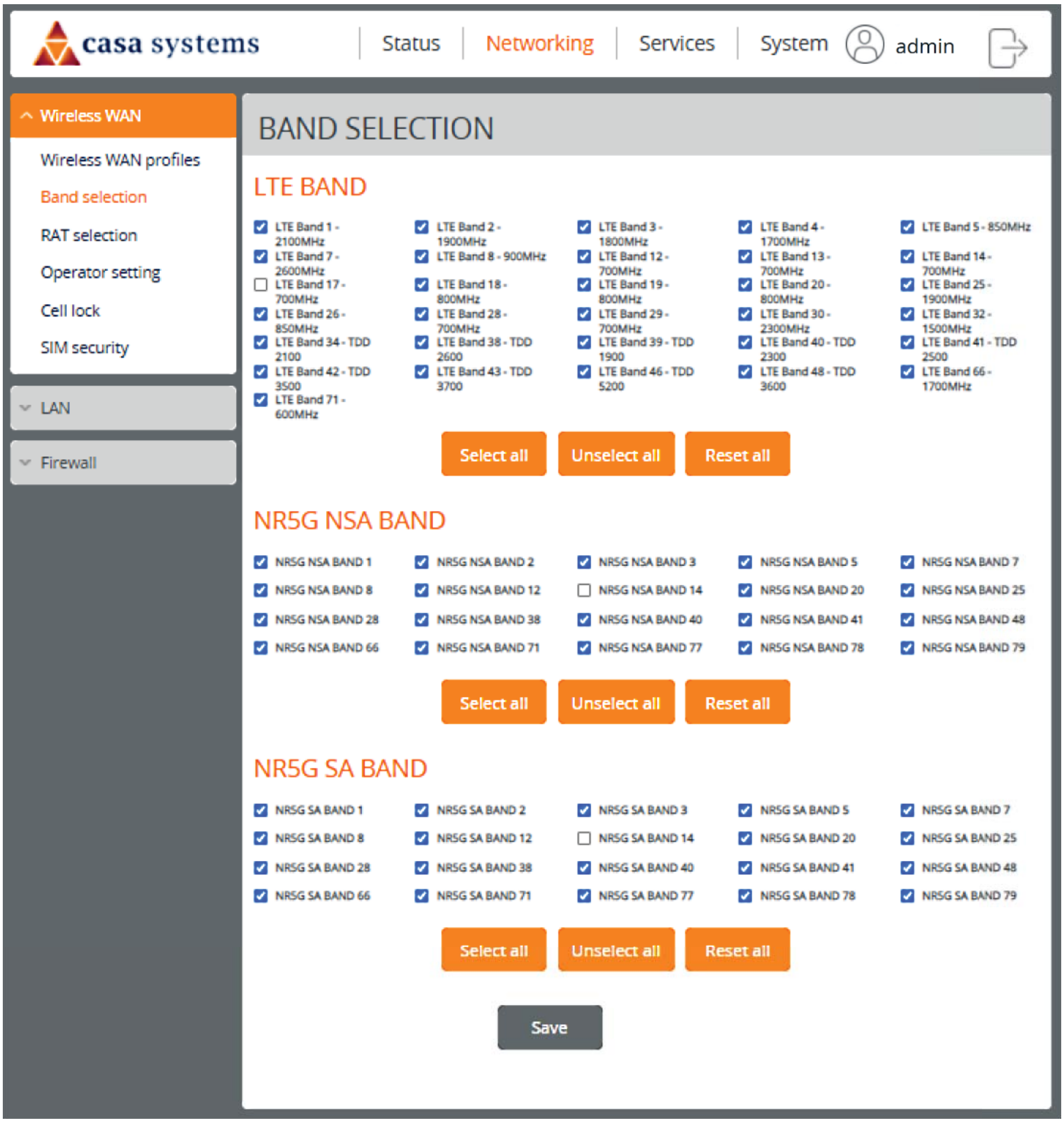
Figure 33 - Wireless WAN Profile Settings

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 AurusLINK+.
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
PDP Type	Select the **PDP type** (IP protocol) to use for the connection. a ⦿ IPv4 – Sets a single stack IPv4 connection through which the AurusLINK+ receives only IPV4 network and DNS addresses. b ⦿ IPv6 – Sets a single stack IPv6 connection through which the AurusLINK+ 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 AurusLINK+ 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 (AurusLINK+) 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 15 - 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

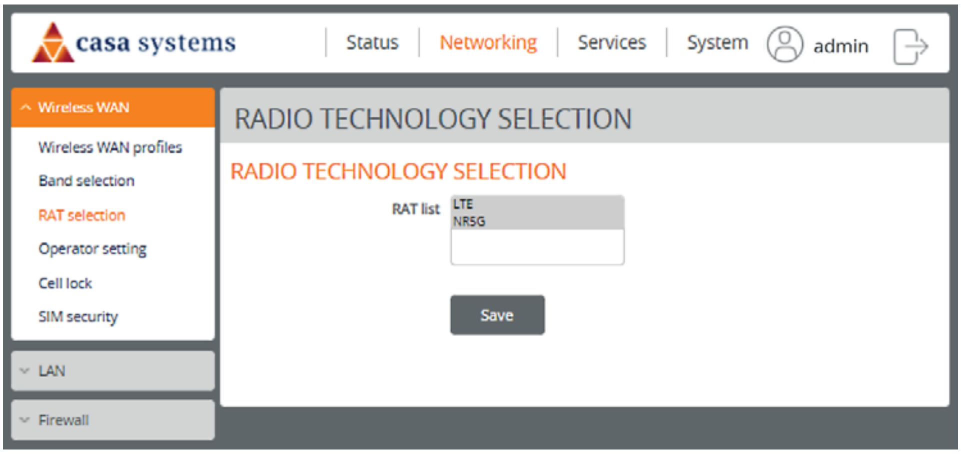
Figure 34 - Wireless WAN – Band selection page

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*

Note – Depending upon the model of AurusLINK+ different frequency bands will be available for selection.
Please refer to your model's datasheet to ascertain which bands are applicable.

6.2.1.3 RAT selection

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



RADIO TECHNOLOGY SELECTION

RADIO TECHNOLOGY SELECTION

RAT list: LTE, NR5G

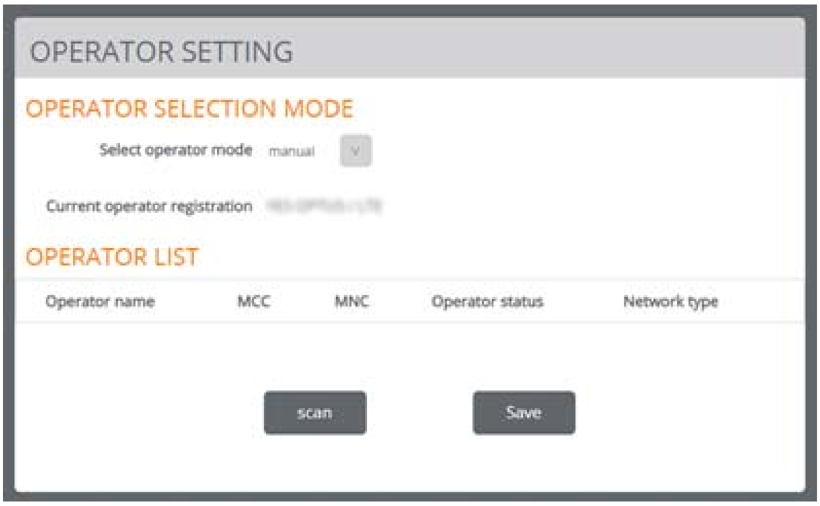
Save

Figure 35 - 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 AurusLINK+ 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.



OPERATOR SETTING

OPERATOR SELECTION MODE

Select operator mode: manual

Current operator registration

OPERATOR LIST

Operator name	MCC	MNC	Operator status	Network type

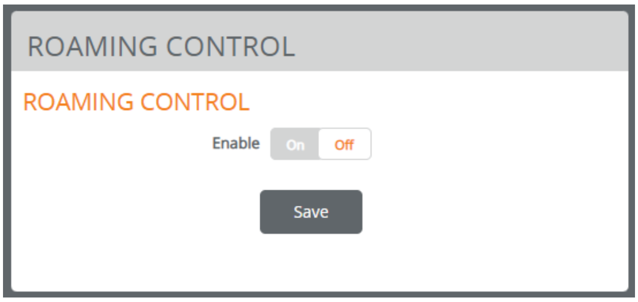
scan

Save

Figure 36 - Wireless WAN – Operator Settings

6.2.1.5 Roaming control

Select On to enable Roaming Control.


ROAMING CONTROL

ROAMING CONTROL

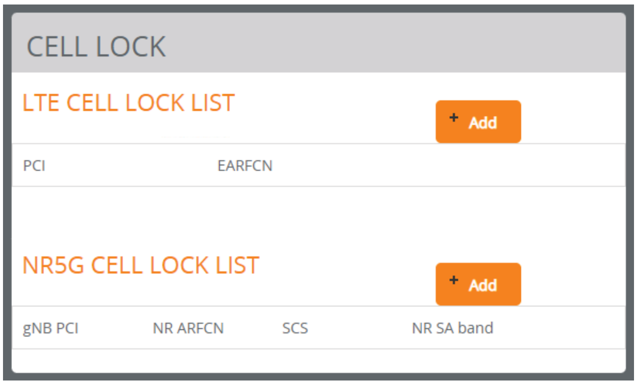
Enable On Off

Figure 37 - Roaming control page

6.2.1.6 Cell lock

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

Two types of cells can be locked: LTE and NR5G


CELL LOCK

LTE CELL LOCK LIST

PCI	EARFCN

NR5G CELL LOCK LIST

gNB PCI	NR ARFCN	SCS	NR SA band

Figure 38 – 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.

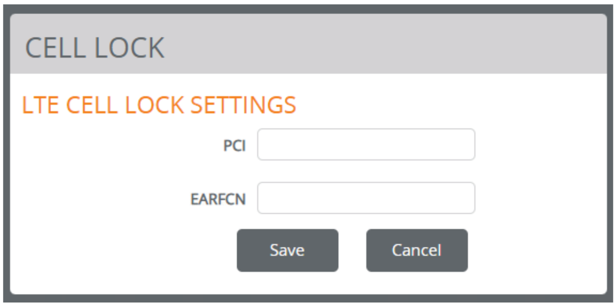


Figure 39 - LTE Cell Lock settings

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.

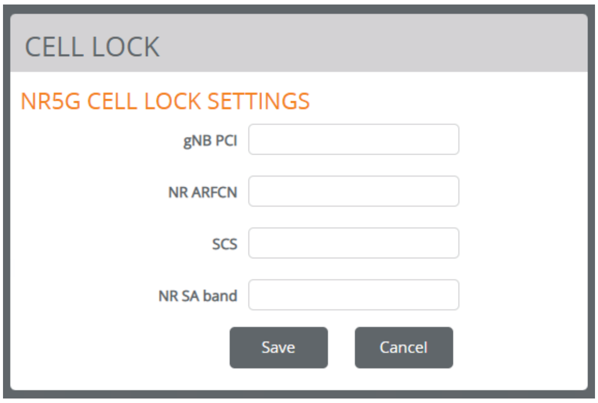


Figure 40 – NR5G Cell Lock settings

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

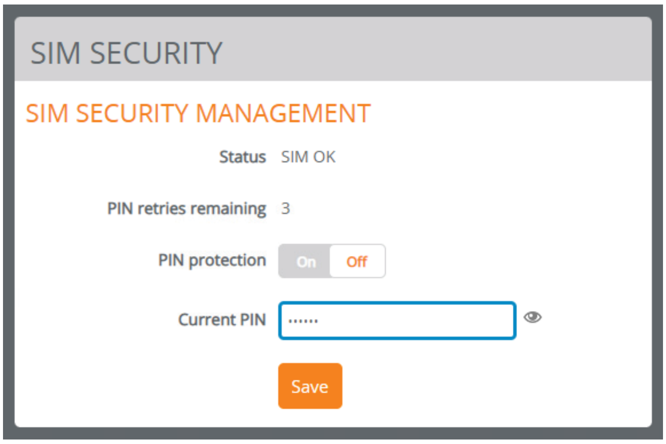
The **SIM security** settings page can be used for authenticating SIM cards that have been configured with a security PIN.

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 41 - 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

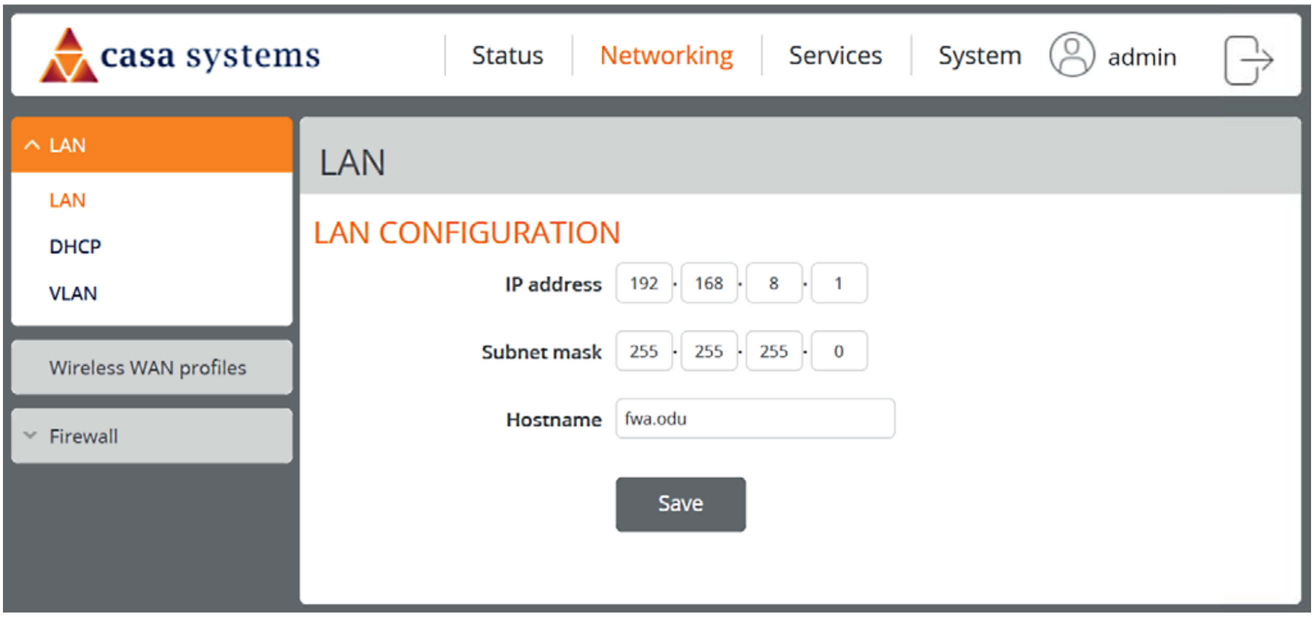
The **LAN configuration** page is used to configure the LAN settings of the AurusLINK+.

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 AurusLINK+.



LAN

LAN CONFIGURATION

IP address 192 . 168 . 8 . 1

Subnet mask 255 . 255 . 255 . 0

Hostname fwa.odu

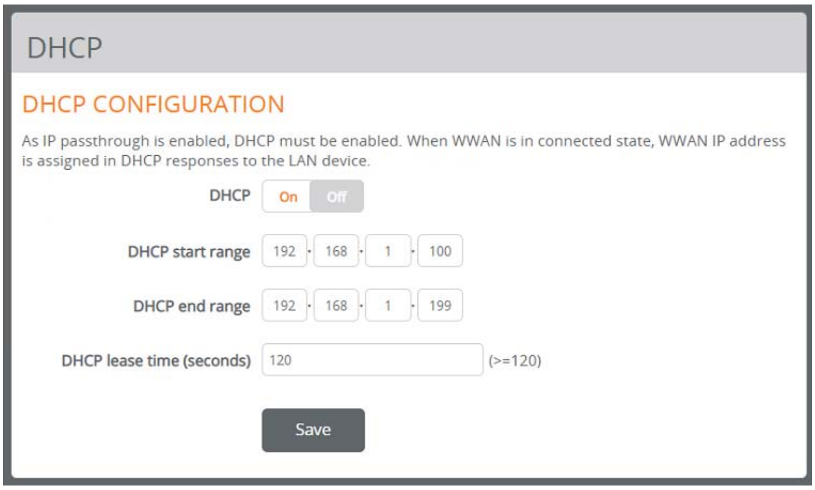
Figure 42 - LAN Information

LAN Configuration	
IP	The IP address of the AurusLINK+.
Subnet mask	The subnet mask of the AurusLINK+.
Hostname	The label used to identify the device.

Table 16 - LAN Information fields

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

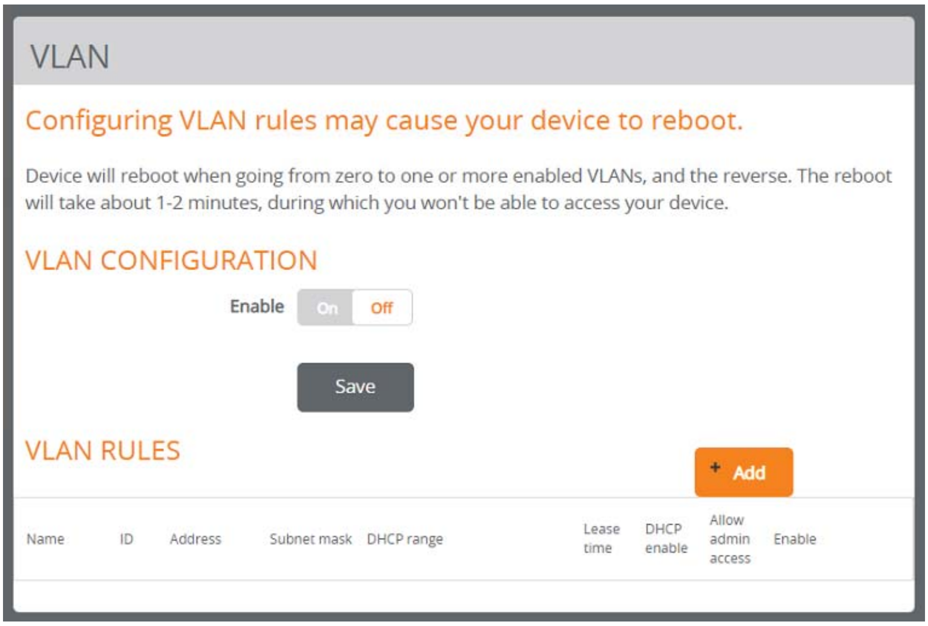
DHCP lease time (seconds) 120 (>=120)

Figure 43 - 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 44 - VLAN Rules list page

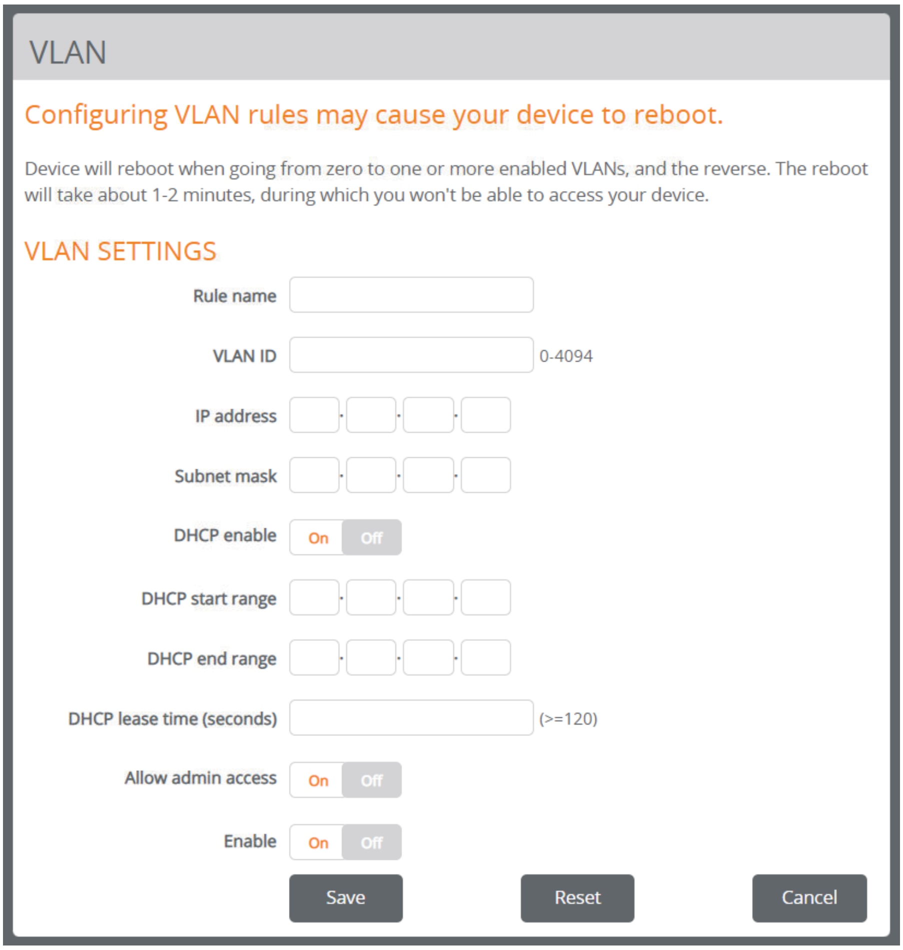
VLAN Settings

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 45 - 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 AurusLINK+. To access the Port forwarding page, click the **Networking** menu at the top of the screen, click the **Firewall** menu on the left.

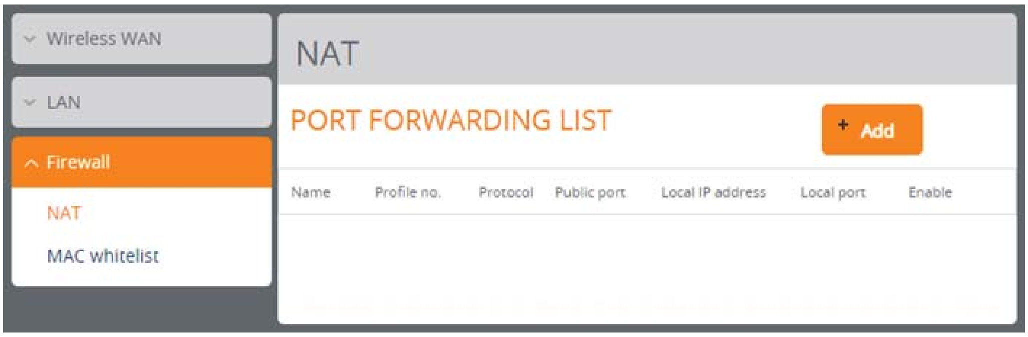


Figure 46 – NAT Port forwarding list

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.

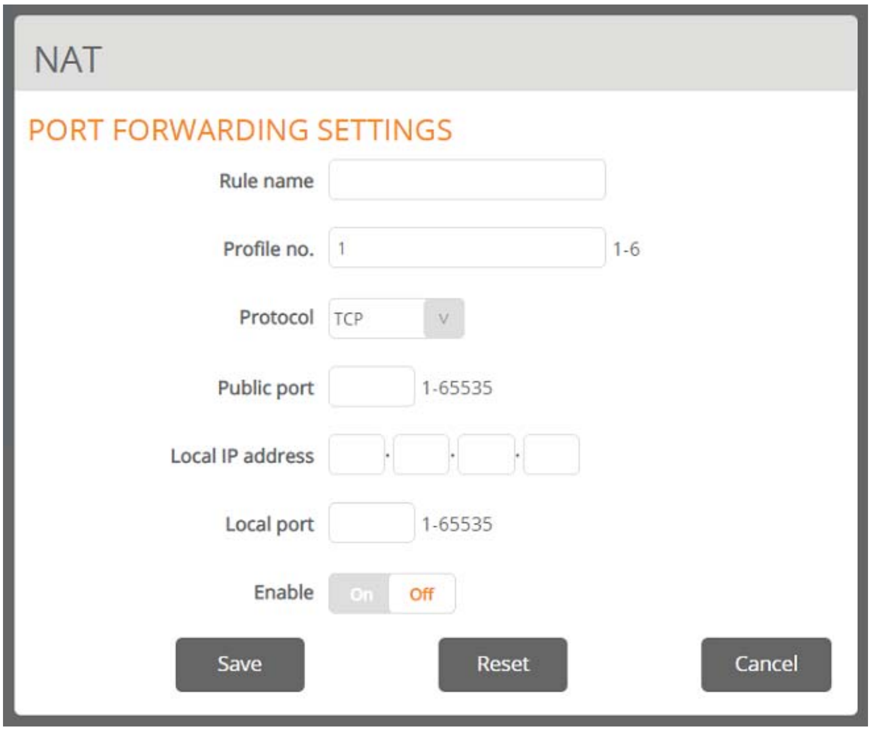
ⓘ Note – Some carriers block inbound connections, or require a public IP address in order to get inbound requests.

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 47 - 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 AurusLINK+ 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.

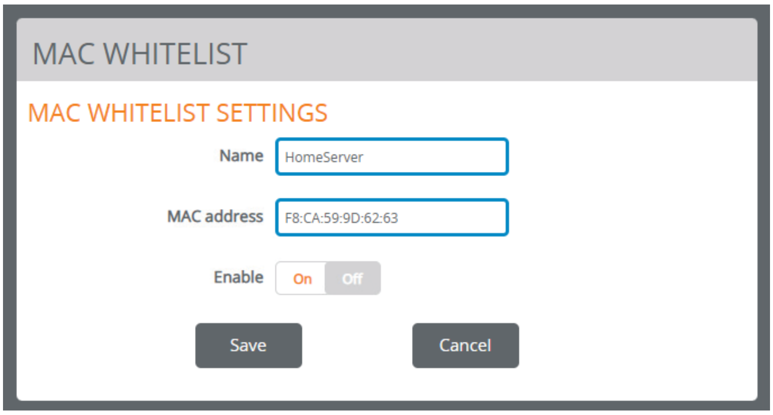
9 Click the **Save** button to confirm your settings.

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 48 – MAC whitelist page

To create an access filter based on MAC address:

1 Click the Add button.

The MAC WHITELIST SETTINGS page will open.

2 Enter a Name to reference the whitelisted device with.

3 Enter the MAC address you want to allow access to

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

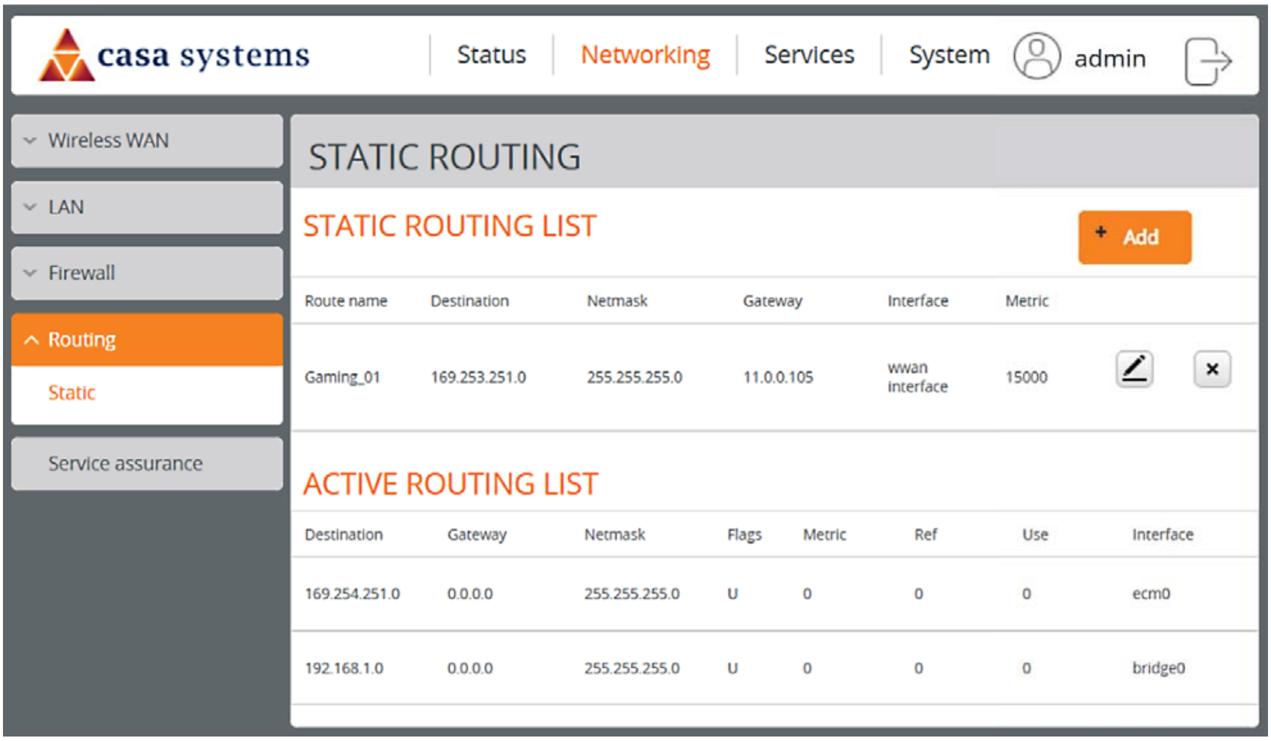
5 Click the Save button.

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 Routes and well as the Active Routes.



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

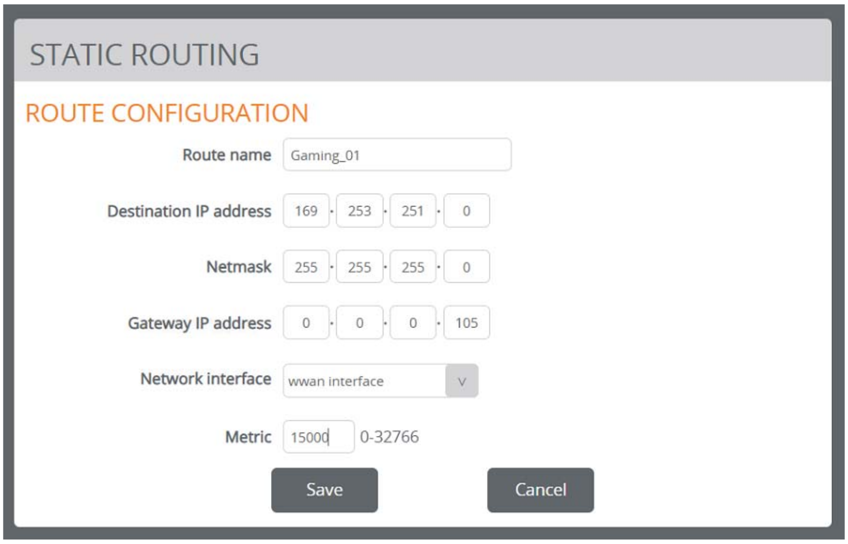
Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
169.254.251.0	0.0.0.0	255.255.255.0	U	0	0	0	ecm0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	bridge0

Figure 49 – Static/Active routing lists

Click the Add button to define a new Static Route.

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 50 – Route configuration page

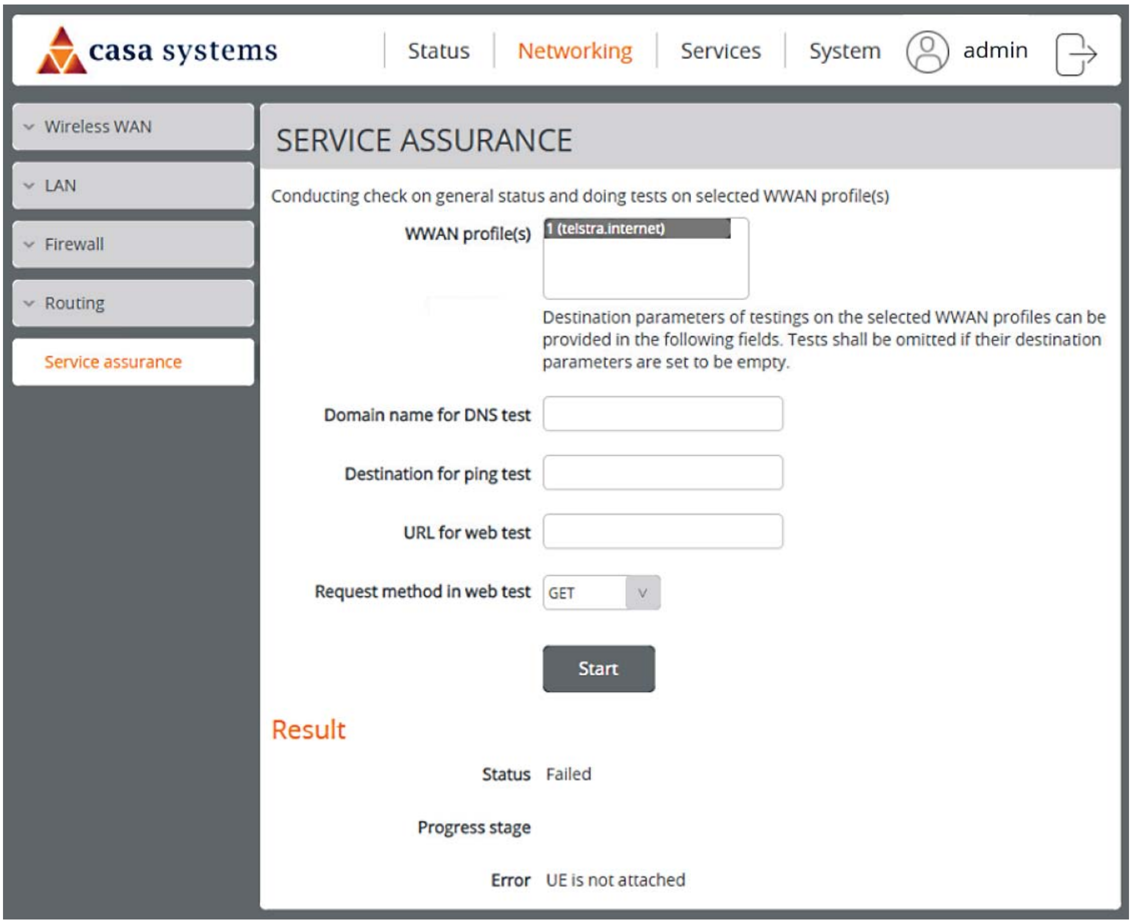
Route configuration

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 from the drop down list.
Metric	Enter a metric in the range of 0 through 32766
Save button	Click to save the changes and add the new route 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 the route permanently from the system.

Table 17 – 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.



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

Status: Failed

Progress stage

Error: UE is not attached

Figure 51 – 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

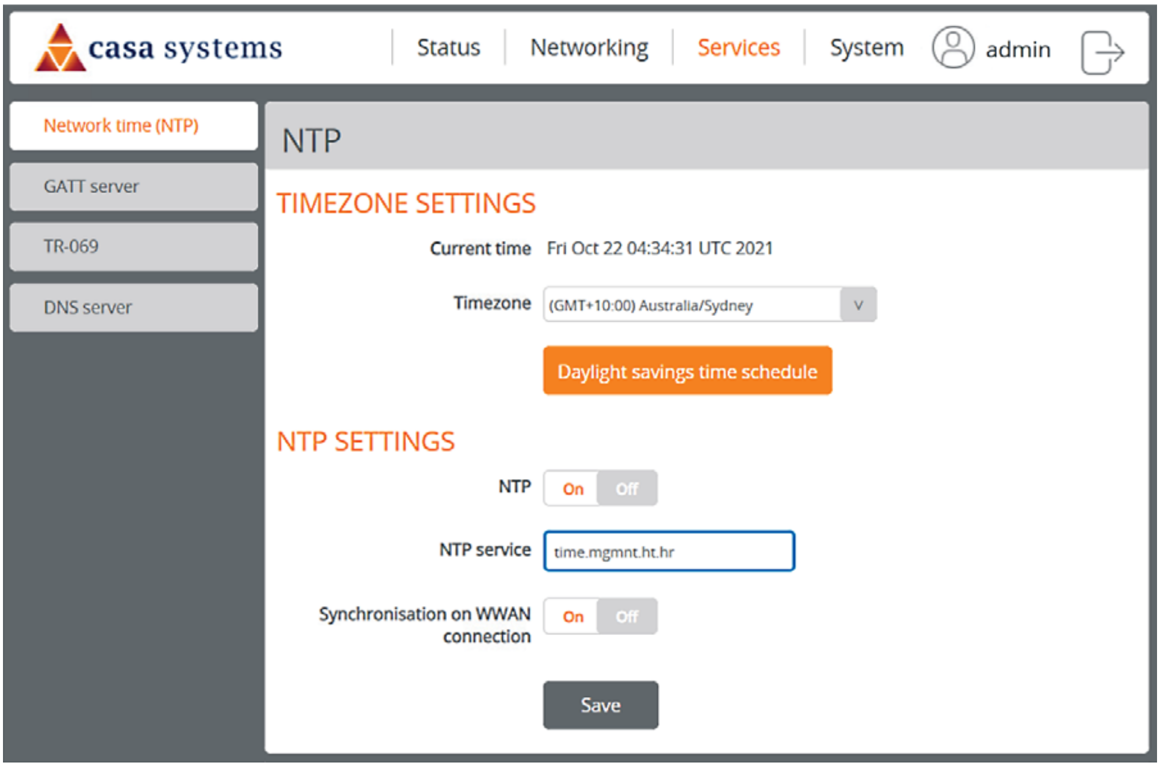
In this section the **Status**, **Progress stage** and any **Error** message will be displayed.

6.3 Services

6.3.1 Network Time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the AurusLINK+ 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

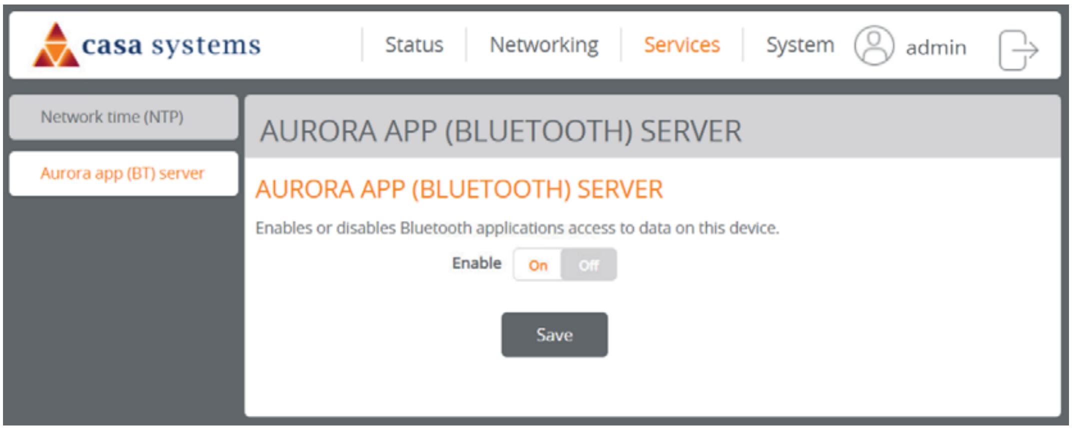
Synchronisation on WWAN connection On Off

Figure 52 - 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

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

Enable [✓ On] Off

Figure 53 - 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.

When the Aurora App (Bluetooth) server is enabled it is automatically activated upon device power up for a maximum of a few minutes. After that period of time the server is automatically deactivated. it can be re-activated at a later time by rebooting the device from the power switch.

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

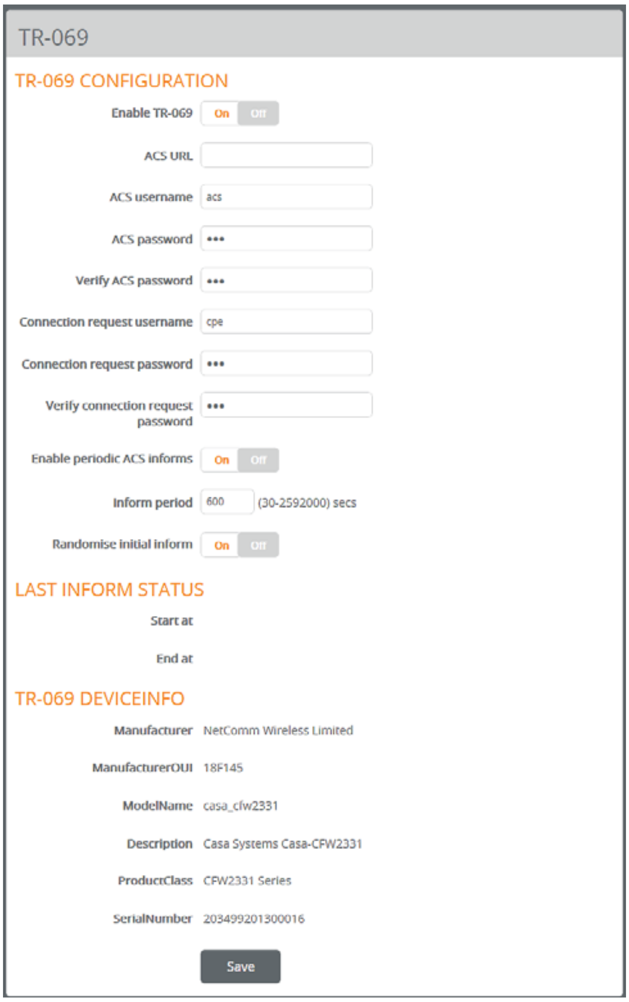
Note – You must have your own compatible ACS infrastructure to use TR-069. To access and configure the TR-069 settings, you must be logged into the router with the root account.
When a factory reset of the router is performed via TR-069, the TR-069 settings are preserved.

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 54 - 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.

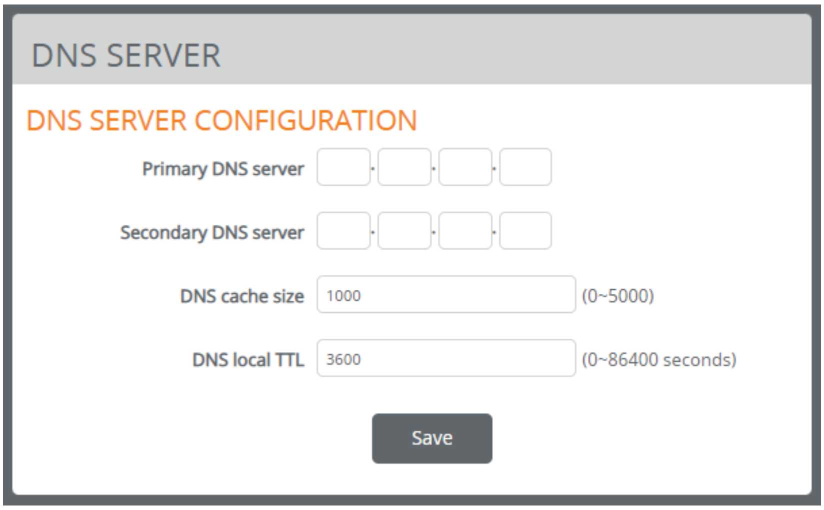
7 The inform message acts as a beacon to inform the ACS of the existence of the router. Select **Enable periodic ACS informs** toggle key to **ON** in order to turn on the periodic ACS inform messages.

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 55 - 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.

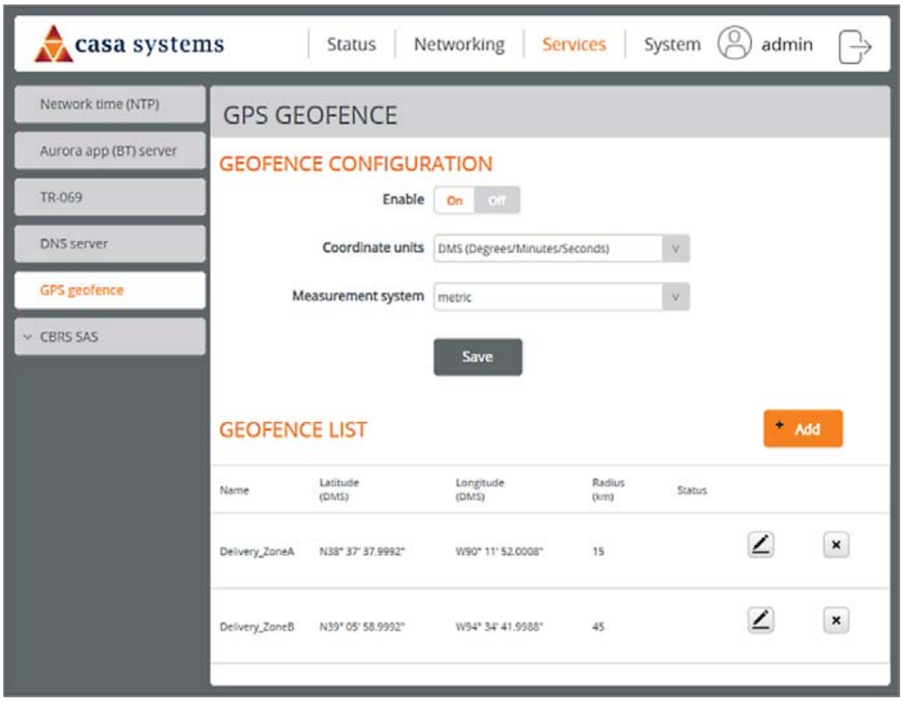
Click the **Save** button to apply the settings to the DNS server.

6.3.5 Geofence

Note – Please note that not all AurusLINK+ devices support GPS or its Geofencing functionality.
In case GPS and Geofence are not supported on your device, the **Geofence** menu item on the **Services** menu will be disabled and this screen will not be accessible.

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.



GEOFENCE CONFIGURATION

Enable: On / Off

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 56 – Geofence options

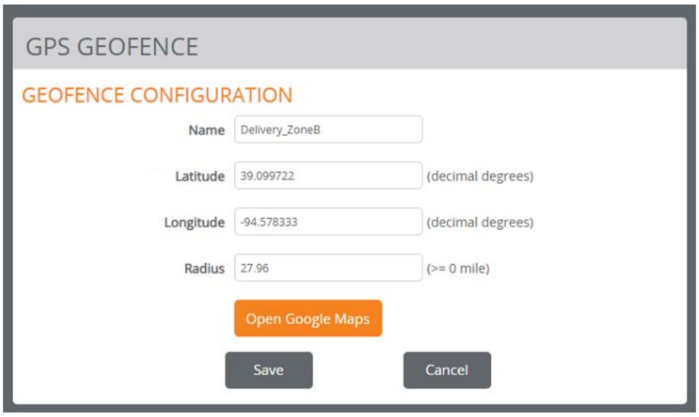
Item	Description
GEOFENCE CONFIGURATION	
Enable button	Toggles Geofence operation On or Off. When on your currently defined Geofences appear in the Geofence list, see below.
Coordinate units	Select either: ● DMS (Degrees/Minutes/Seconds), or ● Decimal degrees Changing this will change the display in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

Item	Description
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 18 – 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 57 – 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: Platte Woods Liberty Parkville Gladstone River Ben Missouri River North Kansas City Missouri River Independence
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 19 – Geofence configuration options

6.4 System

6.4.1 Log – System log

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

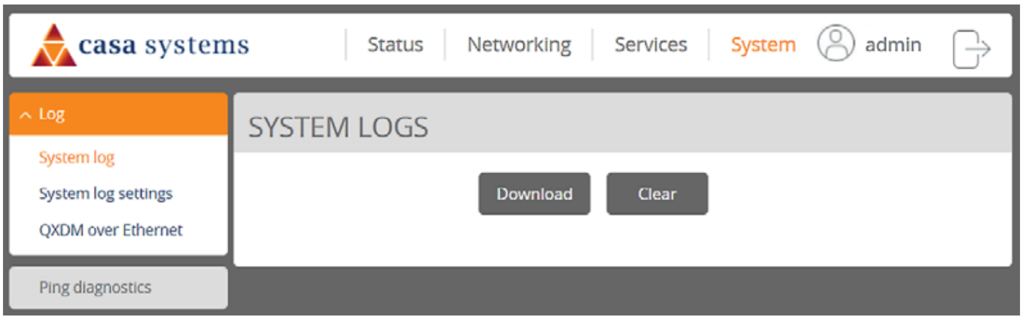


Figure 58 - System Log page

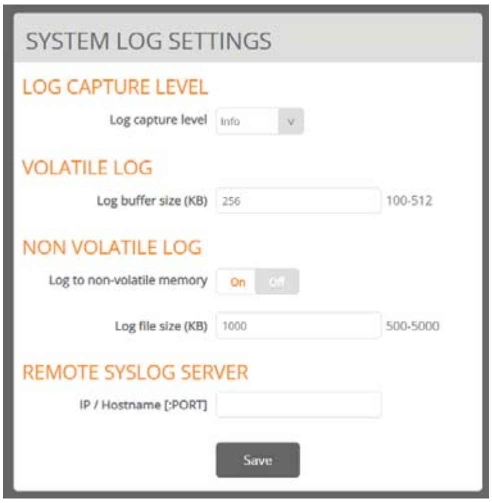
You can download the log file to your local computer by clicking on the **Download** button.

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]:

Figure 59 - 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 20 – 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 AurusLINK+ 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 AurusLINK+ 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.

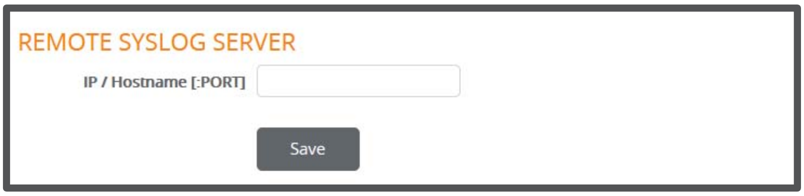
Remote syslog server

The AurusLINK+ 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 AurusLINK+ 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.


REMOTE SYSLOG SERVER

IP / Hostname [:PORT]

Figure 60 – 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 AurusLINK+ will use the default UDP port 514.

3 Click the Save button to save the configuration.

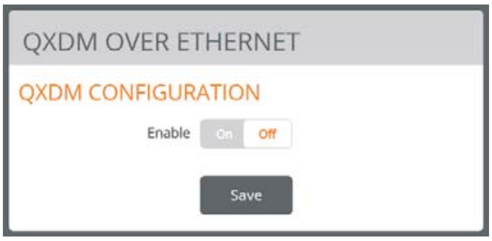
6.4.1.2 QXDM over Ethernet

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.


QXDM OVER ETHERNET

QXDM CONFIGURATION

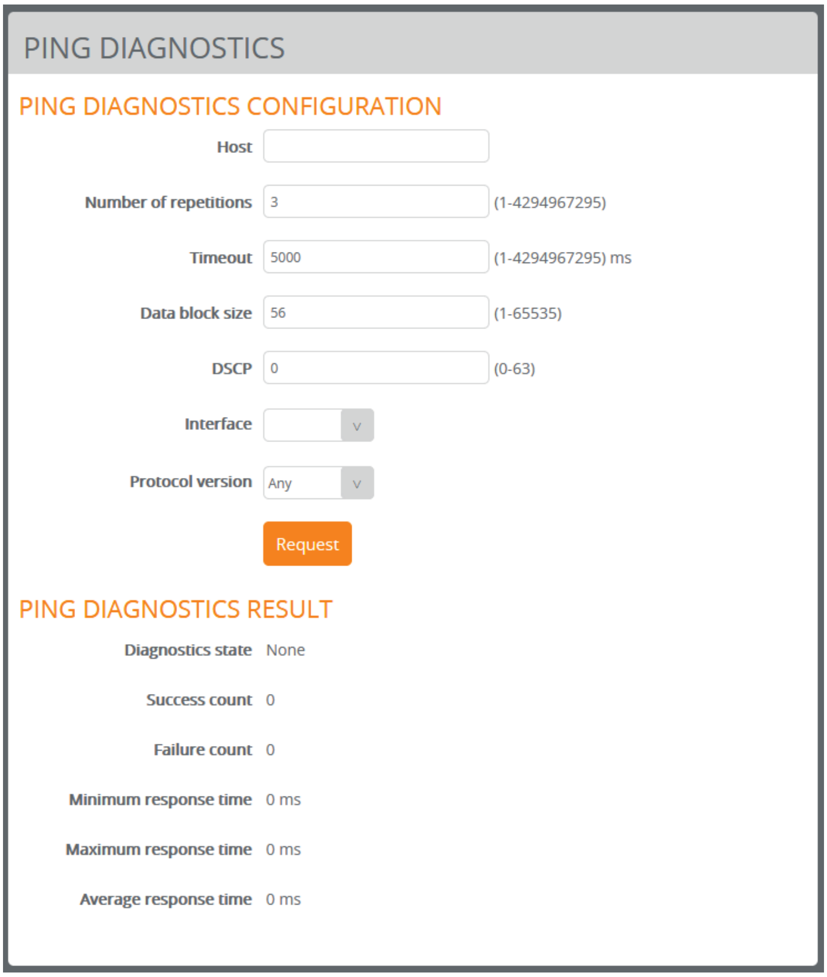
Enable On Off

Figure 61 - 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 AurusLINK+ 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 62 - 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 AurusLINK+ 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

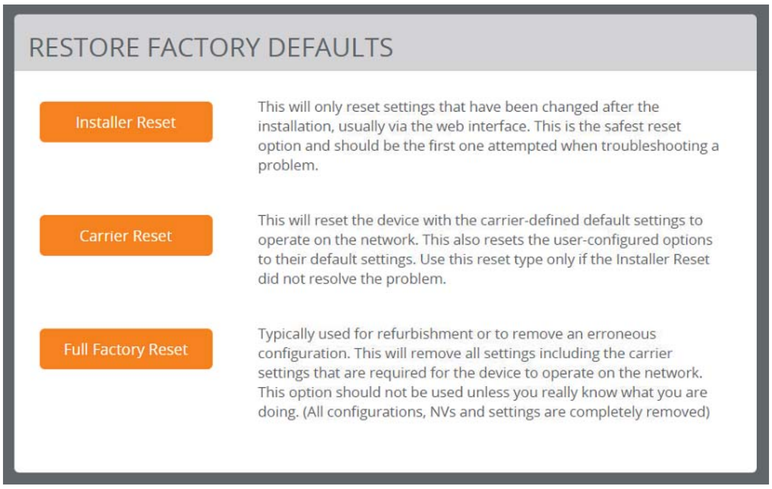
Restoring factory defaults will reset the AurusLINK+ to its factory default configuration. There are three different levels of factory reset. The Installer level reset is the lowest level reset and should be the first one attempted when troubleshooting. The Carrier reset level is the next highest level and erases additional settings while the Full Factory reset option will reset all settings to their factory defaults.

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

1 Open a browser window and navigate to the IP address of the AurusLINK+ (default address is http://192.168.1.1).

2 Log in to the AurusLINK+ Web User Interface (refer to section **5.1 Log in as Administrator via Web UI** on page 24).

3 Select the **System** item from the top menu bar, then **System configuration** on the left menu and then select the **Restore factory defaults** menu item.



RESTORE FACTORY DEFAULTS

Installer Reset

This will only reset settings that have been changed after the installation, usually via the web interface. This is the safest reset option and should be the first one attempted when troubleshooting a problem.

Carrier Reset

This will reset the device with the carrier-defined default settings to operate on the network. This also resets the user-configured options to their default settings. Use this reset type only if the Installer Reset did not resolve the problem.

Full Factory Reset

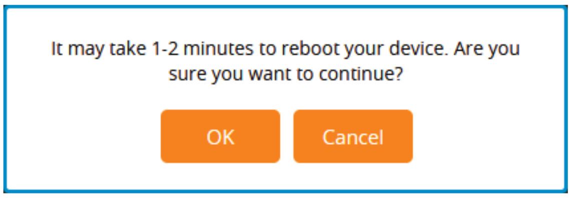
Typically used for refurbishment or to remove an erroneous configuration. This will remove all settings including the carrier settings that are required for the device to operate on the network. This option should not be used unless you really know what you are doing. (All configurations, NVs and settings are completely removed)

Figure 63 - Restore Factory Defaults page

4 Select a reset type to perform: Installer Reset, Carrier Reset or Full Factory Reset

Reset type	Description
Installer Reset	This will only reset settings that have been changed after the installation, usually via the web interface. This is the safest reset option and should be the first one attempted when troubleshooting a problem.
Carrier Reset	This will reset the device with the carrier-defined default settings to operate on the network. This also resets the user-configured options to their default settings. Use this reset type only if the Installer Reset did not resolve the problem.
Full Factory Reset	Typically used for refurbishment or to remove an erroneous configuration. This will remove all settings including the carrier settings that are required for the device to operate on the network. This option should not be used unless you really know what you are doing. (All configurations, NVs and settings are completely removed)

5 A notice is displayed informing you that the process may take one or two minutes.



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

Figure 64 – Restore Factory Defaults Confirmation Message

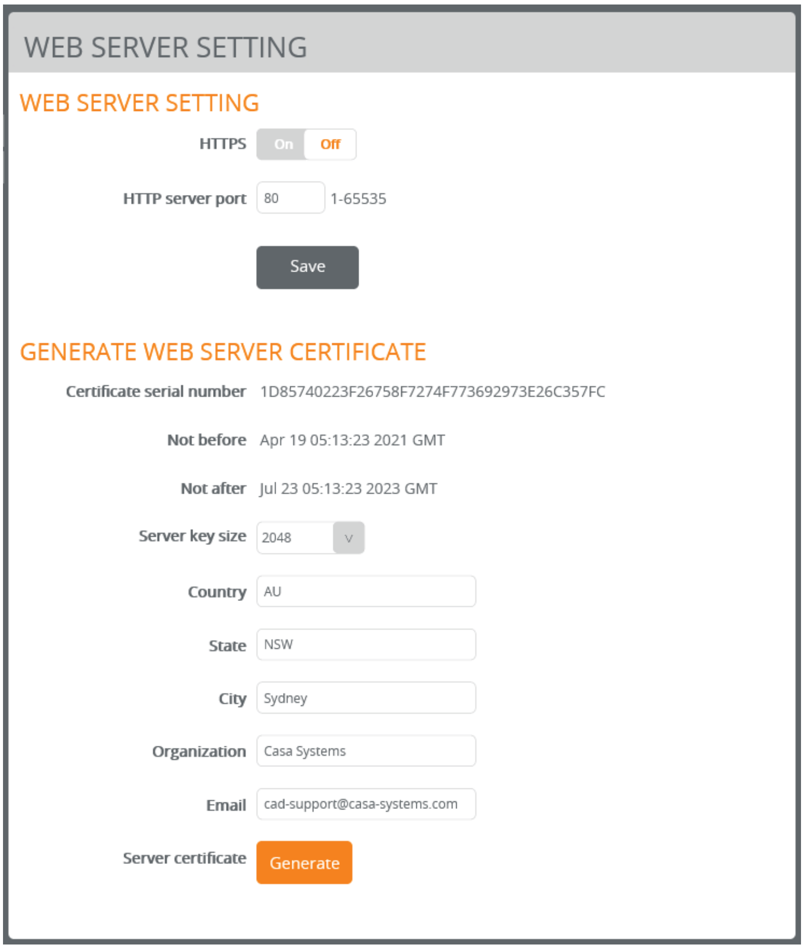
6 Click OK to reboot the AurusLINK+.

7 The AurusLINK+ reboots with the default settings applied.

Note – There is also a manual reset button on the bottom of the CPE.
The manual reset button supports two types of reset.
For more information refer to 3.2 Interface on page 10 of this User Guide.

6.4.3.2 Web server settings

You can configure whether the AurusLINK+'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

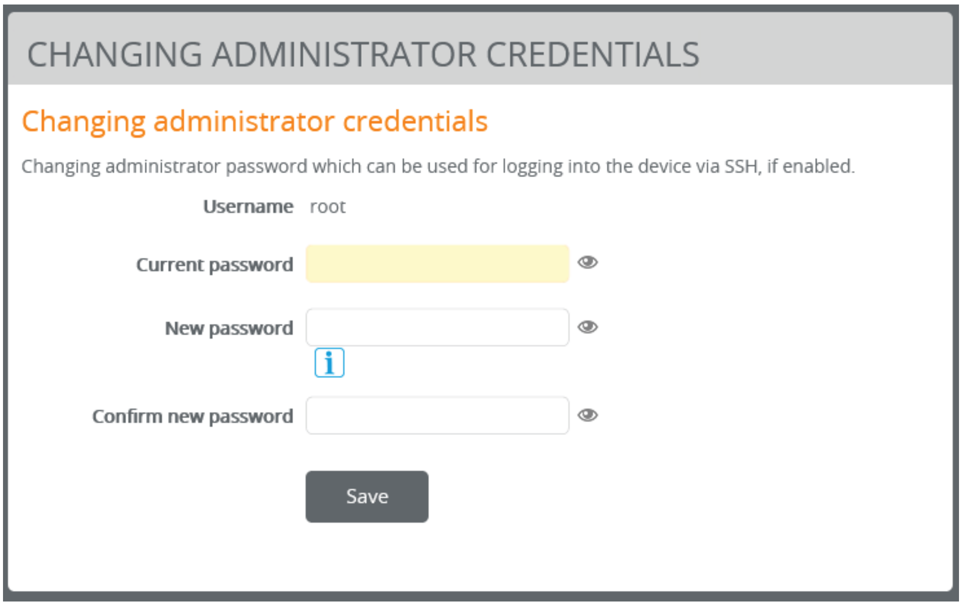
Server certificate

Figure 65 - Web server settings

6.4.3.3 Administrator credentials

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

The default **User Name** and **User Password** for SSH access should be obtained from your local mobile carrier or Casa Systems representative:



CHANGING ADMINISTRATOR CREDENTIALS

Changing administrator credentials

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

Username	root
Current password	
New password	
Confirm new password	

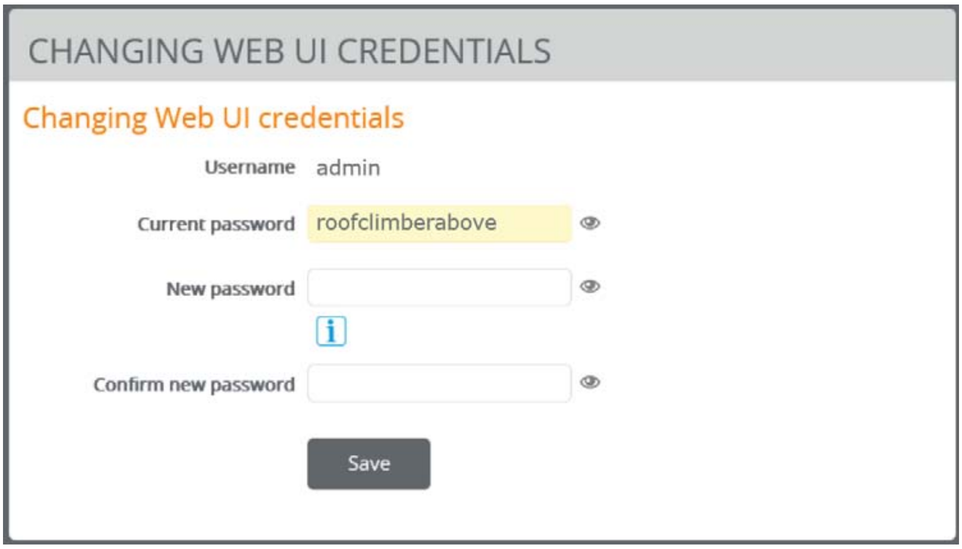
Figure 66 - Changing administrator credentials

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 24).



CHANGING WEB UI CREDENTIALS

Changing Web UI credentials

Username admin

Current password roofclimberabove

New password

Confirm new password

Figure 67 - 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	admin
Password	roofclimberabove

Table 21 - Login details – Administrator account via Web UI

⚠ Important – Please note that User Password is recommended to be changed by the mobile carrier at the time of factory production.
Please contact your local mobile carrier or Casa Systems representative if the default value does not work on first time installation.

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

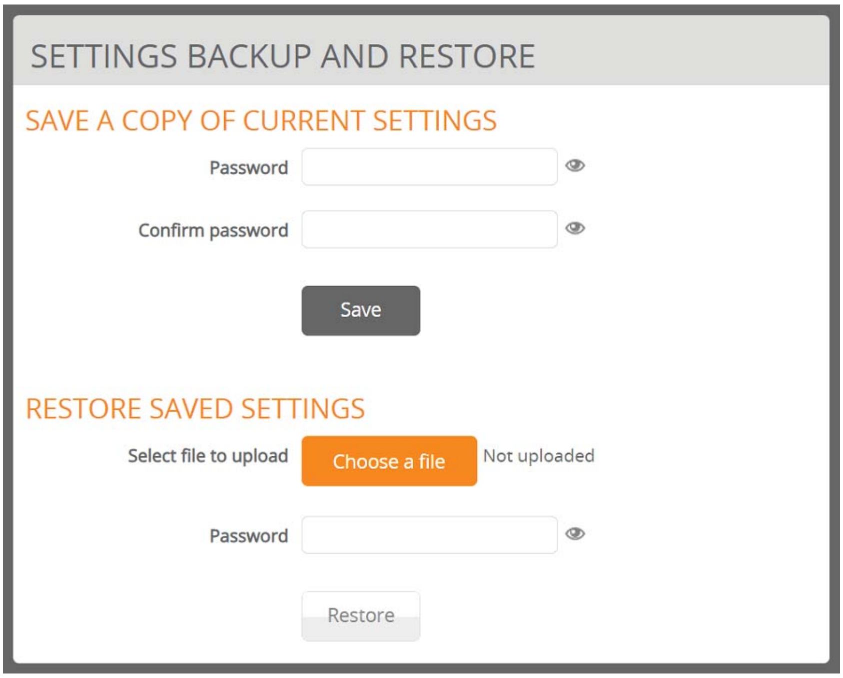
Use this page to save your current settings in a backup file and then to retrieve the backup file to restore your previous settings should this be necessary.

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 68 - 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:

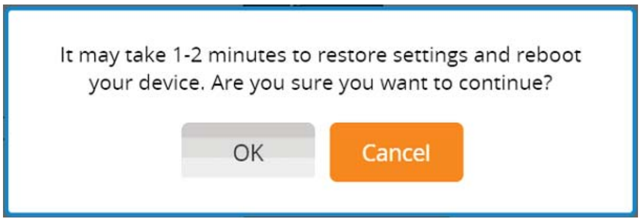
1 Click the Choose a file button and navigate to the backup file.

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 69 – Confirmation of restore message

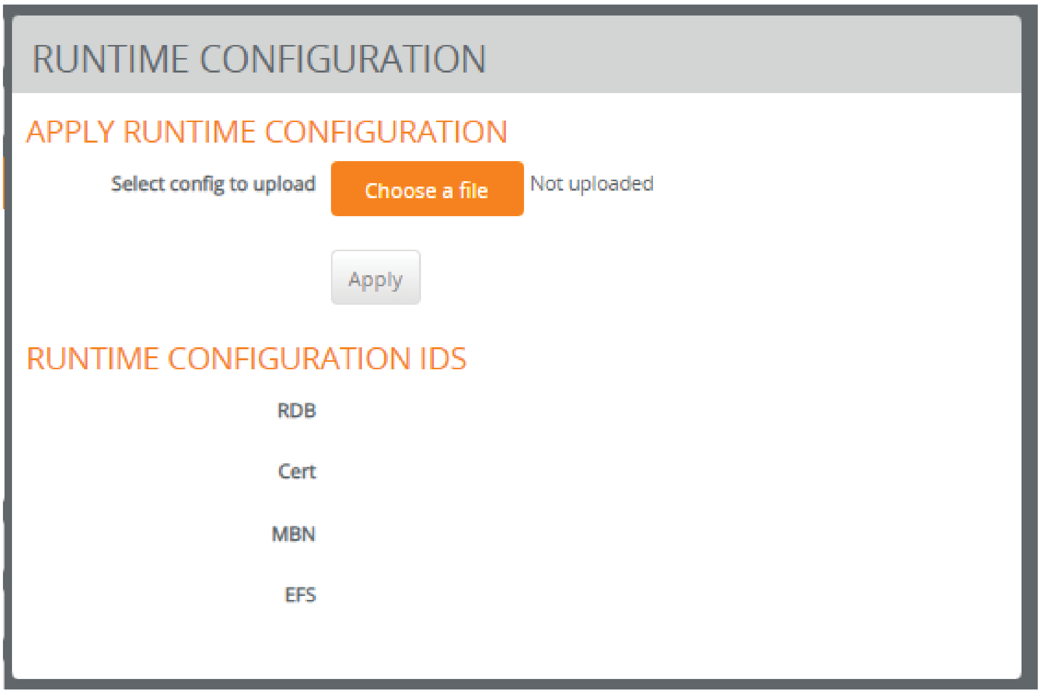
6 Click the OK button to proceed with the restoration of your previous settings.

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



RUNTIME CONFIGURATION

APPLY RUNTIME CONFIGURATION

Select config to upload: Not uploaded

RUNTIME CONFIGURATION IDS

RDB

Cert

MBN

EFS

Figure 70 - 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.

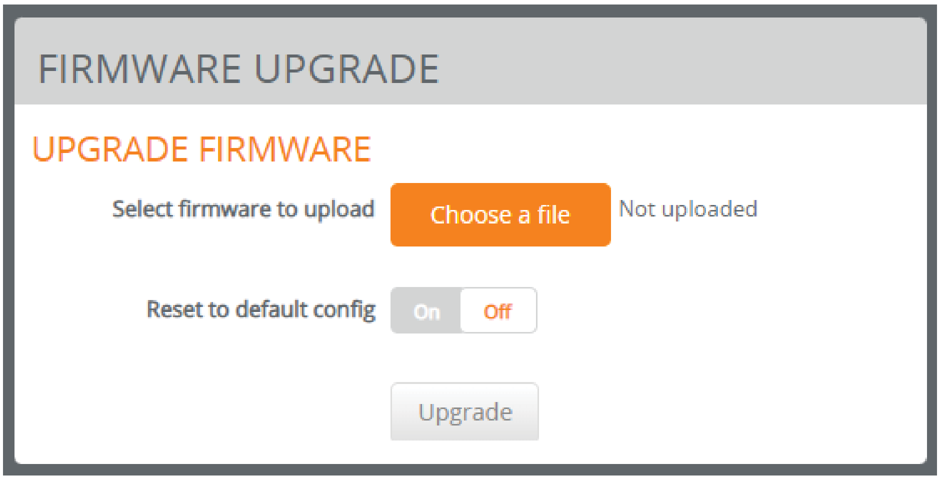
3 Select the Apply button to install the configuration file.

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: Off

Figure 71 - Firmware Upgrade page

To upgrade the firmware of the AurusLINK+:

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.

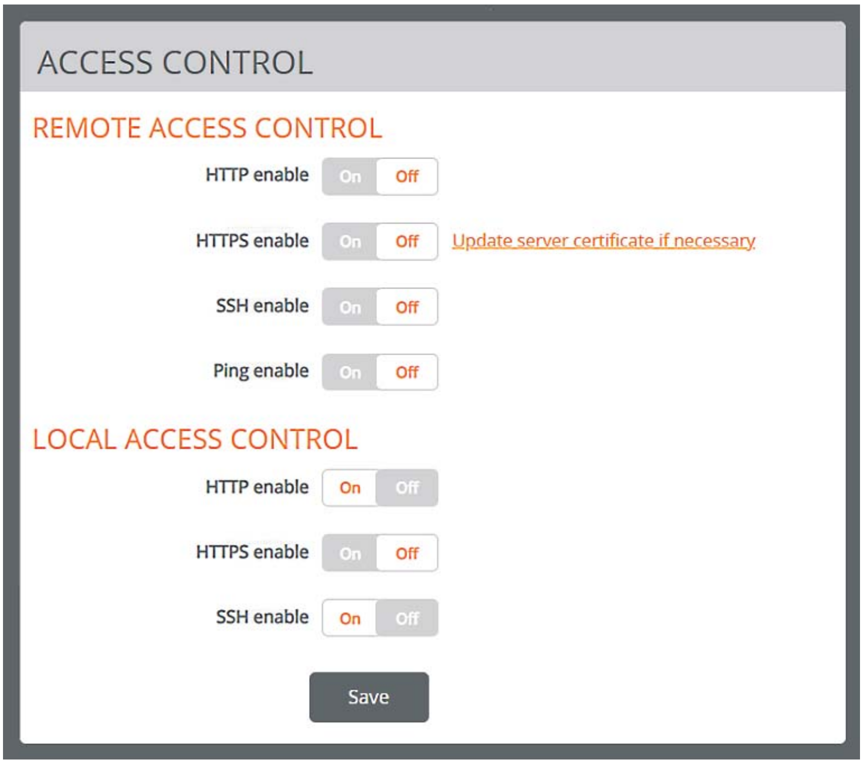
Selecting Off for Reset to default config will save all current user defined settings and apply them using the new firmware.

3 Click the Upgrade button.

4 The AurusLINK+ 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] Update server certificate if necessary

SSH enable On [✓ Off]

Ping enable On [✓ Off]

LOCAL ACCESS CONTROL

HTTP enable [✓ On] Off

HTTPS enable On [✓ Off]

SSH enable [✓ On] Off

Figure 72 - 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.
Update server certificate link	If necessary, click this link to go to the WEB SERVER SETTINGS page. Refer to *6.4.3.4 Web UI credentials* on page 70 for details on updating this certificate.
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 CPE from a local connection.

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

Table 22 - 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

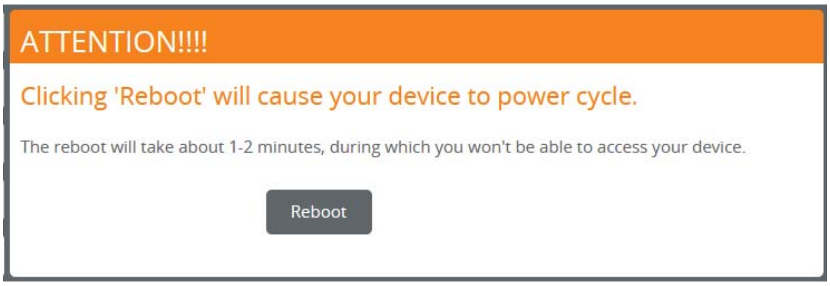
The **Reboot** option in the **System** section performs a soft reboot of the device. This can be useful if you have made configuration changes you want to implement.

To reboot the AurusLINK+:

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 AurusLINK+ displays a warning that you are about to perform a reboot.



ATTENTION!!!!

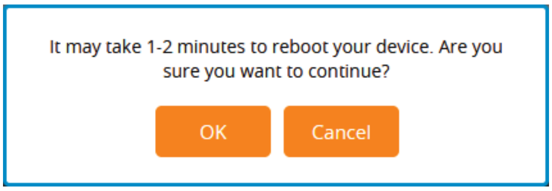
Clicking 'Reboot' will cause your device to power cycle.

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

Figure 73 - Reboot warning 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?*”



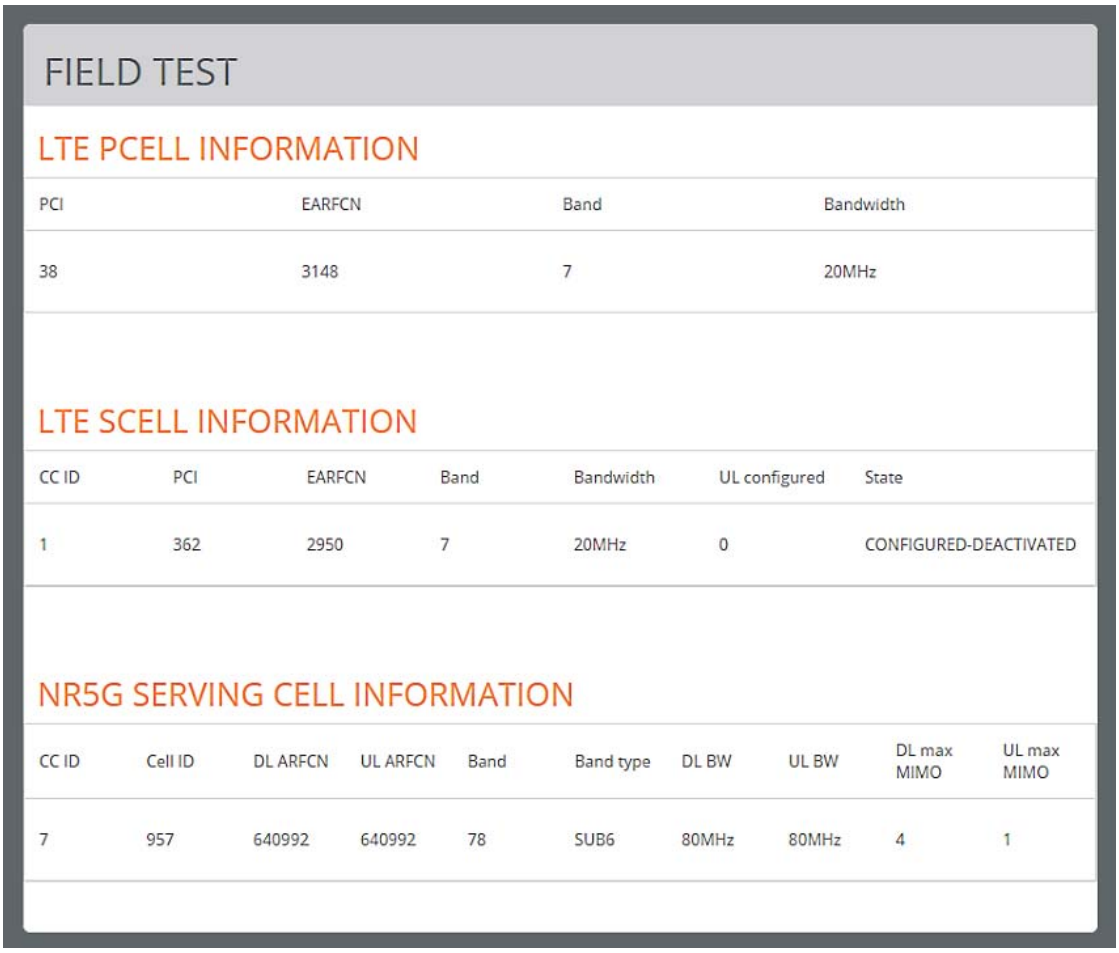
It may take 1-2 minutes to reboot your device. Are you sure you want to continue?

Figure 74 - 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

LTE PCELL INFORMATION

PCI	EARFCN	Band	Bandwidth
38	3148	7	20MHz

LTE SCELL INFORMATION

CC ID	PCI	EARFCN	Band	Bandwidth	UL configured	State
1	362	2950	7	20MHz	0	CONFIGURED-DEACTIVATED

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
7	957	640992	640992	78	SUB6	80MHz	80MHz	4	1

Figure 75 - Field test

FIELD TEST data	
LTE PCell Information	
PCI	The Physical Cell ID
ERFCN	E-UTRA Absolute Radio Frequency Channel Number.
Band	The LTE band number
Bandwidth	The LTE band’s current bandwidth

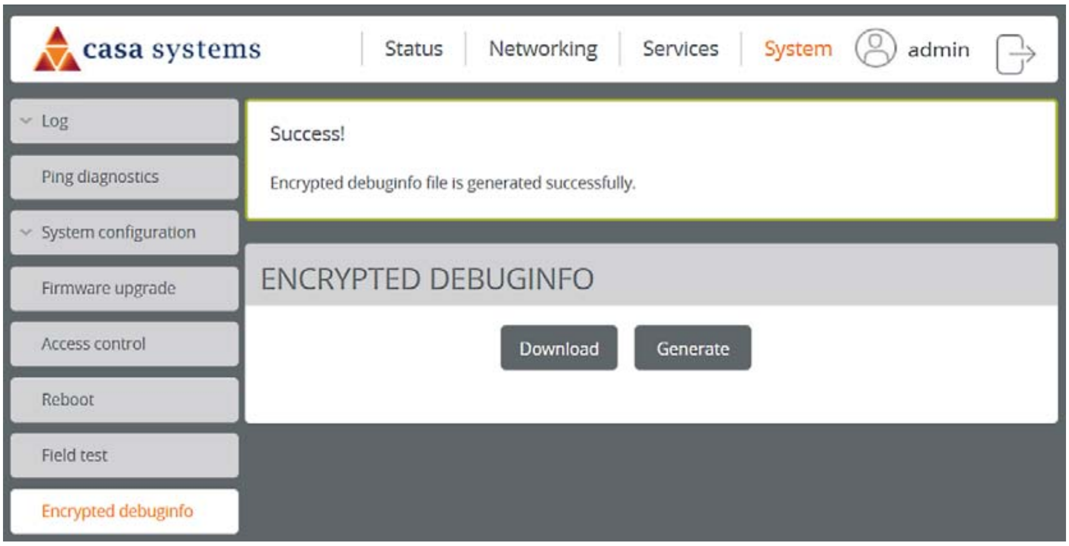
FIELD TEST data	
LTE SCell Information	
CCID	The cell identifier
PCI	The Physical Cell I
ERFCN	E-UTRA Absolute Radio Frequency Channel Number
Band	The LTE band number
Bandwidth	The LTE band’s current bandwidth
UL configured	Indicated whether the cell is configured
State	The current state of the LTE Scell
NR5G Serving Cell Information	
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 (MIMO).
UL max MIMO	Uplink maximum Multiple Input Multiple Output (MIMO).

Table 23 - 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.

Figure 76 - 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`**

Note – This debug file is encrypted and can only be decrypted by Casa Systems personnel.
The file cannot be decrypted by users.
Normally this file with only be generated if Casa Technical Support requests it.

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 20cm between the radiator& your body.

FCC Statement

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

- -40°C to 55°C

Company details

Casa Systems, Inc.

100 Old River Road, Andover, Massachusetts 01810 USA

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

Product details

Product:	5G Sub-6 Self Install Outdoor CPE
Model No:	CFW-3212

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.