

# User Guide

## CBRS Survey UE



Doc No. UG01287

## 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 CFW-2172 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

Copyright© 2020 Casa Systems. All rights reserved.

The information contained herein is proprietary to Casa Systems. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Casa Systems.

Trademarks and registered trademarks are the property of Casa Systems or their respective owners. Specifications are subject to change without notice. Images shown may vary slightly from the actual product.



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

## Document history

This document relates to the following product:

### CFW-2172 CBRS Survey UE

Ver.	Document description	Date
v0.5	First release	September 30, 2020
V0.6	Modified RF Exposure statements, Removed SAS registration	December 1, 2020

*Table i. – Document revision history*

# Contents

<b>Overview</b> .....	<b>5</b>
Introduction .....	5
Target audience .....	5
Prerequisites.....	5
Notation .....	5
<b>Product introduction</b> .....	<b>6</b>
Product overview.....	6
Package contents .....	6
<b>Physical dimensions and interfaces</b> .....	<b>7</b>
Physical dimensions.....	7
Interfaces.....	8
Insert SIM card .....	9
Assemble and attach the mounting bracket .....	12
Overview of completed mounting.....	12
Power the CBRS Survey UE.....	20
Ethernet cable weather seal assembly.....	20
PoE-03 power supply .....	24
PoE-03 LED indicators .....	24
<b>Installation</b> .....	<b>25</b>
Typical Fixed Wireless antenna installation.....	25
<b>Configuration interface</b> .....	<b>26</b>
Normal configuration.....	26
Advanced configuration.....	26
Log in.....	26
Confirm successful connection .....	27
<b>Status</b> .....	<b>28</b>
Configuration tool menus .....	31
<b>Networking</b> .....	<b>32</b>
Wireless WAN.....	33
Data connection.....	33
Manually configuring a connection profile.....	34
Confirming a successful connection .....	36
Checking data usage .....	36
Operator settings.....	38
Operator settings.....	38
SIM security settings.....	39
Unlocking a PIN locked SIM.....	39

Enabling/Disabling SIM PIN protection .....	41
Changing the SIM PIN code.....	41
Unlocking a PUK locked SIM .....	42
LAN .....	43
LAN configuration.....	43
DNS masquerading.....	44
<b>Services.....</b>	<b>45</b>
Network time (NTP).....	46
Timezone settings .....	46
NTP settings .....	46
Remote management .....	47
TR-069.....	47
TR-069 configuration .....	48
SAS.....	49
Speed Test .....	49
Run speed test.....	49
Speed test settings.....	50
Test results.....	51
<b>System .....</b>	<b>53</b>
Log .....	53
System log .....	54
Log file .....	54
System log settings.....	55
Log capture level .....	55
Non-volatile log.....	56
Remote syslog server .....	56
System Configuration .....	56
Administration.....	58
Administration settings .....	58
Accessing the antenna configuration pages remotely .....	60
Reboot .....	60
<b>Logging out.....</b>	<b>61</b>
<b>Appendix A – Default Settings .....</b>	<b>62</b>
<b>Appendix B – Safety and compliance .....</b>	<b>63</b>
RF Exposure.....	63
FCC Statement.....	63
FCC compliance.....	63
FCC regulations.....	63
Company details .....	64
Product details.....	64

# Overview

## Introduction

This document provides all the information required to configure and deploy the Casa Systems CFW-2172 antenna.

This User Guide relates to the CFW-2172's physical components and its web user interface.

Normally only the installing technician would require access to the CFW-2172's web user interface, if at all. End users would not normally ever need to access this web user interface and would probably be unaware of it.

Ordinarily a customer/end user's connection to the internet would be exclusively governed by the settings of their **Wi-Fi Gateway**. Those settings would depend on the model or brand of gateway, type of connection, requirements of the service provider, etc. and are beyond the scope of this document.

## Target audience

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

## Prerequisites




Before using the CFW-2172 CBS Survey UE, please confirm that you have:

- ▲ A WiFi-enabled smartphone with the Google Chrome™ browser or the Safari® browser.
- ▲ read the entire Safety and product care section of this document and RF Exposure information.

You may also require other screws and fasteners depending on your circumstances.

## 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.

# Product introduction

## Product overview

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

Designed to optimize signal strength in weak signal areas, the CBRS Survey UE allows an installer to find the position on the premises with the strongest signal and therefore the optimal position to install the customer device.

## Package contents

The CFW-2172 in-box contents include:

- ▲ 1 x CFW-2172 CBRS Survey UE
- ▲ 1 x Handle
- ▲ 1 x Smartphone holder
- ▲ 1 x Mounting bracket

Accessories used in this solution (packaged separately):

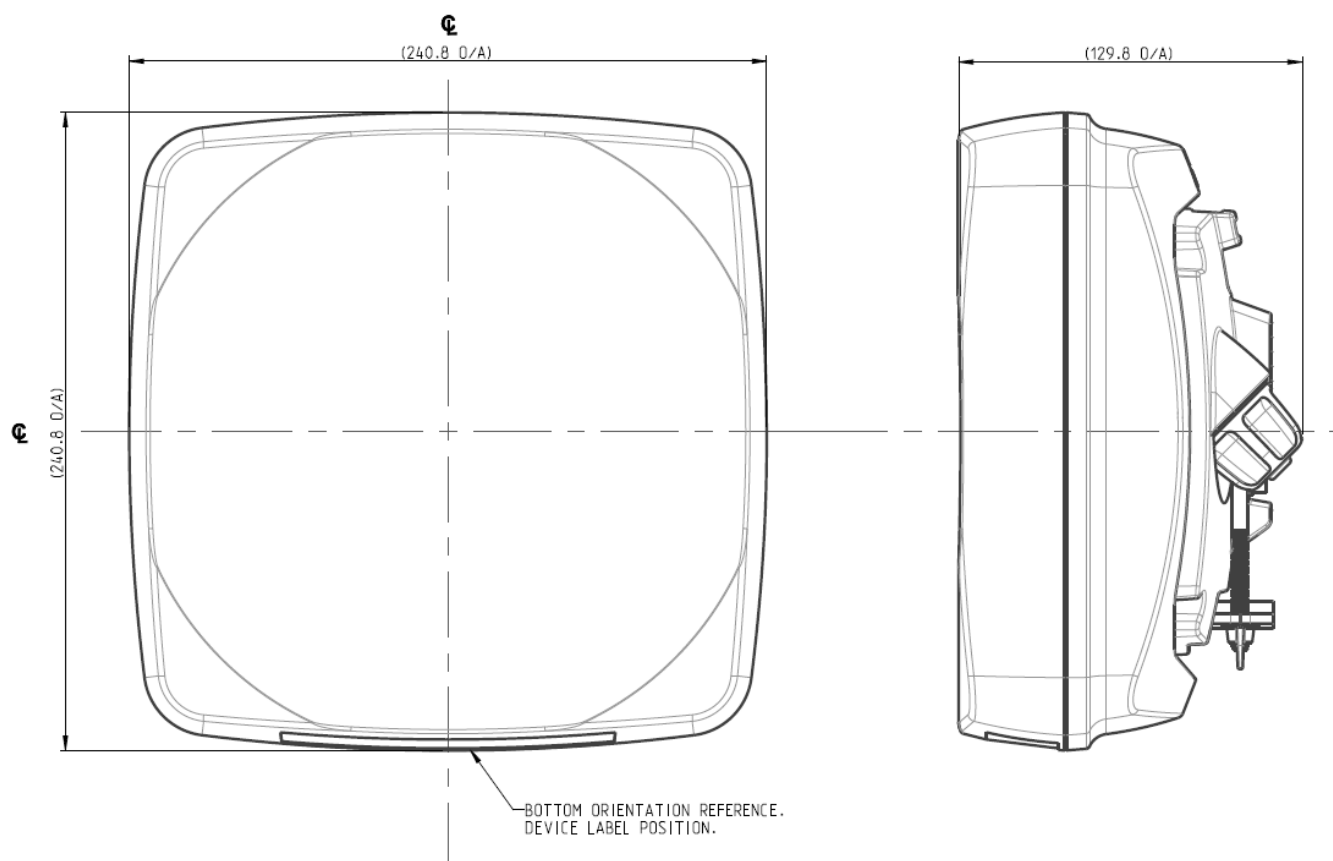
- ▲ 1 x Smart Antenna Tool – used to power the CFW-2172 during normal operation

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

# Physical dimensions and interfaces

## Physical dimensions

Below is a list of the physical dimensions of the CFW-2172.



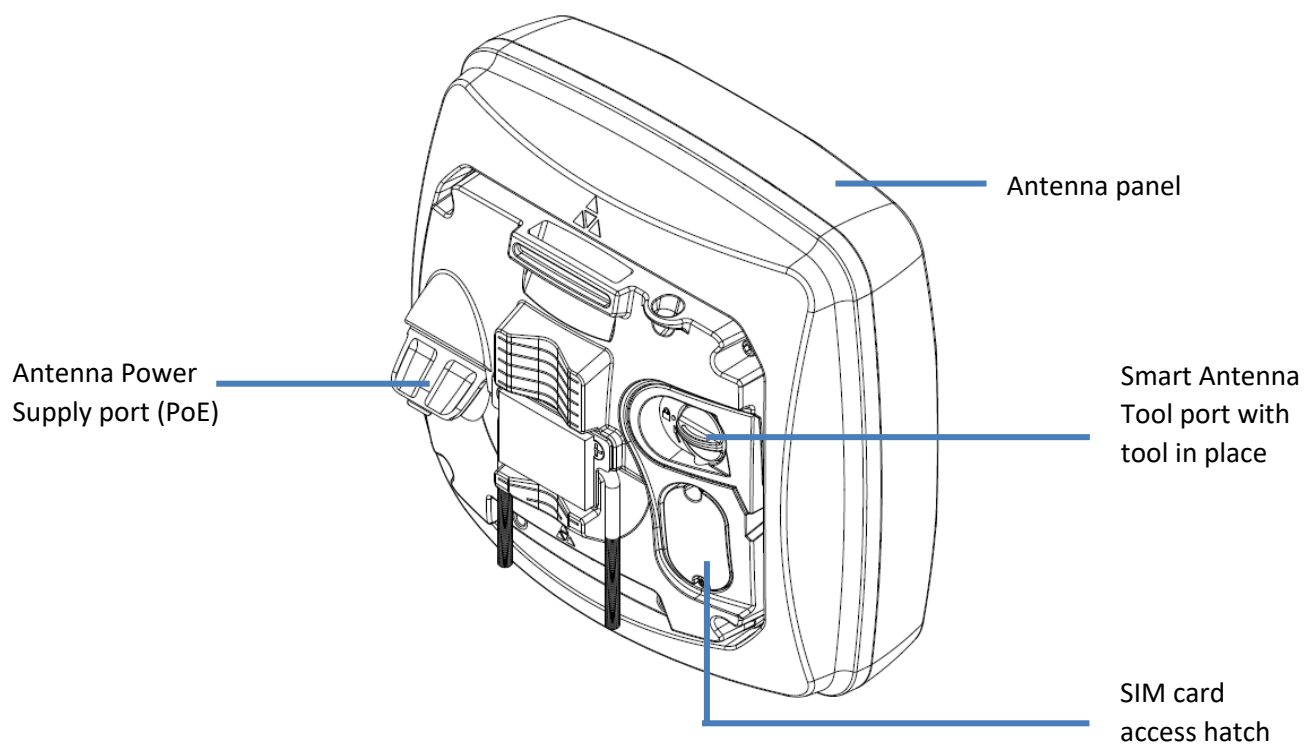
*Figure 1 – CFW-2172 Dimensions*

**CFW-2172 Dimensions**

Length	241 mm
Width	241 mm
Height	130 mm
Weight	TBC

*Table 1 - Device Dimensions*

## Interfaces



*Figure 2 – Interfaces*

Item	Description
Antenna panel	Includes 2 pairs Cross polarised antennas and GPS antenna
Smart Antenna Tool port	Connect the Smart Antenna Tool here
SIM hatch	Open the hatch to insert SIM here
Antenna Power Supply port (PoE)	Provides power and data connectivity to the CFW-2172 with Ethernet cable

*Table 2 – Interfaces*



## Insert SIM card

The CFW-2172 accepts SIM cards in Mini-SIM (3FF) format. Follow the instructions below to insert a SIM card.

- 1 On the back of the CFW-2172 antenna, locate the SIM hatch. Using a T10 screwdriver, unscrew the two screws on the SIM hatch then remove the cover to reveal the SIM card slot.



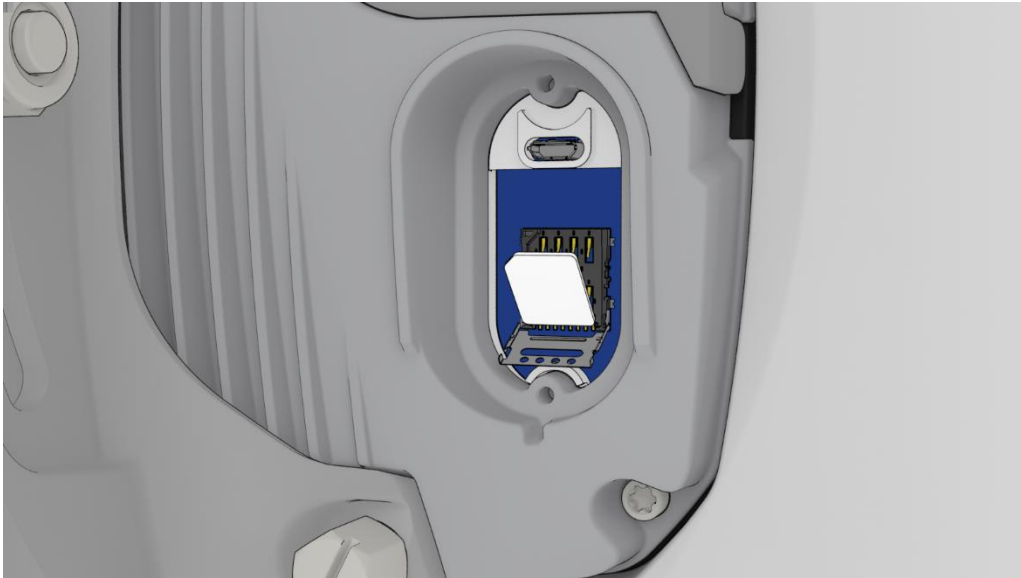
*Figure 3 - Removing screws from the SIM hatch*

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



*Figure 4 – Opening the SIM locking mechanism*

- 3 Place the SIM card onto the SIM card reader as shown in the picture below.



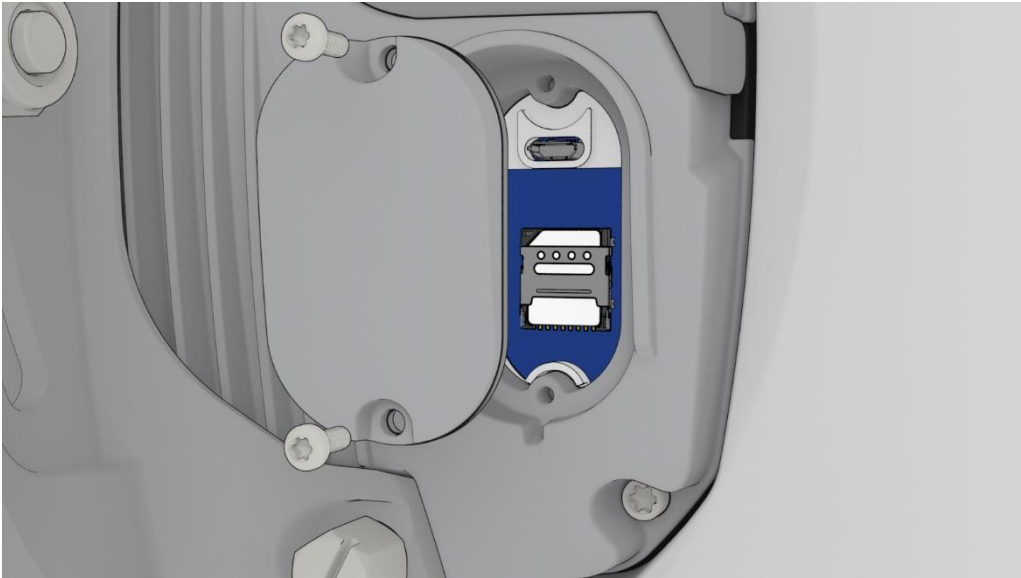
*Figure 5 – Placing the SIM card onto the SIM card reader*

- 4 While holding the SIM card onto the reader, swing the locking mechanism up and ensure that it clips into place to secure the SIM card.



*Figure 6 - SIM card locked in place*

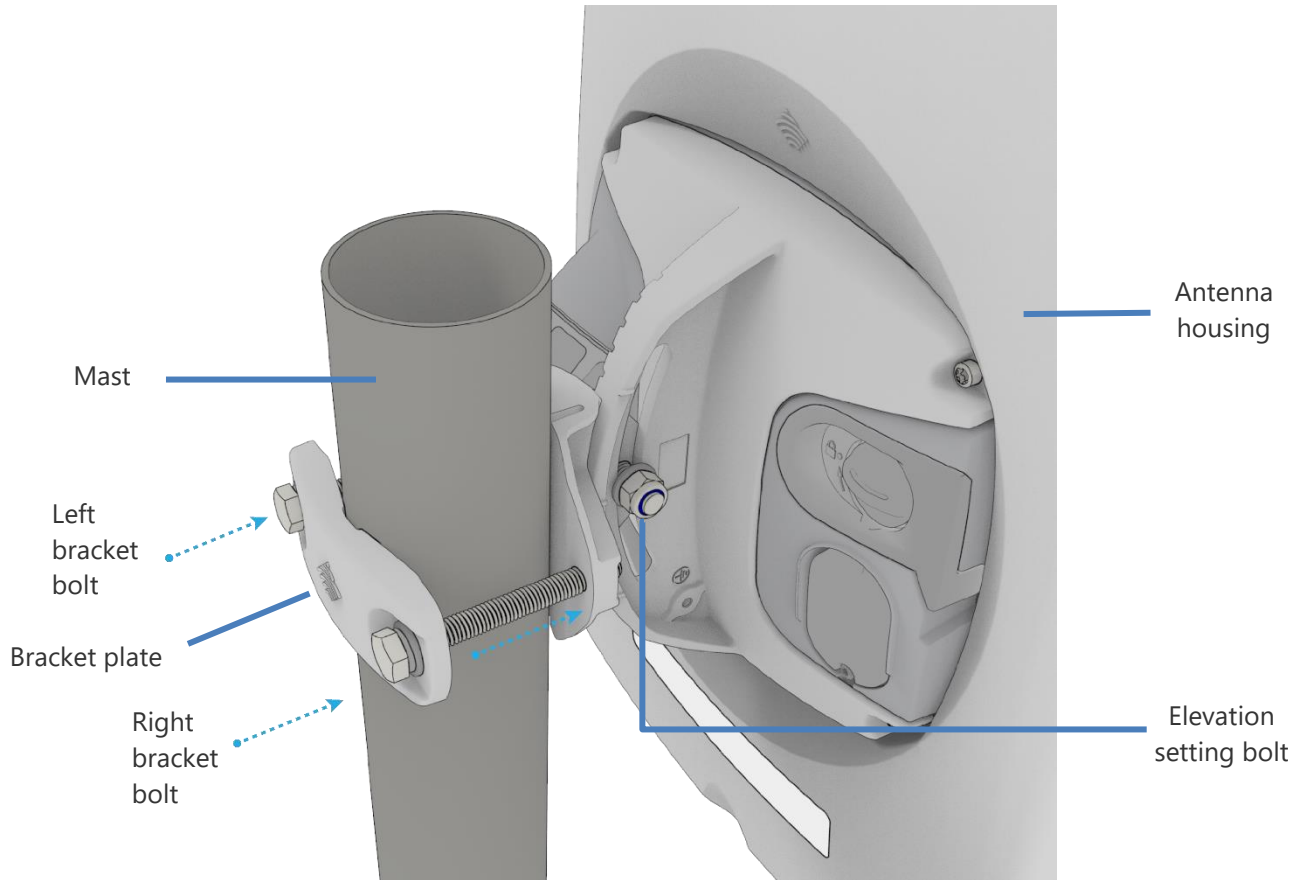
- 5 Replace the SIM hatch and seal, insert the two screws and firmly hand tighten them using a T10 screwdriver.



*Figure 7 - Replacing the SIM hatch*

## Assemble and attach the mounting bracket

### Overview of completed mounting



*Figure 8 - CFW-2172 mounting bracket and bolts*

#### Notes on mounting:

- Use a standard 13m socket wrench for all bolts
- Tighten bolts to the following torque settings:
  - Captive radome mount bolts: 4 Nm / 35 in-lbs
  - Angle pivot bolt: 7 Nm / 65 in-lbs
  - Pipe clamp bolt: 7 Nm / 65 in-lbs
- Do not over tighten bolts



## Handle assembly

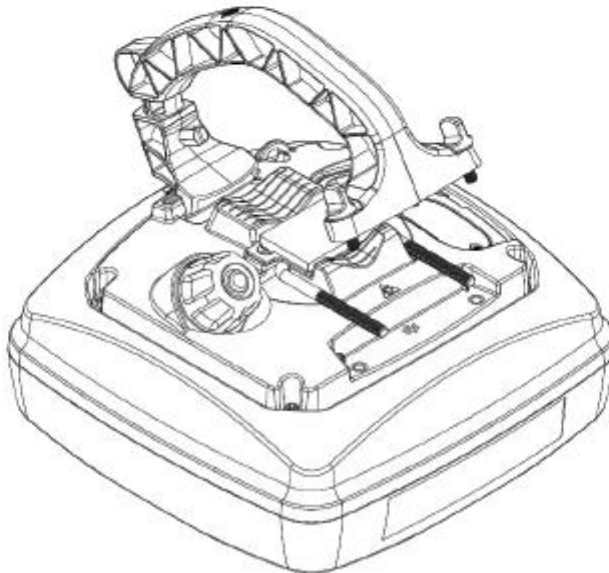
1

Place on table.



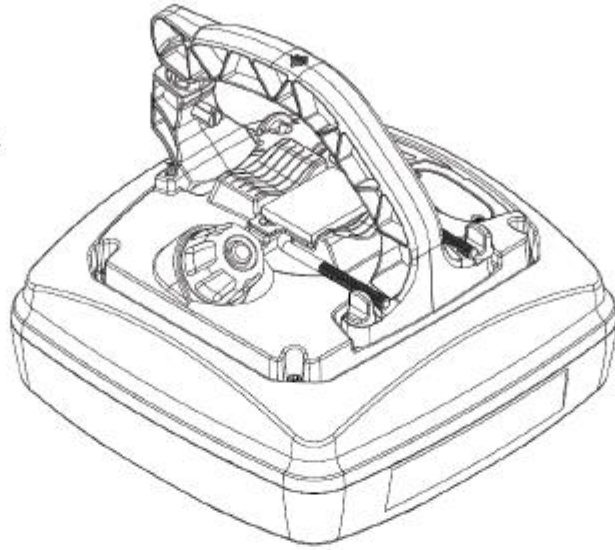
2

Attach handle.



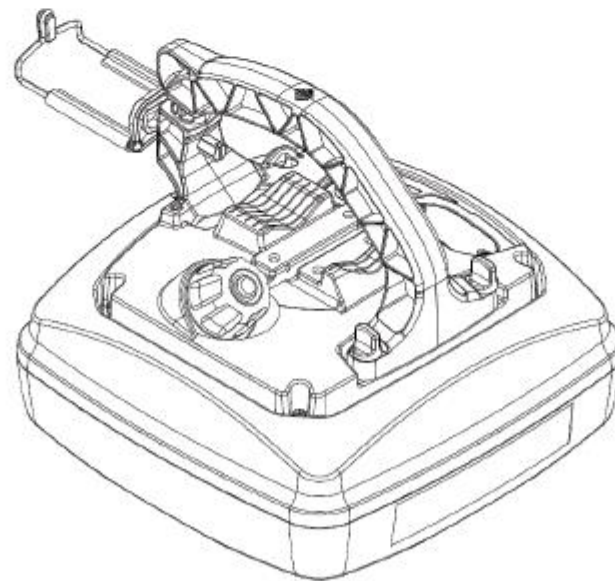
3

Secure handle bolts.



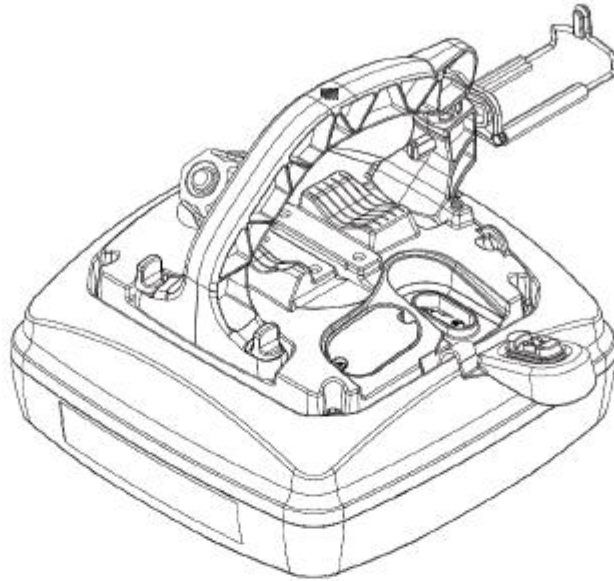
4

Attach mobile phone holder.



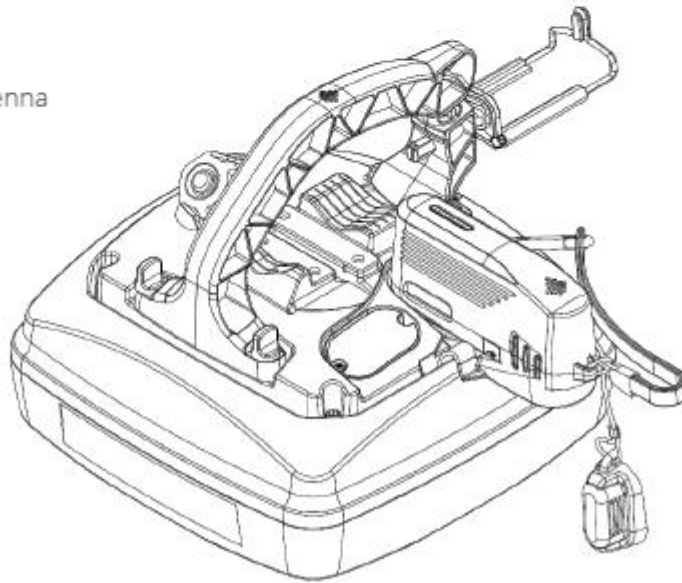
5

Open Smart Antenna  
Tool port.



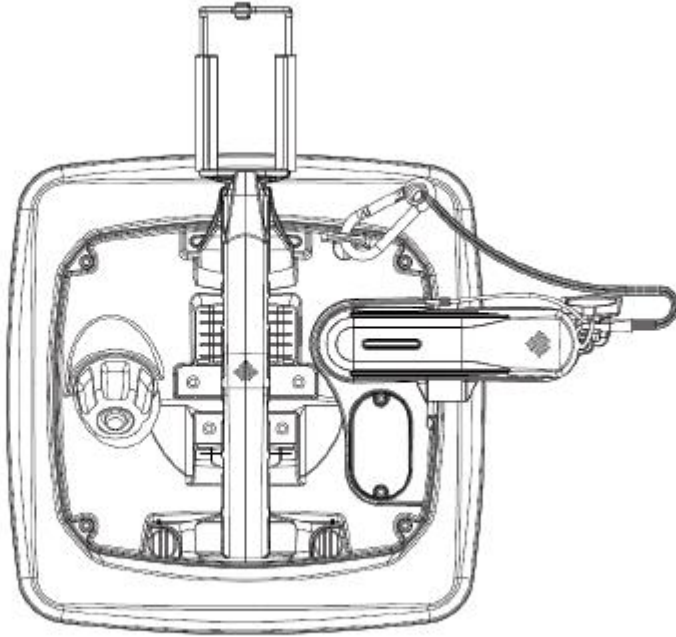
6

Connect Smart Antenna  
Tool.



7

Attach Smart Antenna Tool's lanyard/carabena to the provided hook.

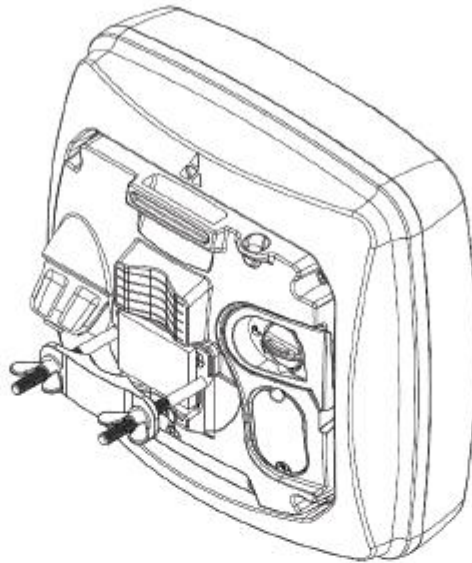




## Pole mount assembly

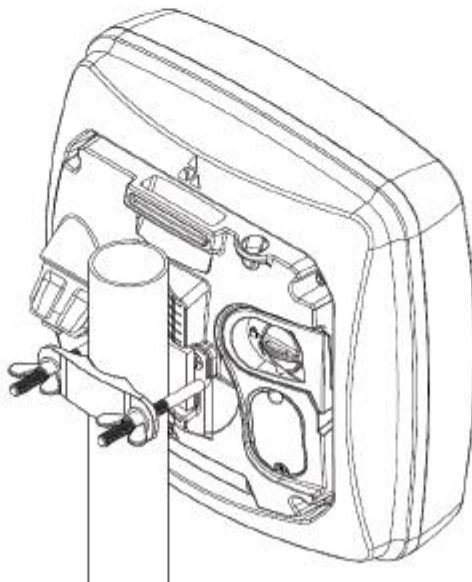
1

Lift U-bolt, place clamp bracket over bolt and fasten with wingnuts.



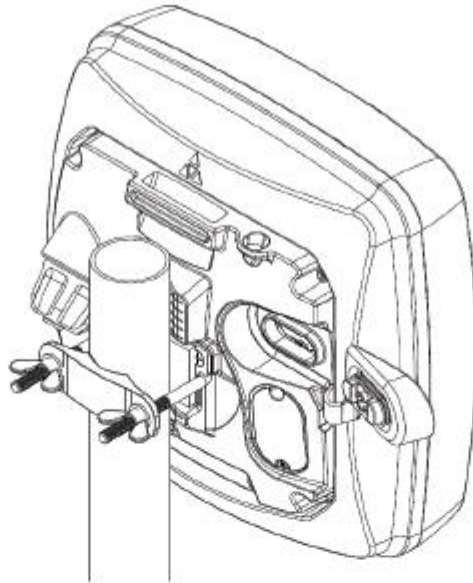
2

Place over pole and hand-tighten wingnuts.



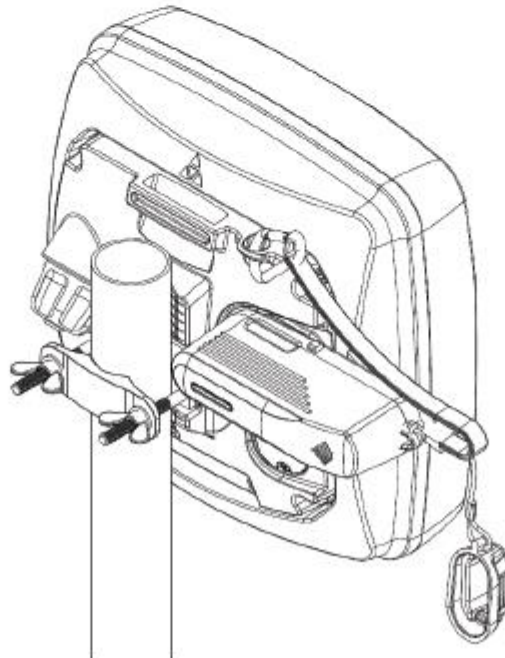
3

Open Smart Antenna  
Tool port.



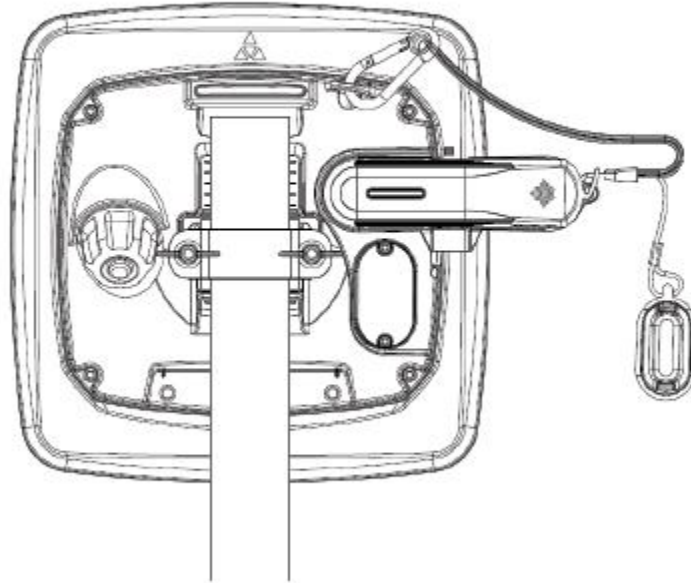
4

Connect Smart  
Antenna Tool.



## 5

Attach Smart Antenna Tool's lanyard/carabena to the provided hook.



## Power the CBRS Survey UE

Power over Ethernet (PoE) is a method of connecting network devices through Ethernet cable where power and data are passed along a single cable. It is therefore a convenient method of powering the CBRS Survey UE.



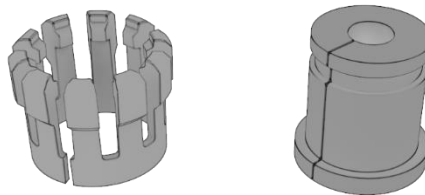
**Note** – The CFW Power supply is packaged and supplied separately.

### Ethernet cable weather seal assembly

The CFW-2172 antenna's power supply weather seal must be properly attached to prevent dust and water from entering the CFW-2172's housing.

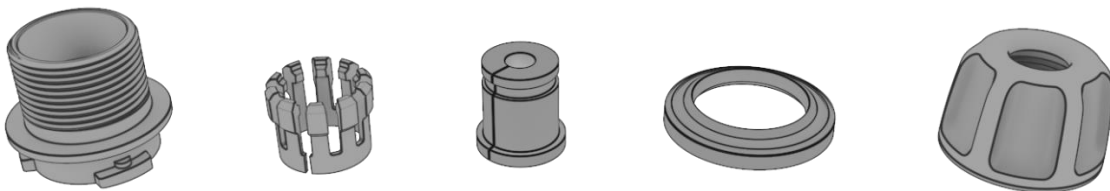
To connect Ethernet cable via the power supply weather seal:

- 1 Unscrew the weather cap and remove the rubber gasket.
- 2 Separate the rubber seal and the ferrule.



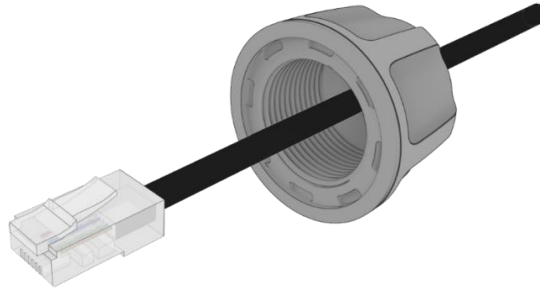
*Figure 9 - Rubber seal and ferrule*

- 3 Twist the neck for the seal counter-clockwise to remove it from the CFW-2172 housing. You should now have 5 pieces of the weather seal.



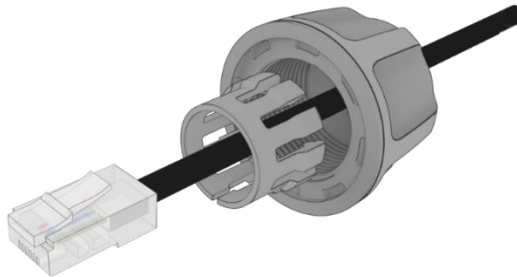
*Figure 10 - Weather seal in five parts*

- 4 Place the Ethernet cable through the nut first, as shown below.



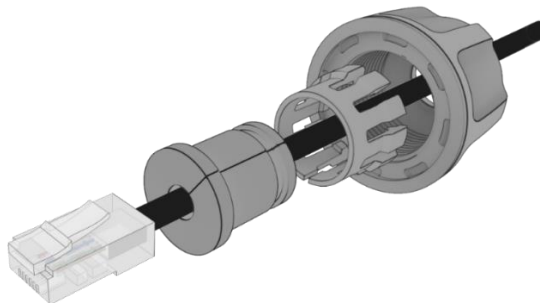
*Figure 11 - Nut placed over Ethernet cable*

- 5 Place the ferrule over the Ethernet cable as shown, making sure that the "teeth" are facing the nut.



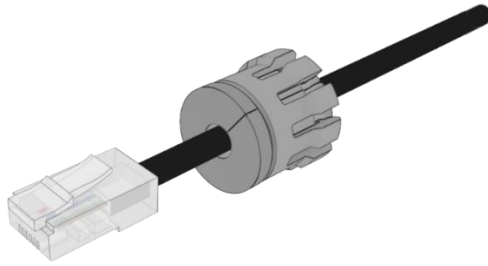
*Figure 12 - Ferrule placed over Ethernet cable*

- 6 Place the rubber seal over the Ethernet cable with the wide end toward the RJ45 plug. See the image below for the correct orientation.



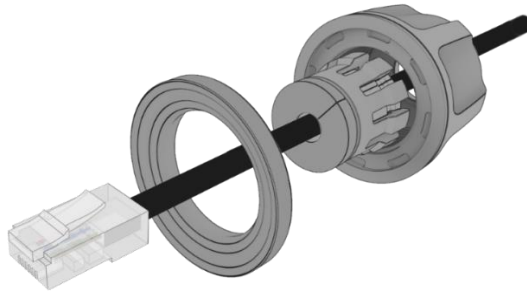
*Figure 13 - Rubber seal placed over Ethernet cable*

- 7 Push the ferrule over the rubber seal to prevent it from coming apart.



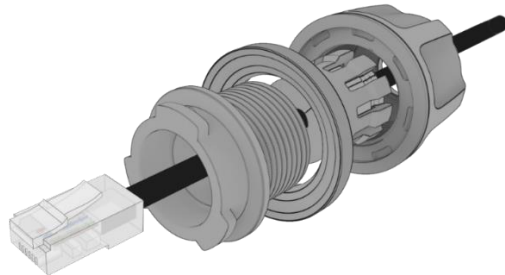
*Figure 14 - Ferrule placed over rubber seal*

- 8 Place the washer seal over the Ethernet cable as shown below. Ensure that the inside protruding lip is on the opposite side of the Ethernet plug.



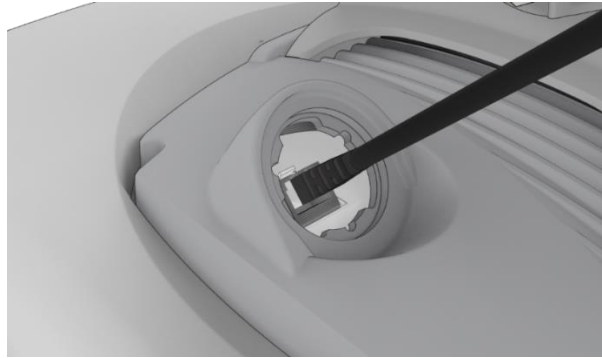
*Figure 15 - Washer seal placed over Ethernet cable*

- 9 Place the neck over the Ethernet cable as shown below.



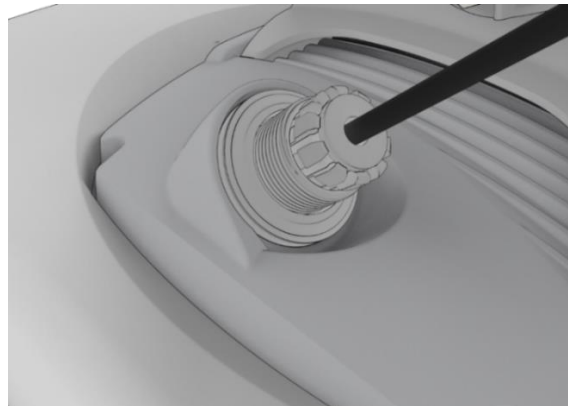
*Figure 16 - Neck placed over Ethernet cable*

- 10 Plug the Ethernet cable into the Ethernet port.



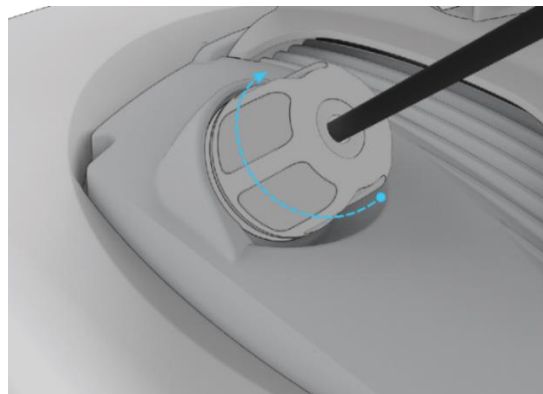
*Figure 17 - Plugging in the Ethernet cable*

- 11 Put the neck into the opening and turn the neck clockwise until it locks in place.
- 12 Push the rubber seal and ferrule into the neck then screw the nut on to the neck.



*Figure 18 - Rubber seal and ferrule inserted into neck*

- 13 Turn the nut clockwise to tighten it the washer seal against the housing. Continue turning the nut until completely assembled. This will allow the washer seal to grip the cable while also applying enough pressure to the washer seal to prevent dust and moisture entering the unit.



*Figure 19 - Turning the nut clockwise*

## PoE-03 power supply

Use the PoE-03 power supply to power your CBRS Survey UE:

- 1 Connect the Antenna Power Supply (POE-03) to a dedicated AC power outlet away from running water, steam and excessive heat. Switch the outlet ON if required.
- 2 Plug the end of the R45 Ethernet cable that does not have the weather-sealed plug into the R45 socket named **WALL** on the PoE-03.
- 3 Fasten the end of the R45 Ethernet cable that has the weather-sealed plug into the antenna power supply port on the back of the antenna as per instructions in steps 11, 12 and 13 in the previous section.
- 4 The lights on the POE-03 injector housing will indicate whether the power supply is connected using its LED indicator lights. When the POWER LED is red and ANTENNA LED is green, the CBRS Survey UE is correctly powered and connected.

### PoE-03 LED indicators

The table below describes the status of the POWER and ANTENNA LEDs on the PoE injector.

LED	Status	Description
POWER	Solid red	Antenna power supply is connected to AC power.
ANTENNA	Solid green	Antenna power supply is connected to AC power and the PoE port is connected to the CBRS Survey UE.

*Table 3 - POE-02 LED indicators*

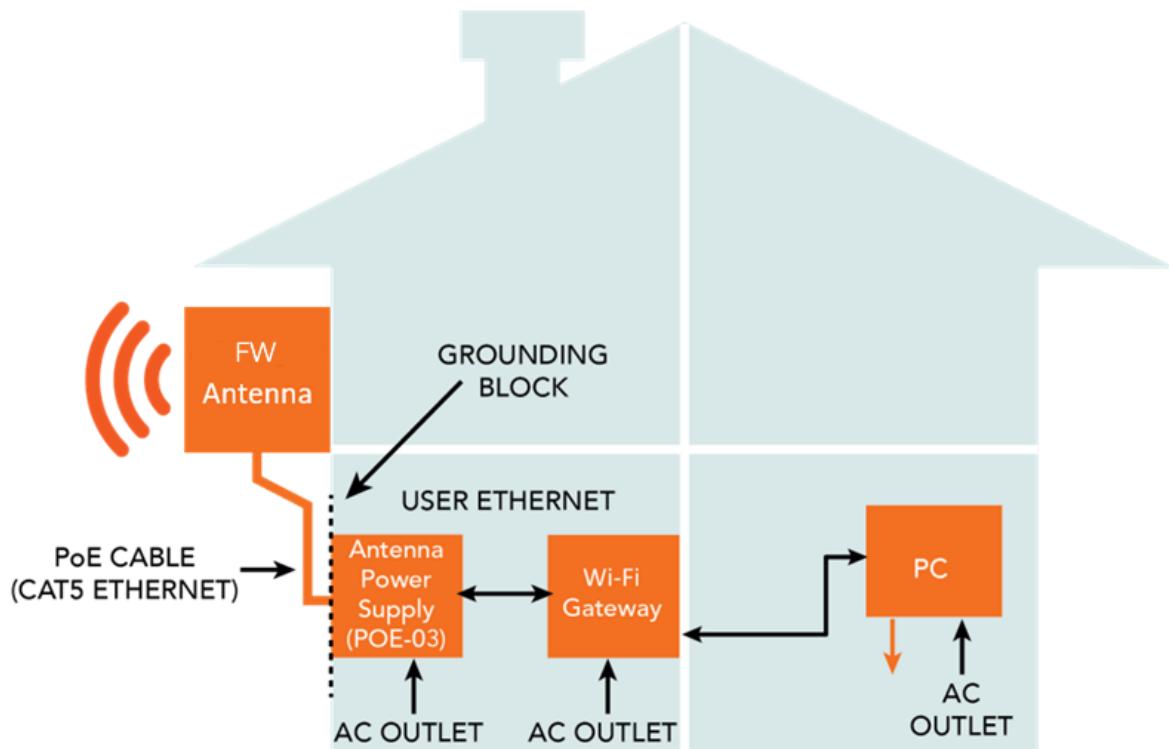


## Installation

The positioning and installation of an antenna is achieved by a trained technician using the CBRS Survey UE and the Smart Antenna Tool.

### Typical Fixed Wireless antenna installation

The image below illustrates a typical installation of the CBRS Survey UE on the side of a building.



*Figure 20 – Typical CBRS Survey UE Installation*

Note that this User Guide relates to the CFW-2172's physical components and its web user interface.

Normally only the installing technician would require access to the CFW-2172's web user interface, if at all.

Ordinarily a customer's connection to the internet would be exclusively governed by the settings of the **Wi-Fi Gateway**, see Figure 3. Those settings would depend on the type of connection, brand of gateway, requirements of the service provider, etc.

# Configuration interface

## Normal configuration

In most cases the default settings should work as soon as the Ethernet power supply is connected to AC power and the PoE port is connected to the CBRS Survey UE device.

## Advanced configuration

For advanced configuration, log in to the web-based user interface of the CFW-2172.

### Log in

To log in to the web-based user interface:

- 1 Open a web browser (e.g. Internet Explorer, Firefox, Safari), type <https://192.168.1.1> into the address bar and press **Enter**.
- 2 The web-based user interface **Log in** screen is displayed.

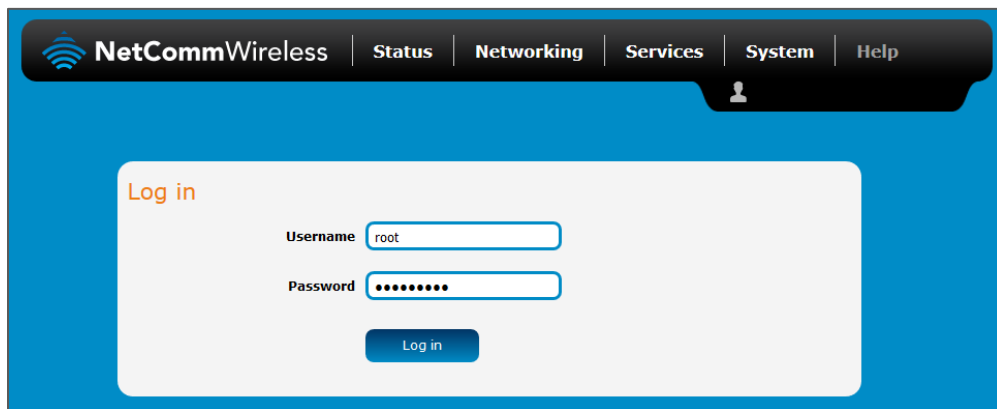


Figure 21 – Log in prompt for the web-based user interface

- 3 Enter the login **Username** and **Password**.

Admin manager account	
<b>Username</b>	root
<b>Password</b>	*****

Table 4 - Management account login details – Admin manager

## Confirm successful connection

To confirm the connection status, click the **Status** menu item at the top of the page to display the **Status** page. When there is a mobile broadband connection, the **WWAN connection status** section is expanded showing the details of the connection and the **Status** field displays **Connected**.

To see details on the connected session, you can click the **Show data usage** button.

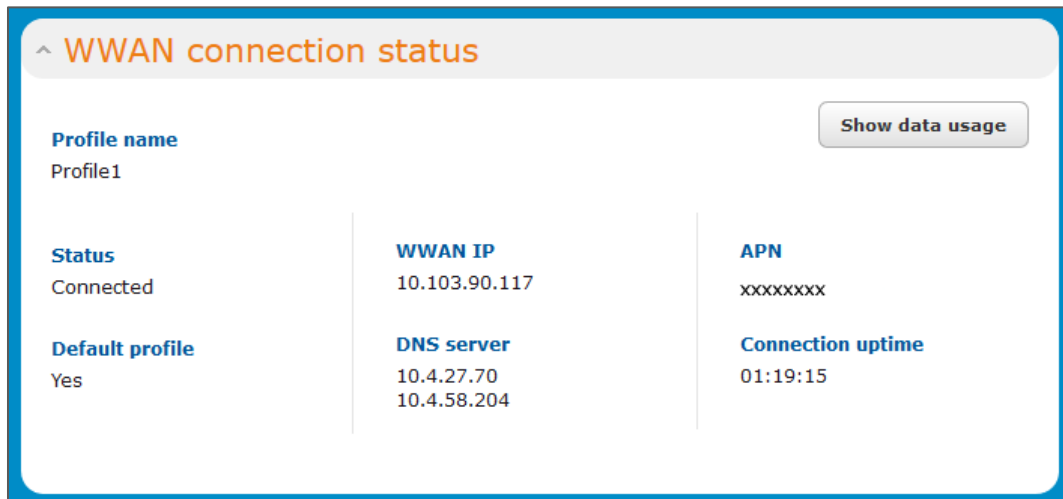


Figure 22 - WWAN connection status section

# Status

The **Status** page of the web interface provides system related information and is displayed when you initially log in to the CFW-2172 management console.

The screenshot shows the NetCommWireless management console interface. The 'Status' tab is selected in the top navigation bar. The page is divided into several sections:

- System information:**
  - System up time:** 00:02:55
  - Device version:** Hardware version 1.4, Serial number 070028194400052, Firmware version V1.1.25.94349
  - Cellular module:** Model MDM9350, Module firmware MPSS.AT.2.5.1-00605-9655\_GEN\_PACK-1.223146.2.224735.1, IMEI 354237100010610, Hardware 10001
- LAN:** IP 192.168.7.1 / 255.255.255.0, MAC address F8:CA:59:20:FA:1E, Ethernet port status: Down
- Cellular connection status:**
  - SIM status:** SIM OK
  - Signal strength (dBm):** -88 dBm (High)
  - Network registration status:** Registered, home network
  - Operator selection:** Automatic
  - Current operator:** CarrierName
  - Roaming status:** Not roaming
  - Allowed bands:** LTE Band 48 - TDD 3600
  - Current band:** LTE Band 48 - TDD 3600
  - Coverage:** LTE
- WWAN connection status:**
  - Profile name:** Profile1
  - Status:** Connected
  - Default profile:** Yes
  - WWAN IP:** 192.168.3.6
  - DNS server:** 192.168.3.1, 2001:4860:4860:1:8888
  - APN:** wldata
  - Connection uptime:** 00:01:30
- Advanced status:**
  - Mobile country code:** 312
  - Mobile network code:** 680
  - SIM ICCID:** 89860000502000180722
  - Tracking Area Code (TAC):** 1
  - IMSI:** 001010123456789
  - Cell ID:** 27447297
  - Channel number:** XXXXXXXXXXXXX
  - Reference Signal Received Power (RSRP):** -88 dBm
  - Reference Signal Received Quality (RSRQ):** -4 dB
  - Packet service status:** Attached
- Cell information:**

PCI	EARFCN	RSRP	RSRQ	Serving
1	56340	-87.4	-3.7	✓
2	56490	-93.6	-10.4	
3	56490	-94.7	-11.5	
4	56490	-94.8	-11.6	
5	56640	-98.5	-6.2	

Figure 23 – Status page

The **Status** page shows **System information**, **LAN details**, **Cellular connection** status, **WWAN connection** status, **Advanced** status and **Cell information** details.

You can toggle the sections from view by clicking the  or  buttons to expand or collapse the amount of information displayed for each.

The following table contains a description of each of the items on the Status page.

Item	Definition
<b>System information</b>	
System up time	The current uptime of the CBRS Survey UE.
Hardware version	The hardware version of the CBRS Survey UE.
Serial Number	The serial number of the CBRS Survey UE.
Firmware version	The firmware version of the CBRS Survey UE.
Model	The type of phone module and the firmware version of the 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.
Hardware	A hardware identifier.
<b>LAN</b>	
IP	The IP address and subnet mask of the CBRS Survey UE.
MAC address	The MAC address of the CBRS Survey UE.
Ethernet port status	Displays the current status of the Ethernet port and its operating speed.
<b>Cellular connection status</b>	
SIM Status	Displays the activation status of the CBRS Survey UE on the carrier network.
Signal strength (dBm)	The current signal strength measured in dBm
Network registration status	The status of the CBRS Survey UE's registration for the current network.
Operator selection	The mode used to select an operator network.
Current operator	The current operator network in use.
Roaming status	The roaming status of the CBRS Survey UE.
Allowed bands	The bands to which the CBRS Survey UE may connect.
Current band	The current band being used by the CBRS Survey UE.
Coverage	The type of mobile coverage being received by the CBRS Survey UE.
<b>WWAN connection status</b>	
Profile name	The name of the currently active profile.

Item	Definition
Status	The connection status of the currently active profile.
Default profile	Indicates whether the current profile in use is the default profile.
WWAN IP	The IP address assigned by the mobile broadband carrier network.
DNS server	The primary and secondary 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.
<b>Advanced status</b>	
Mobile country code	The Mobile Country Code (MCC) of the mobile network operator.
Mobile network code	The Mobile Network Code (MNC) of the mobile network operator.
SIM ICCID	The Integrated Circuit Card Identifier of the SIM card used with the CBRS Survey UE, a unique number up to 19 digits in length.
Tracking Area Code (TAC)	Identifies a tracking area within a particular network.
IMSI	The International Mobile Subscriber Identity is a unique identifier of the user of a cellular network.
Cell ID	A unique code that identifies the base station from within the location area of the current mobile network signal.
Channel number	The number assigned to the frequency of the current cellular connection.
Reference Signal Received Quality (RSRQ)	RSRQ calculates signal quality taking into consideration the RSSI. It is calculated by $N \times RSRP / RSSI$ where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.
Reference Signal Received Power (RSRP)	A cell-specific reference signal used to determine RSRP.
Packet service status	Displays whether the packet service is <b>Attached</b> or <b>Detached</b> . When APN or username/password is changed, the device detaches and reattaches to the network.
<b>Cell Information</b>	
PCI	Physical Cell Identity is used to identify a cell based on a combination of its Primary Synchronization Signal (PSS) and (Secondary Synchronization Signal (SSS).
EARFCN	The absolute radio-frequency channel number (ARFCN) is a code that identifies the physical radio uplink/downlink channel pair used for transmission and reception.
RSRP	The Reference Signal Received Power value is a cell-specific reference signal used to determine RSRP.
RSRQ	The Reference Signal Received Quality value calculates signal quality taking into consideration the RSSI. It is calculated by $N \times RSRP / RSSI$ where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.

Item	Definition
Serving	A ✓ green check mark indicates that the cell location is currently functioning.

Table 5 - Status page item details

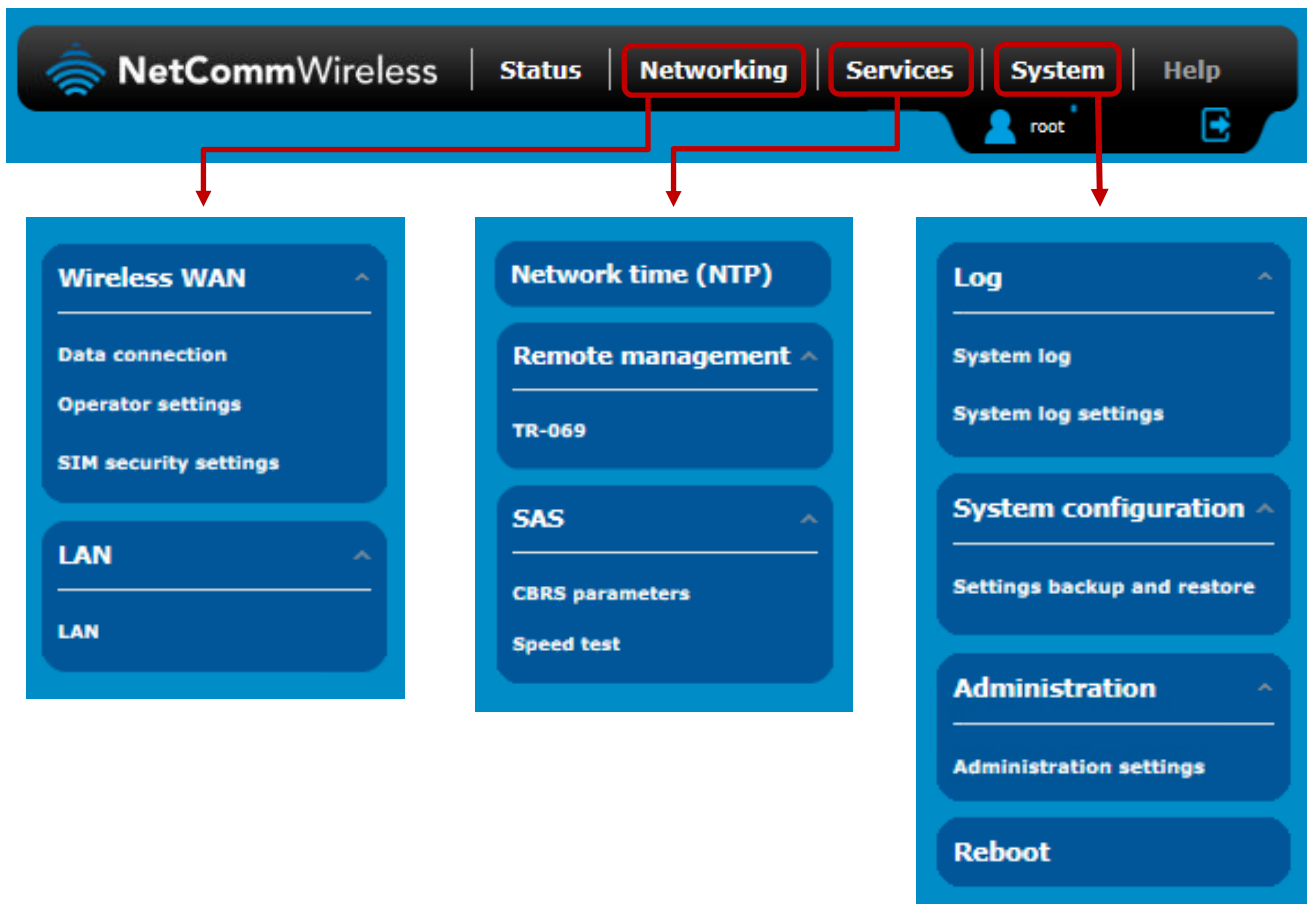
## Configuration tool menus

Advanced configuration settings are arranged into three menu groups accessible by clicking the buttons which appear to the left of the **Status** button in the top tool bar: **Networking**, **Services** and **System**.

Click on one of the menu buttons and its corresponding menu will appear in the left margin.

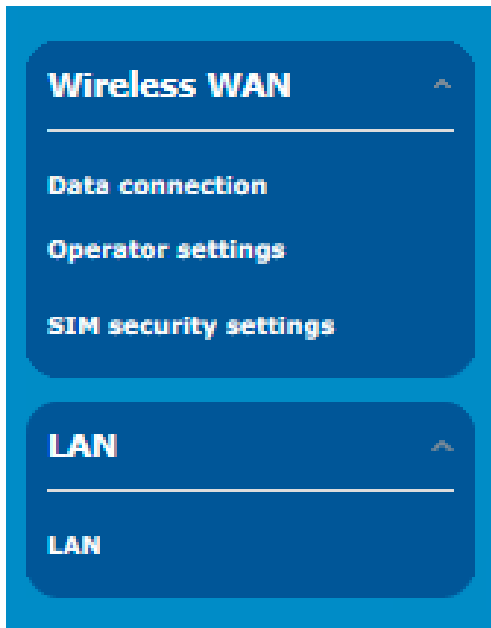
Many of the menu items have submenus. Click the ▼ down arrow to expand the submenus.

The following diagram shows each expanded menu and its submenus with an arrow from its corresponding menu button:



Each configuration tool group will be explained in the following sections.

# Networking



The **Networking** tool group provides configuration options for **Wireless WAN** and **LAN** connections.

The **Wireless WAN** section contains three groups useful in managing your network connection and SIM card security.

Settings in the **LAN** section allow you to configure a new IP Address and/or Subnet mask for the antenna and to enable or disable DNS Masquerading.



## Wireless WAN

### Data connection

The data connection page allows you to configure and enable/disable connection profiles. To access this page, click on the **Networking** menu, and under the **Wireless WAN** menu, select the **Data connection** item.

The profile refers to a set of configuration items which are used by the antenna to activate a Packet Data (PDP) context.

There is only one profile defined for the CFW-2172.

Profile name				
	Default	Status	APN	Username
Profile1	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	Blank	
Profile2	<input type="radio"/>	<input type="checkbox"/>	ims	
Profile3	<input type="radio"/>	<input type="checkbox"/>	SOS	
Profile4	<input type="radio"/>	<input type="checkbox"/>	Blank	
Profile5	<input type="radio"/>	<input type="checkbox"/>	Blank	
Profile6	<input type="radio"/>	<input type="checkbox"/>	Blank	

Figure 24 – Data connection settings

Item	Definition
<b>Profile name</b>	System reference name, cannot be changed by user.
<b>Default</b>	Sets the corresponding profile to be the default gateway for all outbound traffic except traffic for which there are configured static route rules or profile routing settings.
<b>Status</b>	Toggles the corresponding profile <b>ON</b> or <b>OFF</b> . Only one profile may be turned on at any time.
<b>APN</b>	The Access Point Name assigned to the corresponding profile.

<b>Username</b>	The username used to log on to the corresponding APN.
<b>Save button</b>	Click the <b>Save</b> button to save and apply any changes.

*Table 6 - Data connection item details*

## Manually configuring a connection profile

To manually configure a connection profile:

- 1 Click the  **Edit** button corresponding to the Profile that you wish to modify.

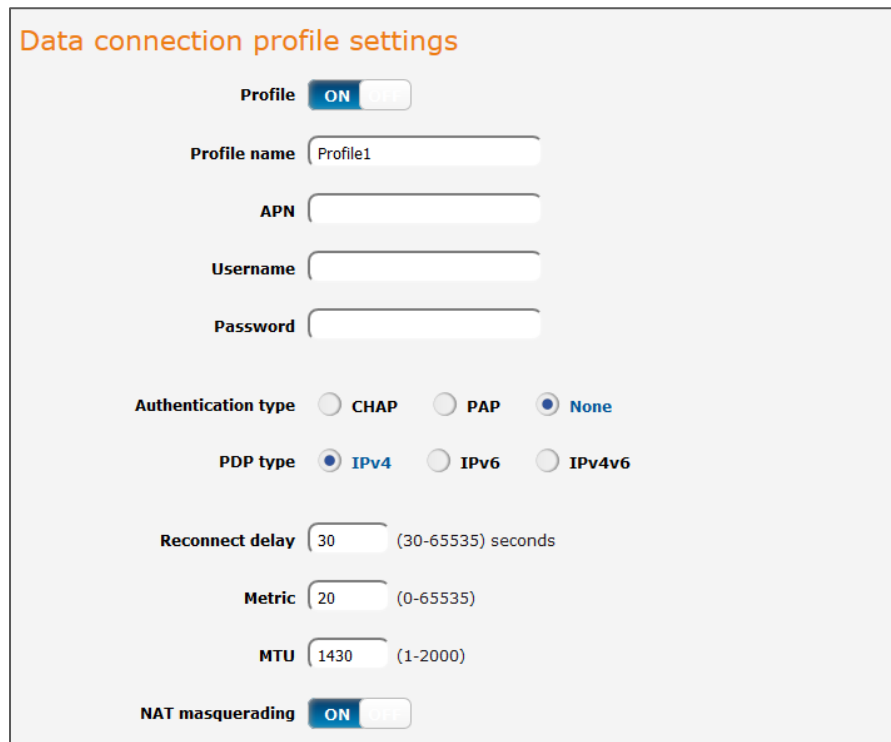
The **Data connection profile settings** page is displayed.



The screenshot shows the 'Data connection profile settings' page. At the top, the title 'Data connection profile settings' is displayed in orange. Below the title, there are three main sections: 'Profile' with a toggle switch set to 'OFF', 'Profile name' with a text input field containing 'Profile1', and 'Automatic APN selection' with a toggle switch set to 'OFF'.

*Figure 25 - Data connection profile settings*

- 2 Click the **Profile** toggle key to turn the profile **ON**.
- 3 Once enabled, additional profile details will display:



The screenshot shows the 'Data connection profile settings' page with the 'Profile' toggle switch now set to 'ON'. The 'Profile name' field remains 'Profile1'. Below this, several additional fields are visible: 'APN', 'Username', and 'Password' (all empty text input fields). Under 'Authentication type', the 'None' radio button is selected. Under 'PDP type', the 'IPv4' radio button is selected. The 'Reconnect delay' is set to 30 seconds (range 30-65535), 'Metric' is set to 20 (range 0-65535), and 'MTU' is set to 1430 (range 1-2000). At the bottom, the 'NAT masquerading' toggle switch is set to 'ON'.

*Figure 26 - Data connection settings - Profile turned on*

- 4 The **Profile name** is a system defined name used to reference the profile.

- 5 In the **APN** field, enter the APN Name (Access Point Name) and if required, use the **Username** and **Password** fields to enter your login credentials (if required).
- 6 Next to **Authentication** type, select the either **CHAP**, **PAP** or **None** depending on the type of authentication used by your provider.
- 7 The **Reconnect delay** field specifies the number of seconds to wait between connection attempts. The default setting of 30 seconds is sufficient in most cases but you may modify it to wait up to 65535 seconds if you wish.
- 8 The **Metric** value is used by antenna to prioritise routes (if multiple are available) and is set to 25 by default. This value is sufficient in most cases but you may modify it if you are aware of the effect your changes will have on the service.
- 9 The **Maximum Transmission Unit (MTU)** is the maximum packet size for the connection profile. Contact your carrier for their preferred setting.
- 10 Use the **NAT masquerading** toggle key to turn NAT Masquerading on or off. NAT masquerading, also known simply as NAT is a common routing feature which allows multiple LAN devices to appear as a single WAN IP via network address translation. In this mode, the antenna modifies network traffic sent and received to inform remote computers on the internet that packets originating from a machine behind the antenna actually originated from the WAN IP address of the antenna's internal NAT IP address. This may be disabled if a framed route configuration is required and local devices require WAN IP addresses.
- 11 Click the **Save** button when you have finished entering the profile details.

## Confirming a successful connection

After configuring the packet data session, and ensuring that it is enabled, click on the Status menu item at the top of the page to return to the **Status** page.

When there is a mobile broadband connection, the **WWAN connection status** section is expanded showing the details of the connection and the **Status** field displays **Connected**. To see details on the connected session, you can click the **Show data usage** button.

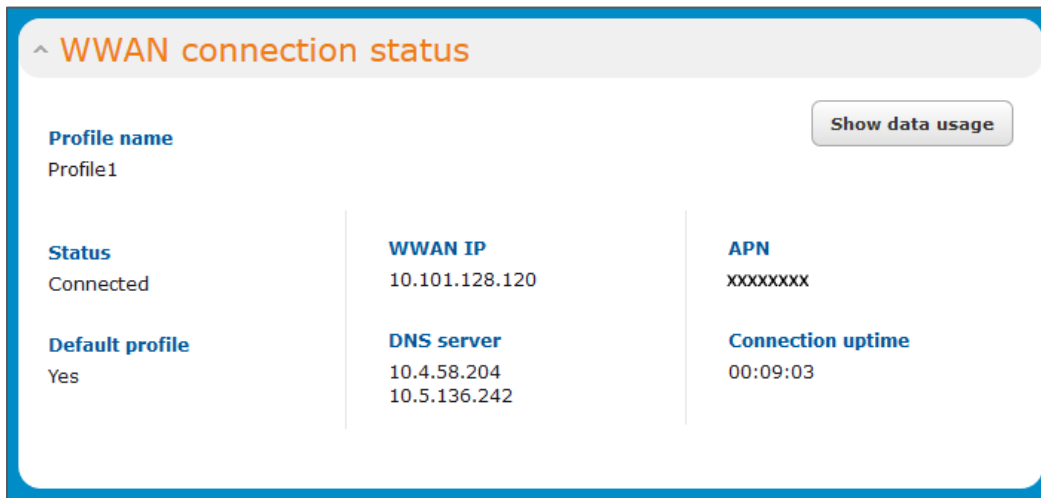


Figure 27 - WWAN connection status section

## Checking data usage

In the **WWAN connection status** section of the **Status** page, each packet data connection profile has a **Show data usage** button which displays the amount of data received, sent and a total data usage figure.

To show the data use for a connected profile, click the **Show data usage** button.

The data usage for the last 10 sessions is displayed in addition to the current session and the button name will change to **Hide data usage**.

**^ WWAN connection status**

**Profile name**  
Profile1

<b>Status</b> Connected	<b>WWAN IP</b> 10.101.128.120	<b>APN</b> XXXXXXXX
<b>Default profile</b> Yes	<b>DNS server</b> 10.4.58.204 10.5.136.242	<b>Connection uptime</b> 00:09:03

**Show duration**

Session start	Session end time	Data received (bytes)	Data sent (bytes)	Total data (bytes)
02/07/2018 05:26:40	Current session	255,024	178,016	433,040
01/01/2000 00:17:08	01/01/2000 01:54:53	5,901,397	2,535,155	8,436,552
01/01/2000 00:01:59	01/01/2000 00:15:19	331,467	178,244	509,711
29/06/2018 01:12:58	29/06/2018 02:45:13	39,371,651	3,400,024	42,771,675
29/06/2018 00:21:53	29/06/2018 01:11:02	17,790,684	1,300,695	19,091,379

\*Not for billing purposes

Figure 28 - Data usage

Click the **Show duration** link to toggle the display to show the duration of each session rather than the start and end times.

Session start	Session duration	Data received (bytes)	Data sent (bytes)	Total data (bytes)
02/07/2018 05:26:40	00:09:03	307,809	246,955	554,764
01/01/2000 00:17:08	01:37:45	5,901,397	2,535,155	8,436,552

Figure 29 - Data usage with connection duration

## Operator settings

The **Operator settings** page enables you to select which frequency band you will use for your connection and enables you to scan for available network operators in your area.

You may want to do this if you're using the antenna in a country with multiple frequency networks that may not all support LTE. You can select the antenna to only connect on the network frequencies that suit your requirements.

### Operator settings

The operator settings feature allows you to select whether to allow the antenna to automatically select a network or to manually scan for a network to which the antenna is locked.

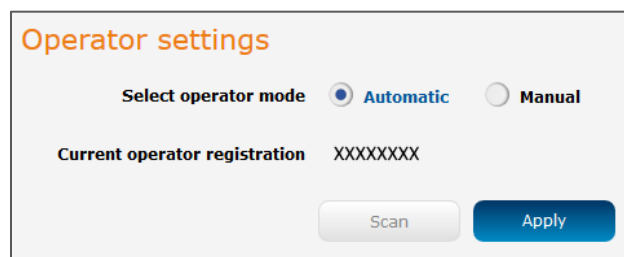


Figure 30 - Operator settings

To scan for available networks, set the **Select operator mode** from **Automatic** to **Manual** then click the **Scan** button. This operation can take a few minutes and requires that the packet data session be disconnected prior to scanning.

A list of the detected service carriers in your area is displayed.

	Operator name list	MCC	MNC	Operator status	Network type
<input checked="" type="radio"/>	Telstra	505	01	Current	LTE (4G)
<input type="radio"/>	Telstra	505	01	Available	UMTS (3G)
<input type="radio"/>	vodafone AU	505	03	Forbidden	UMTS (3G)
<input type="radio"/>	Optus AU	505	02	Forbidden	LTE (4G)
<input type="radio"/>	Optus AU	505	02	Forbidden	UMTS (3G)
<input type="radio"/>	vodafone AU	505	03	Forbidden	LTE (4G)

Figure 31 - Detected operator list

Select the most appropriate service from the list shown and click the **Apply** button.

When **Select operator mode** is set to **Automatic**, the antenna selects the most appropriate operator based on the inserted SIM card. This is the default option and is sufficient for most users.

## SIM security settings

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**.

The screenshot shows the 'PIN settings' page. At the top, there is a red warning icon and the text 'SIM is PIN locked - remaining attempt(s) 3'. Below this, there are three input fields: 'Current PIN', 'Confirm current PIN', and 'Remember PIN' (which is a checkbox). At the bottom, there is a blue 'Save' button.

Figure 32 - SIM security settings - SIM PIN locked

- 2 Enter the PIN in the **Current PIN** field and then enter it again in the **Confirm current PIN** field to confirm the PIN.
- 3 If you are placing the antenna in a remote, unattended location, you may wish to check the **Remember PIN** option. This feature allows the antenna to automatically send the PIN to the SIM each time the SIM asks for it (usually at power up). This enables the SIM to be PIN locked (to prevent unauthorised re-use of the SIM elsewhere), while still allowing the antenna to connect to the cellular service.
- 4 When this feature is enabled, the PIN you enter when setting the **Remember PIN** feature is encrypted and stored locally on the antenna. The next time the SIM asks the antenna for the PIN, the antenna decrypts the PIN and automatically sends it to the SIM without user intervention.

- When this feature is disabled and the SIM is PIN locked and the PIN must be manually entered via the antenna's configuration interface. In situations where the antenna will be unattended, this is not desirable.



**Note** – Select Remember PIN if you do not want to enter the PIN code each time the SIM is inserted.

- Click the **Save** button.

If successful, the antenna displays the following screen:

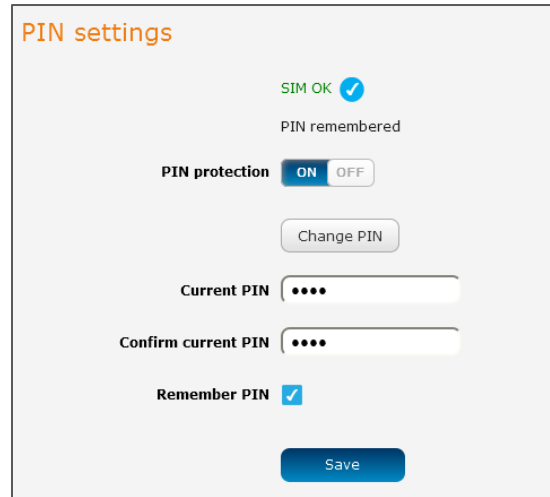
The screenshot shows a user interface for SIM security settings. At the top, a yellow-bordered box contains the text "Success!" and "The SIM unlock was successful". Below this, the "PIN settings" section is displayed. It includes a "SIM OK" status with a green checkmark, "Retries remaining: 0", and a "PIN protection" toggle switch currently set to "ON". There is a "Change PIN" button, two input fields for "Current PIN" and "Confirm current PIN", and a "Remember PIN" checkbox which is currently unchecked. A "Save" button is located at the bottom of the settings area.

*Figure 33 - SIM security settings - SIM unlock successful*



## Enabling/Disabling SIM PIN protection

The security PIN protection can be turned on or off using the **PIN protection** toggle key.

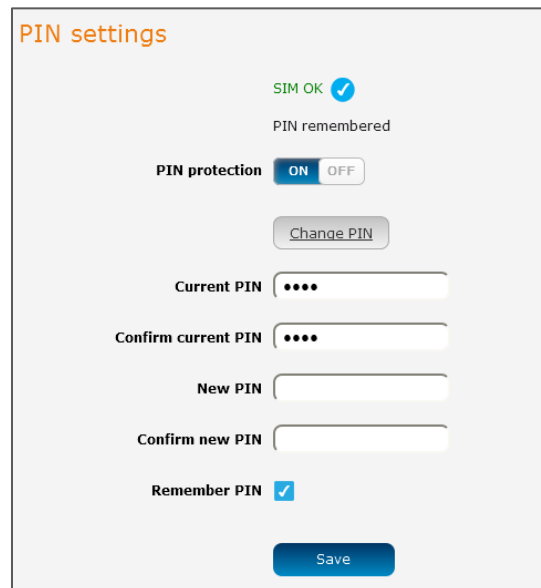


The screenshot shows the 'PIN settings' interface. At the top, it says 'SIM OK' with a blue checkmark and 'PIN remembered'. Below that is a 'PIN protection' toggle switch currently set to 'ON'. A 'Change PIN' button is visible. There are two input fields for 'Current PIN' and 'Confirm current PIN', both containing four black dots. At the bottom, there is a 'Remember PIN' checkbox which is checked, and a blue 'Save' button.

Figure 34 - PIN Settings

## Changing the SIM PIN code

If you would like to change the PIN, click the **Change PIN** button and enter the current PIN into the **Current PIN** and **Confirm current PIN** fields, then enter the desired PIN into the **New PIN** and **Confirm new PIN** fields and click the **Save** button.



This screenshot is identical to Figure 34, but the 'Change PIN' button is highlighted with a grey border, indicating it is the next step in the process. The rest of the interface, including the 'ON' toggle, the current PIN fields, and the 'Remember PIN' checkbox, remains the same.

Figure 35 - PIN settings - Change PIN

When the PIN has been changed successfully, the following screen is displayed:

Success!  
Your settings have been changed successfully

**PIN settings**

SIM OK

PIN remembered

**PIN protection**  ON  OFF

Change PIN

**Current PIN**

**Confirm current PIN**

**Remember PIN**

Save

Figure 36 - SIM security settings – PIN unlock successful

## Unlocking a PUK locked SIM

After three incorrect attempts at entering the PIN, the SIM card becomes PUK (Personal Unblocking Key) locked and you are requested to enter a PUK code to unlock it.

Oops, something went wrong...  
Your SIM is PUK locked now. Please enter the PUK code to unlock. You have 10 remaining attempt(s).

**PIN settings**

SIM is PUK locked

Change PIN

**Current PIN**

**Confirm current PIN**

**PUK**

**Confirm PUK**

**Remember PIN**

Save

*Figure 37 - SIM security - SIM PUK locked*



**Note** – To obtain the PUK unlock code, you must contact your service provider.

You will be issued a PUK to enable you to unlock the SIM and enter a new PIN. Enter the new PIN and PUK codes. Click the **Save** button when you have finished entering the new PIN and PUK codes.

## LAN

### LAN configuration

The LAN configuration page is used to configure the LAN settings of the antenna and to enable or disable DNS Masquerading. To access the LAN configuration page, click on the **Networking** menu at the top of the screen, then click on the **LAN** menu on the left.

*Figure 38 – LAN configuration settings*

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 reboot the antenna and enter the new IP address into your browser address bar.

## DNS masquerading

DNS masquerading allows the antenna to proxy DNS requests from LAN clients to dynamically assigned DNS servers. When enabled, clients on the antenna's LAN can then use the antenna as a DNS server without needing to know the dynamically assigned cellular network DNS servers.

The **DNS masquerading** toggle key is **OFF** by default.

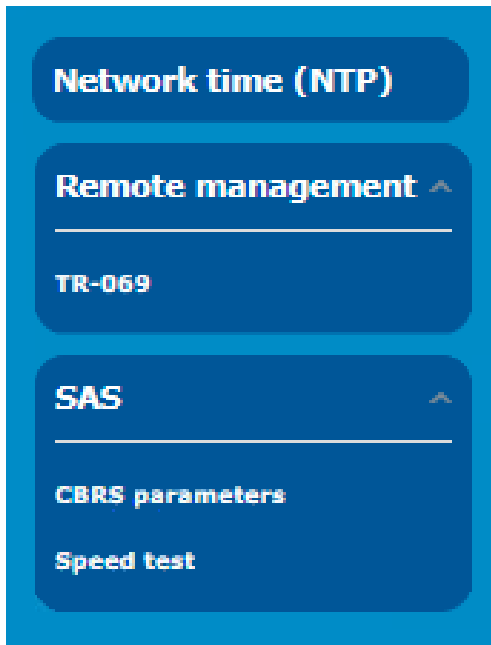
With DNS masquerading **OFF**, the DHCP server hands out the upstream DNS server IP addresses to downstream clients directly, so that downstream clients send DNS requests directly to the upstream DNS servers without being proxied by the CFW-2172 antenna.

With DNS masquerading **ON**, the DHCP server embedded in the CFW-2172 antenna hands out its own IP address (e.g. 192.168.0.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the CFW-2172 antenna which proxies them to the upstream DNS servers.

You may also override the DNS Masquerading option by specifying custom DNS Server IP addresses in the DHCP Server configuration mentioned in the next section of this guide. In this case the DHCP server assigns downstream devices the manually configured addresses and the DNS Masquerading option is ignored.

The **DNS masquerading** toggle key is **OFF** by default.

## Services



The **Services** tool group provides configuration options for features that support extended utilisation of your CFW-2172 and in the case of SAS access to 5G broadband channels in the United States.

Click the **Services** menu in the top tool bar to open its menu in the left margin.

**Network Time (NTP)** allows you to synchronize the CFW-2172 antenna's internal clock with a global Internet time server.

Use the **Speed test** to check your upload and download speeds using server locations and test files of your choice.

## Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the CFW-2172 antenna to synchronize its internal clock with a global Internet Time server and specify the time zone for the location of the antenna. 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 0.netcomm.pool.ntp.org.

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

Figure 39 - NTP settings

### Timezone settings

To configure time zone settings:

- 1 The **Current time** field shows the time and date configured on the antenna.
  - a If this is not accurate, use the **Time zone** drop-down list to select the correct time zone for the antenna.
  - b If the selected zone observes daylight savings time, a **Daylight savings time schedule** link appears below the drop-down list. Click the link to see the start and end times for daylight savings.
- 2 When you have selected the correct time zone, click the **Save** button to save the settings.

### NTP settings

To configure NTP settings:

- 1 Click the **Network time (NTP)** toggle key to switch it to the **ON** position.

- 2 In the **NTP service** field, enter the address of the NTP server you wish to use.
- 3 The **Synchronization on WWAN connection** toggle key enables or disables the antenna from performing a synchronization of the time each time a mobile broadband connection is established.
- 4 The **Daily synchronisation** toggle key enables or disables the antenna from performing a synchronization of the time each day.
- 5 When you have finished configuring NTP settings, click the **Save** button to save the settings.

## Remote management

### 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 antenna with the root account.

When a factory reset of the antenna is performed via TR-069, the TR-069 settings are preserved.

The NetComm Wireless antenna 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.

## TR-069 configuration

To access the TR-069 configuration page, click the **Services** menu item, then select the **TR-069** item from the **Remote Management** submenu on the left.

### TR-069 configuration

**Enable TR-069**  ON  OFF

**ACS URL**

**ACS username**

**ACS password**

**Verify ACS password**

**Connection request username**

**Connection request password**

**Verify connection request password**

**Enable periodic ACS informs**  ON  OFF

**Inform period**  (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** ntc\_ifwa631

**Description** NetComm NTC-IFWA631 Fixed Wireless 4G LTE Outdoor Unit

**ProductClass** IFWA631 Series

**SerialNumber** A6C9E5

Figure 40 - TR-069 configuration

To configure TR-069:

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

## SAS

**Citizens Broadband Radio Service (CBRS)** is a 150 MHz wide broadcast band of the 3.5 GHz band (3550 MHz to 3700 MHz) in the United States.

FCC has authorized the full use of the CBRS band for wireless service provider commercialization under a three-tiered spectrum authorization framework to accommodate a variety of commercial uses on a shared basis with incumbent federal and non-federal users. With this service, wireless carriers using CBRS are able to deploy 5G mobile networks without having to acquire spectrum licenses.

When devices such as your CFW-2172 want to use the CBRS band they put in a request to a cloud-based **Spectrum Access System (SAS)** to reserve unused General Authorized Access channels in a particular geographic area. If channels are free, SAS can grant the requests.

When devices with permission to use channels no longer require access, their unused authorization is put back into the pool that the SAS draws from to grant requests to other users with minimal interference.

## Speed Test

To see the CFW-2172's current upload and download speeds, open the **Services** menu, drop down the **SAS** submenu and select **Speed test**.

### Run speed test

If you have previously used the download and upload server details that are displayed on the page, click the **Run speed test** button to check the current speeds between the CFW-2172 and those respective servers.

The results will be displayed on this page, see below.

## Speed test settings

You can change the download and upload servers that you use to perform the test.

**Run speed test**

**FTP download server details**

Server IP address/domain name

User

Password

Remote file/path name

Local file name

**FTP upload server details**

Server IP address/domain name

User

Password

Local file name

Remote file/path name

Figure 41 – Speed test parameters

The following details can be entered for either the download and upload FTP servers:

Option	Description
<b>Server IP address/ domain name</b>	Enter the IP address or domain name that the FTP server is running on.
<b>User</b>	If an account is required, enter the username here, otherwise leave this blank.
<b>Password</b>	If an account is required, enter the password here, otherwise leave this blank.
<b>Remote file/path name</b>	On the <b>FTP download server</b> – Enter the path to the file you want to download on the remote server.

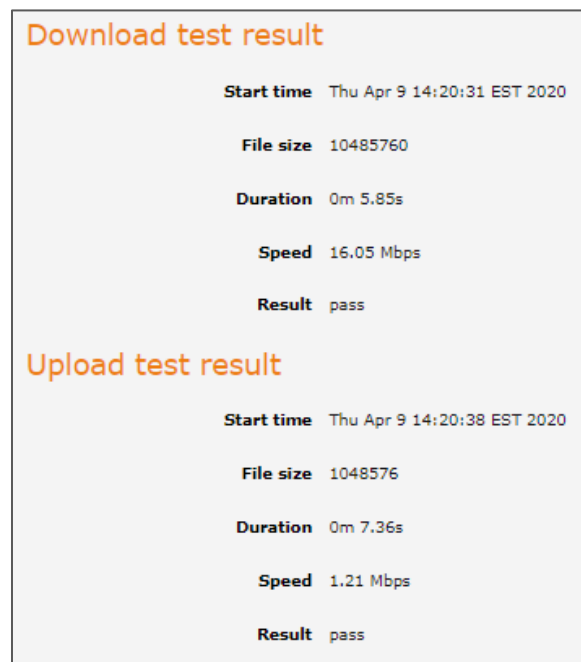
	On the <b>FTP upload server</b> – Enter the path to the file you are uploading to the remote server.
<b>Local file name</b>	On the <b>FTP download server</b> – Enter a name to save the file as on the local device. On the <b>FTP upload server</b> – Enter a name to save the file as on the remote server.
<b>Save button</b>	Click to save the changes you have made. To apply the new details to a new test, click the <b>Run speed test</b> button.

*Table 7 - Speed test parameter details*

## Test results

Click the **Run speed test** button to check the current speeds between the CFW-2172 and the download and upload servers.

A list of results will appear on the page:



*Figure 42 – Speed Test results display*

The following detailed results will be provided for both the download and upload tests:

Option	Description
<b>Start time</b>	The date and exact time the download or upload part of the speed test began.
<b>File size</b>	The size of the file used to measure the speed.
<b>Duration</b>	Time in seconds taken to successfully transfer the full file.
<b>Speed</b>	The download or upload speed in Megabits per second (Mbps)

**Result**

The following results are possible:

**Pass** – Signifies that the test was carried out and the file was fully transferred without errors.

**Fail** – Indicates that the test did not complete correctly.

*Table 8 – Speed Test results details*

If the **Smart Antenna tool** is connected to the CFW-2172 you cannot connect to these setting through this interface.



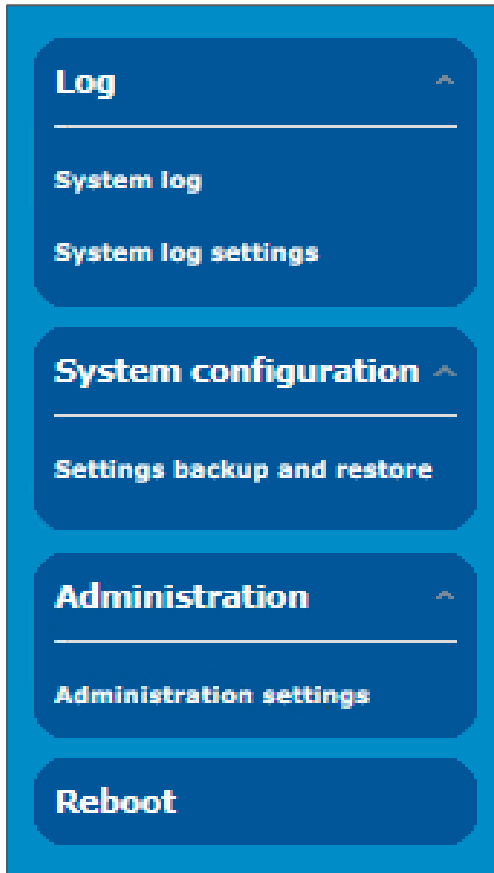
**Important** –

**Speed test is disabled**

Please open a web browser at the connected install tool.

You must either disconnect the **Smart Antenna tool** or run the **Speed test** via the **Smart Antenna** tool's web interface.

# System



The **System** tool group provides configuration options for general maintenance and management of your network connections.

Click the **System** menu in the top tool bar to open its menu in the left margin.

**Log** allows you to customise log reports and save them to remote locations or recipients.

**System Configuration** allows you to restore the factory default settings.

**Administration** allows you to set new passwords and other access settings as well as manage your other security settings.

**Reboot** allows you to reboot the CFW-2172.

## Log

The Log pages are used to display or download the System log on the CBRs Survey UE.

## System log

The **System Log** enables you to troubleshoot any issues you may be experiencing with your CBRS Survey UE.

To display the details currently in the log, open the **System** menu, drop down the **Log** submenu and select **System log**:

Date & Time	Machine	Level	Process	Message
Apr 6 06:02:54	ntc_ifwa661	daemon.err	wmcmd[3533]	failed to post QMI QMI_NAS_PERFORM_NETWORK_SCAN
Apr 6 06:02:54	ntc_ifwa661	user.warn	kernel	[ 1518.553581] NOHZ: local_softirq_pending 08
Apr 6 06:00:54	ntc_ifwa661	user.warn	kernel	[ 1398.108143] NOHZ: local_softirq_pending 08
Apr 6 05:54:53	ntc_ifwa661	user.warn	kernel	[ 1037.309566] NOHZ: local_softirq_pending 08
Apr 6 05:54:53	ntc_ifwa661	user.warn	kernel	[ 1037.268855] NOHZ: local_softirq_pending 08
Apr 6 05:48:52	ntc_ifwa661	user.warn	kernel	[ 676.498923] NOHZ: local_softirq_pending 08
Apr 6 05:48:52	ntc_ifwa661	user.warn	kernel	[ 676.437411] NOHZ: local_softirq_pending 08
Apr 6 05:46:51	ntc_ifwa661	user.warn	kernel	[ 555.643267] NOHZ: local_softirq_pending 08
Apr 6 05:42:51	ntc_ifwa661	user.warn	kernel	[ 314.935491] NOHZ: local_softirq_pending 08
Apr 6 05:42:51	ntc_ifwa661	user.warn	kernel	[ 314.892968] NOHZ: local_softirq_pending 08
Apr 6 05:39:36	ntc_ifwa661	user.warn	kernel	[ 120.117792] QTI:Enable mobileap
Apr 6 05:39:36	ntc_ifwa661	user.warn	kernel	[ 120.111202] QTI:Processing LTNK_UP
Apr 6 05:38:50	ntc_ifwa661	user.notice	flush_conntrack _cache	*****
Apr 6 05:38:50	ntc_ifwa661	user.notice	flush_conntrack _cache	done
Apr 6 05:38:50	ntc_ifwa661	user.notice	flush_conntrack _cache	flushing [ conntrack_cache ]...
Apr 6 05:38:50	ntc_ifwa661	user.notice	flush_conntrack _cache	flushing [ ip route ]...

If the table is empty, select the **Display level** required and click the **Download** button.

Figure 43 - System log file

## Log file

Use the **Display level** drop-down list to select a message level to be displayed. The message levels are described in the table below.

Item	Definition
<b>Debug</b>	Show extended system log messages with full debugging level details.
<b>Info</b>	Show informational messages only.

<b>Notice</b>	Show normal system logging information.
<b>Warning</b>	Show warning messages only.
<b>Error</b>	Show error condition messages only.

*Table 9 - System log display levels*

To download the System log for offline viewing, right-click the **Download** button and choose **Save as..** to save the file.

The downloaded log file is in Linux text format with carriage return (CR) only at the end of a line, therefore in order to be displayed correctly with new lines shown, it is recommended to use a text file viewer which displays this format correctly (e.g. Notepad++).

To clear the system log display, click the **Clear** button.

## System log settings

To access the System log settings page, click the **Services** menu item, open the **Log** submenu on the left and then select **System log settings**.

*Figure 44 - 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, for example, if this is set to a low level, such as "Error", the System log will not be able to display higher log levels.

Item	Definition
<b>Debug</b>	Show extended system log messages with full debugging level details.
<b>Info</b>	Show informational messages only.

<b>Notice</b>	Show normal system logging information.
<b>Warning</b>	Show warning messages only.
<b>Error</b>	Show error condition messages only.

*Table 10 - System log capture levels*

## Non-volatile log

When the CBRS Survey UE is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the CBRS Survey UE. You can specify the size of the logging data. Up to 10,000 KB (10 MB) of log data will be stored before it is overwritten by new log data. Flash memory has a finite number of program-erase operations that it may perform to the blocks of memory. While this number of program-erase operations is quite large, we recommend that you do not enable this option for anything other than debugging to avoid excessive wear on the memory.

## Remote syslog server

The CBRS Survey UE 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 CBRS Survey UE to output log data to a remote syslog server:

- 1 Click the **System** menu from the top menu bar, open the **Log** submenu on the left and then select **System log settings**.
- 2 Under the **Remote syslog server** section, enter the **IP address** or **hostname** of the syslog server in the **IP / Hostname [PORT]** field. 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 CBRS Survey UE will use the default UDP port 514.
- 3 Click the **Save** button to save the configuration.

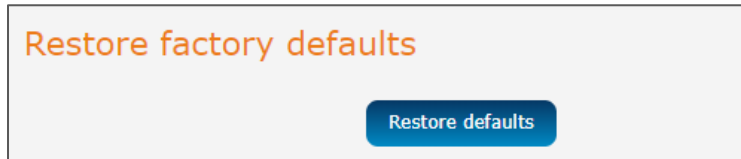
*Figure 45 – Remote syslog server configuration*

## System Configuration

Users can restore the antenna's configuration to its factory default settings.



To access the **Restore factory defaults** page, click on the **System** menu item then select the **System configuration** menu on the left and finally select **Settings backup and restore** beneath it.



*Figure 46 – Restore factory defaults button*

Click the **Restore defaults** button to restore the factory default configuration. The antenna asks you to confirm that you wish to restore factory default settings. If you wish to continue with the restoring of factory defaults, click **OK**.



**Note** – All current settings on the antenna will be lost when performing a restore of factory default settings.

## Administration

Enable or disable local Secure Shell on the antenna. The default setting is disabled.

### Administration settings

To access the Administration Settings page, click on the **System** menu then the **Administration** menu on the left and then click on **Administration settings**.

The Administration settings page is used to enable or disable protocols used for remote access and configure the passwords for the user accounts used to log in to the antenna.

The page is divided into four sections:

- Remote router access control
- Local router access control
- Web User Interface account
- Telnet/SSH account

The screenshot displays the Administration settings page with the following sections:

- Remote router access control:** Five toggle switches for Enable HTTP, Enable HTTPS, Enable telnet, Enable SSH, and Enable ping, all currently set to OFF.
- Local router access control:** Four toggle switches for Enable HTTP, Enable HTTPS (set to ON), Enable local Telnet, and Enable local SSH, all currently set to OFF.
- Web User Interface account:**
  - Username: dropdown menu showing 'root'.
  - Password: text input field (8-128 characters in length).
  - Confirm password: text input field (8-128 characters in length).
  - Password strength: indicator.
  - Login attempt limit: text input field (3) (3-5).
  - Login lock duration: text input field (1) (1-10 minutes).
  - Session timeout: text input field (1800) (300-3600 seconds).
- Telnet/SSH account:**
  - Username: text input field showing 'root'.
  - Password: text input field (8-126 characters in length).
  - Confirm password: text input field (8-126 characters in length).
  - Password strength: indicator.

A blue 'Save' button is located at the bottom of the form.

Figure 47 - Administration page

Option

Definition

### Remote router access control

Note that all remote router access control settings are disabled by default. <input type="checkbox"/> 0	
Enable HTTP	Enable or disable remote HTTP access to the antenna.
HTTP management port	<p>When HTTP is enabled (see previous) you can set the HTTP management port.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p>Enable HTTP <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <p>HTTP management port <input type="text" value="8080"/> (Choose a port between 1 and 65534)</p> </div> <p>Enter a port number between 1 and 65534 to use when accessing the antenna remotely.</p>
Enable SSH	Enable or disable Secure Shell on the antenna.
Remote SSH Access Port	<p>When SSH is enabled (see previous) you can set the remote SSH access port.</p> <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 10px auto;"> <p>Enable SSH <input checked="" type="checkbox"/> ON <input type="checkbox"/> OFF</p> <p>Remote SSH access port <input type="text" value="22"/> (Choose a port between 1 and 65534)</p> </div> <p>Enter the port number for remote SSH access. The port number must be between 1 and 65534.</p>
Enable Ping	Enable or disable remote ping responses on the WWAN connection.
<b>Local router access control</b>	
Enable HTTP	Enable or disable local HTTP access to the antenna. The default setting is disabled.
Enable HTTPS	Enable or disable local secure HTTP access (https). The default setting is enabled.
Enable local Telnet	Enable or disable local telnet (command line) access to the antenna. The default setting is disabled.
Enable local SSH	Enable or disable local Secure Shell on the antenna. The default setting is disabled.
<b>Web User Interface account</b>	
Username	Use the drop-down list to select the root or user account to change its web user interface password.
Password	<p>Enter the desired web user interface password.</p> <p>When logged in with the root account the password will display in clear text, otherwise the password is masked. Only the root account can view and change passwords.</p>
Password strength	<p>The CBRS Survey UE includes algorithms to ensure that the password you enter is strong.</p> <p>Any password configured on the router must now meet the following criteria:</p> <ul style="list-style-type: none"> <li>• Be a minimum of eight characters and no more than 128 characters in length.</li> <li>• Contain at least one upper case, one lower case character and one number.</li> <li>• Contain at least one special character, such as:  <code>~!@#\$\$%^&amp;*()-_+=+[]\ ;:","&lt;.&gt;/?.</code> </li> </ul> <p>Additionally, the password must also satisfy an algorithm which analyses the characters as you type them, searching for commonly used patterns, passwords,</p>

	names and surnames according to US census data, popular English words from Wikipedia and US television and movies and other common patterns such as dates, repeated characters (aaa), sequences (abcd), keyboard patterns (qwertyuiop) and substitution of numbers for letters.
Login attempt limit	Set the number of unsuccessful log in attempts that are allowed before the login lock applies (see next item). You can choose 3, 4 or 5 login attempts. The default is 3.
Login lock duration	Set the time users must wait before they can attempt to login after reaching the login attempt limit, see previous item above. The duration can be set from one minute to ten minutes. The default is one minute.
Session timeout	Set the time in seconds that the system must remain idle before it automatically logs out. 1800 seconds (30 minutes) is the default. You can choose a time between 300 seconds (5 minutes) and 3600 seconds (one hour).
<b>Telnet/SSH account</b>	
Username	Displays the Telnet/SSH.username. This may not be changed.
Password	Enter the desired Telnet/SSH password.
Confirm password	Re-enter the desired Telnet/SSH password.

*Table 11 - Administration configuration options*

## Accessing the antenna configuration pages remotely

To access the antenna's configuration pages remotely:

- 1 Open a new browser window and navigate to the WAN IP address and assigned port number of the antenna, for example <http://123.209.130.249:8080>



**Note** – You can find the antenna's WAN IP address by clicking on the "Status" menu. The WWAN IP field in the WWAN Connection Status section shows the antenna's WAN IP address.

- 2 Enter the username and password to login to the antenna and click **Log in**.



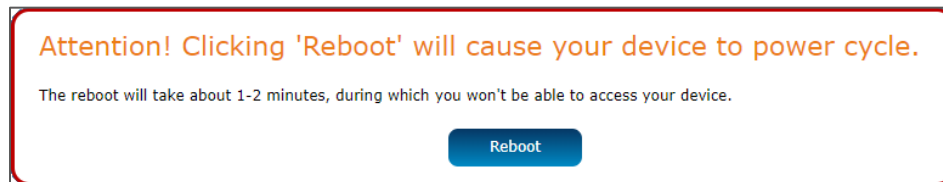
**Note** – To perform functions like Firmware upgrade, device configuration backup and to restore and reset the antenna to factory defaults, you must be logged in with the root manager account.

## Reboot

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

To reboot the antenna:

- 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 antenna displays a warning that you are about to perform a reboot and that the reboot will take about 1-2 minutes during which you won't be able to access your device.




*Figure 48 - Reboot confirmation*

If you wish to proceed, click the **Reboot** button to continue with the reboot process.



**Note** – It can take up to 2 minutes for the antenna to reboot.

## Logging out

To log out of the antenna's web management console, click the  icon at the top right corner of the web user interface.

## Appendix A – Default Settings

The following tables list the default settings of the CBRS Survey UE.

### LAN (Management)

IP Address	192.168.1.1
Subnet Mask:	255.255.255.0

*Table 12 - LAN Management Default Settings*

## Appendix B – 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.

### 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 must not cause harmful interference, and (2) this device must accept any interference received, including interference that will 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.

## Company details

### **Casa Systems, Inc.**

100 Old River Road, Andover, Massachusetts 01810 USA

[www.netcomm.com/contact](http://www.netcomm.com/contact)

## Product details

Product: CBRS Survey UE

Model No: CFW-2172