casa systems

User Guide

CFW-2182 CBRS 4G Outdoor UE

Doc No. UG01233

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-2182 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-2182 CBRS 4G Outdoor UE antenna

Ver.	Document description	Date
v1.0	First release	May 14, 2020
v1.1	Change in FCC Statement	August 7, 2020
v1.2	Changes in RF Exposure section	August 13, 2020

Table i. – Document revision history

© Casa Systems 2020

Contents

Overview 6

Introduction 6
Target audience 6
Prerequisites 6
Notation 6

Product introduction 7

Product overview 7
Package contents 7

Physical dimensions and interfaces 8

Physical dimensions 8
Interfaces 9
Insert SIM card 10
Assemble and attach the mounting bracket 13
Overview of completed mounting 13
Mounting bracket assembly instructions 14
Power the CFW 16
R45 cable weather seal assembly 16
PoE-03 power supply 20
PoE-03 LED indicators 20

Installation 21

Typical CFW antenna installation 21

CFW-2182 configuration interface 22

Normal configuration 22
Advanced configuration 22
Log in 22
Confirm successful connection 23

Status 24

Configuration tool menus 28

Networking 29

Wireless WAN 30
Data connection 30
Manually configuring a connection profile 31
Confirming a successful connection 33
Checking data usage 33
Operator settings 35

© Casa Systems 2020

Operator settings 35
SIM security settings 36
Unlocking a PIN locked SIM 36
Enabling/Disabling SIM PIN protection 38
Changing the SIM PIN code 39
Unlocking a PUK locked SIM 40
LAN 41
LAN configuration 41
DNS masquerading 41

Services 43

Network time (NTP) 44
Timezone settings 44
NTP settings 45
Remote management 45
TR-069 45
TR-069 configuration 46
SAS 48
CBRS Registration Status 48
Speed Test 48
Run speed test 48
Speed test settings 49
Test results 50

System 52

Log 53
System log 53
Log file 54
System log settings 54
Log capture level 55
Non-volatile log 55
Remote syslog server 55
System Configuration 56
Administration 57
Administration settings 57
Accessing the antenna configuration pages remotely 59
Reboot 60

Logging out 60

© Casa Systems 2020

Appendix A – Default Settings 61

Appendix B – Safety and compliance 62

RF Exposure 62
FCC Statement 62
FCC compliance 62
FCC regulations 62
Company details 63
Product details 63

© Casa Systems 2020

Overview

Introduction

This document provides all the information required to configure and deploy the Casa Systems CFW-2182 antenna.

This User Guide relates to the CFW-2182's physical components and its web user interface.

Normally only the installing technician would require access to the CFW-2182'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**, see Figure 3. 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 continuing with the installation of the CFW-2182 antenna please confirm that you have:

- A WiFi-enabled device (laptop, tablet or 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.

© Casa Systems 2020

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 optimise signal strength in weak signal areas, the CFW-2182 CBRS 4G Outdoor UE is positioned on the exterior of the premises to overcome distance limitations and geographical obstructions and deliver high-speed LTE broadband connectivity to wired and wireless clients in the property via an indoor router.

Package contents

The CFW-2182 in-box contents include:

- 1 x CFW-2182 Casa Fixed Wireless antenna
- 1 x Mounting bracket

Accessories used in this solution (packaged separately):

- 1 x Antenna Power Supply (POE-03) – used to power the CFW-2182 during normal operation

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

© Casa Systems 2020

Physical dimensions and interfaces

Physical dimensions

Below is a list of the physical dimensions of the CFW-2182.

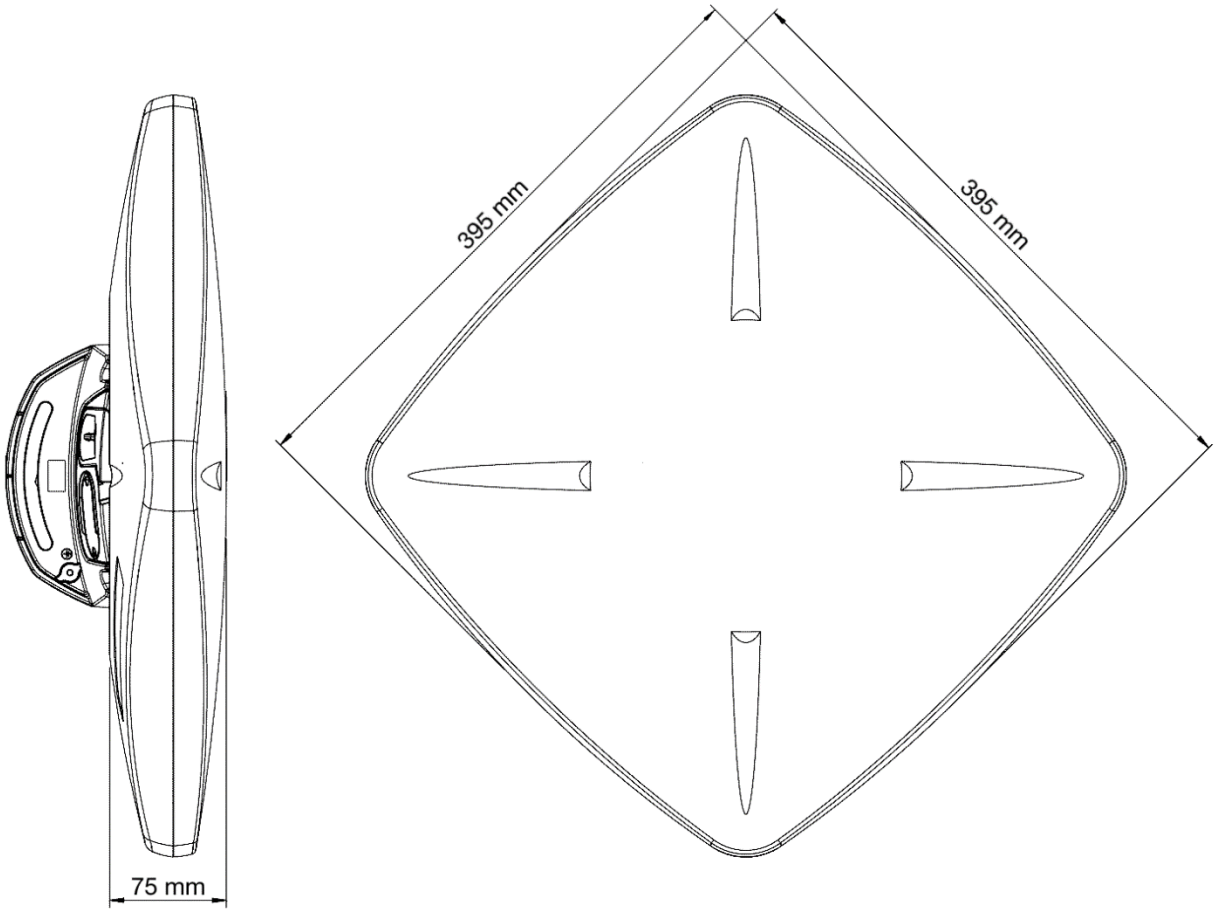


Figure 1 – CFW-2182 Dimensions

CFW-2182 Dimensions	
Length	15 ½" (395 mm)
Width	15 ½" (395 mm)
Height	4 ½" (75 mm)
Weight	~5.7lbs (~2.6 kg)

Table 1 - Device Dimensions

© Casa Systems 2020

Interfaces

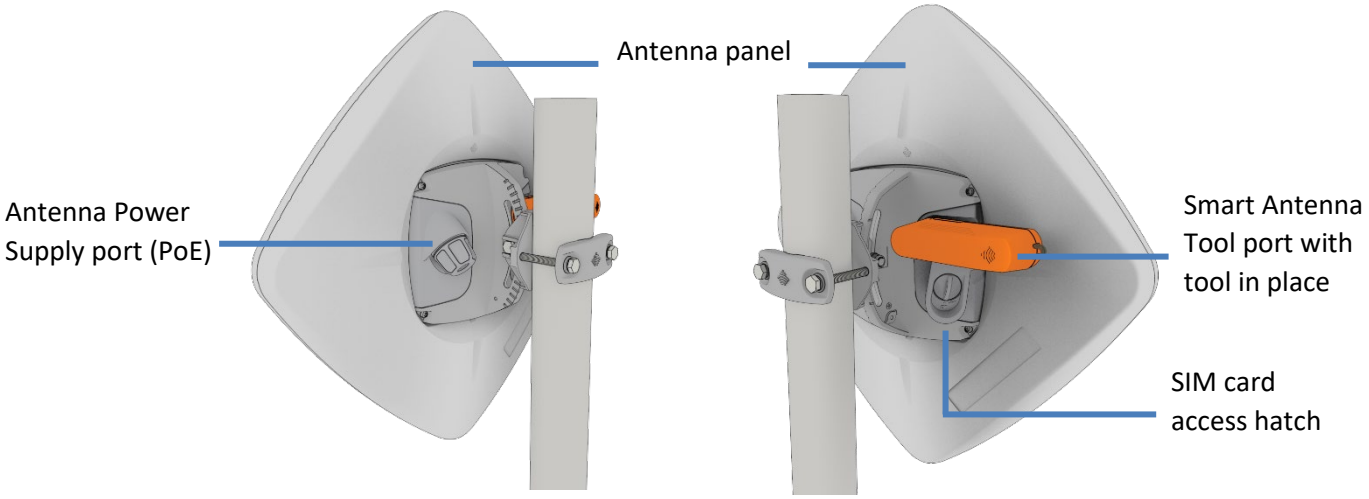


Figure 2 – Interfaces

Item	Description
Antenna panel	Includes 2 x 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-2182 with Ethernet cable

Table 2 – Interfaces

© Casa Systems 2020

Insert SIM card

The CFW-2182 accepts SIM cards in Mini-SIM (3FF) format. Follow the instructions below to insert a SIM card.

1 On the back of the CFW-2182 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

© Casa Systems 2020

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

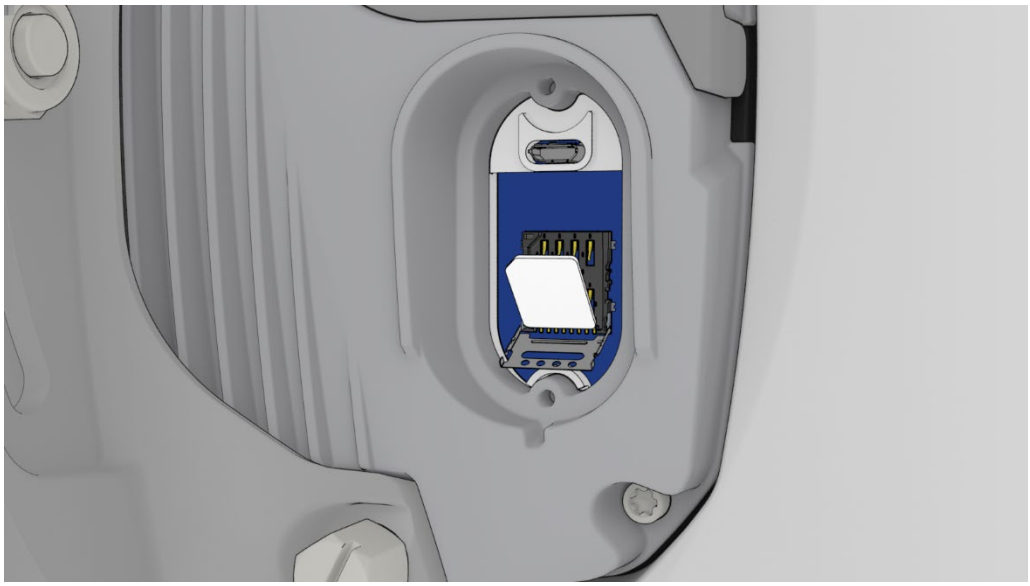


Figure 5 – Placing the SIM card onto the SIM card reader

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

© Casa Systems 2020

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

© Casa Systems 2020

Assemble and attach the mounting bracket

Overview of completed mounting

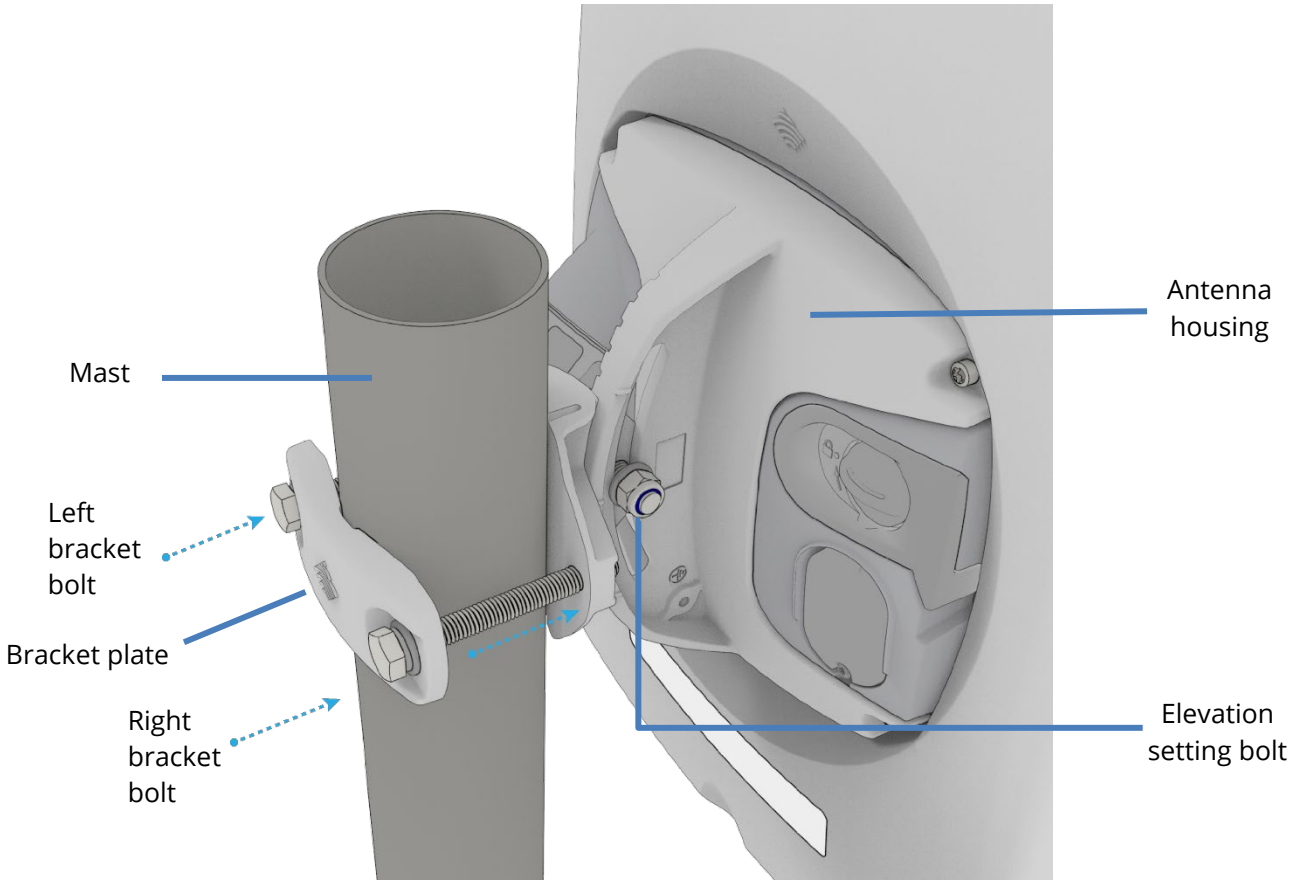


Figure 8 - CFW-2182 mounting bracket and bolts

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

© Casa Systems 2020

Mounting bracket assembly instructions

1 Place the pipe bracket onto the radome mount bracket as shown below.

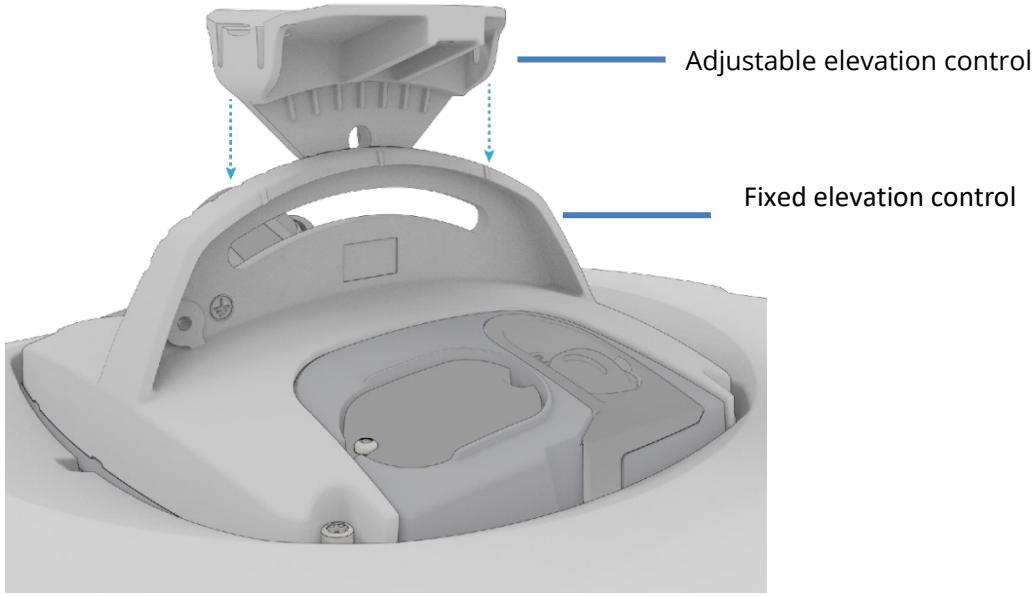


Figure 9 – Elevation control components

2 Insert the pivot bolt into the pipe clamp, then place the washer and nut over the pivot bolt as shown below.

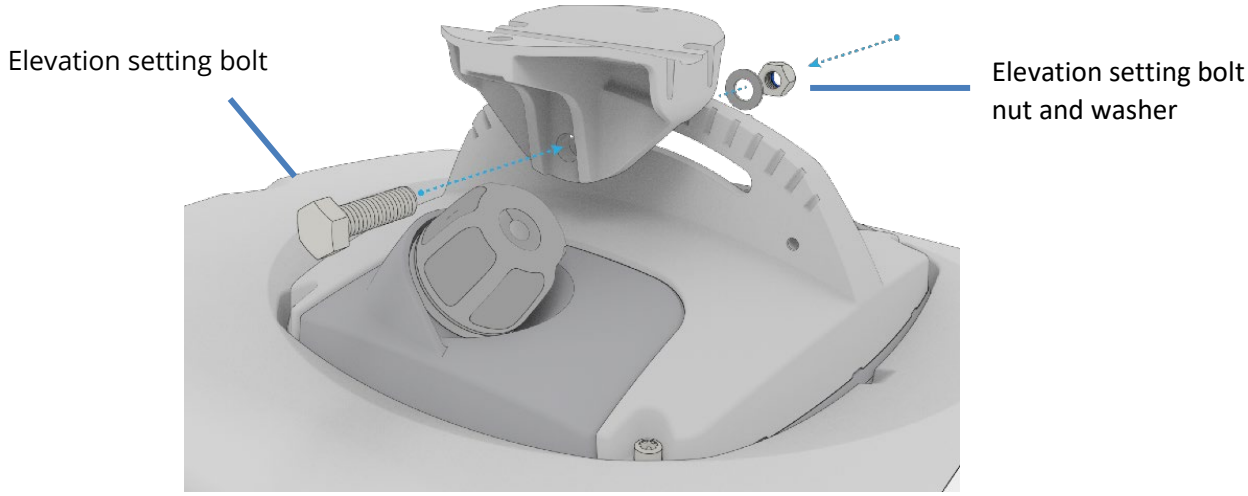


Figure 10 - Attaching the mounting bracket to the CFW-2182 CBRS 4G Outdoor UE

© Casa Systems 2020

3 Tighten the lock nut so that the pipe bracket and radome mount do not swivel easily. Do not overtighten the pivot bolt as some adjustment may be required later.

Figure 11 - Assembling pipe bracket to pole

4 Alternately tighten the top and bottom pipe clamp bolts to maintain even pressure on the pipe, to 80 in-lb.

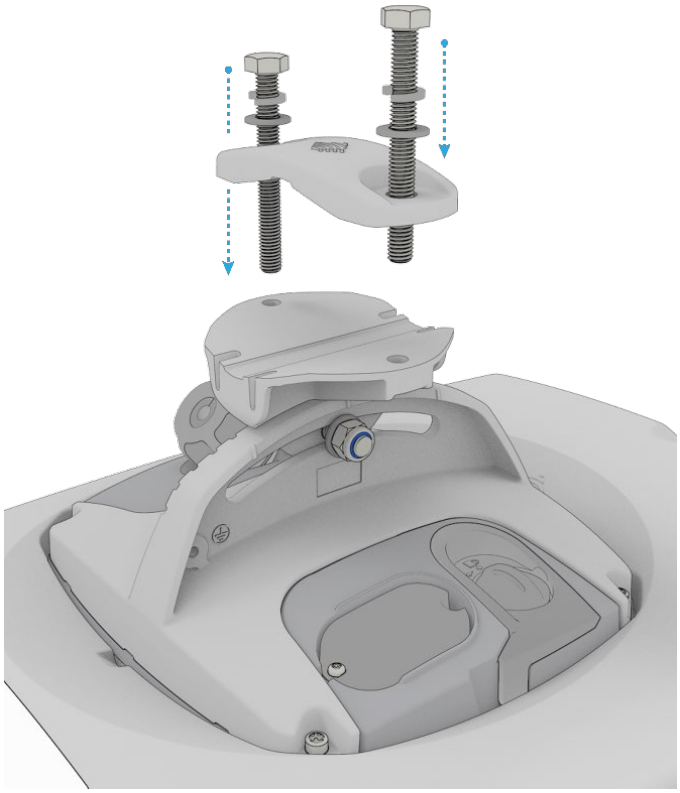


Figure 12 - Tightening pipe clamp bolts

© Casa Systems 2020

Power the CFW

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 CFW.

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

R45 cable weather seal assembly

The CFW-2182 antenna's power supply weather seal must be properly attached to prevent dust and water from entering the CFW-2182'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.

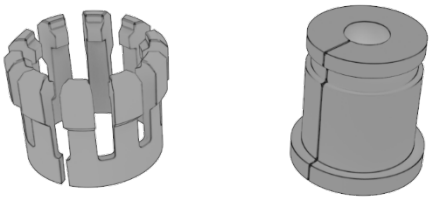


Figure 13 - Rubber seal and ferrule

3 Twist the neck for the seal counter-clockwise to remove it from the CFW-2182 housing. You should now have 5 pieces of the weather seal.

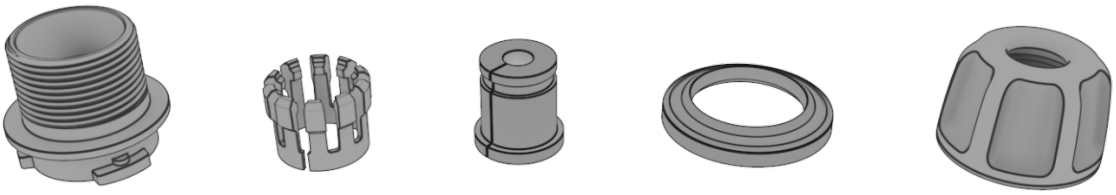


Figure 14 - Weather seal in five parts

© Casa Systems 2020

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

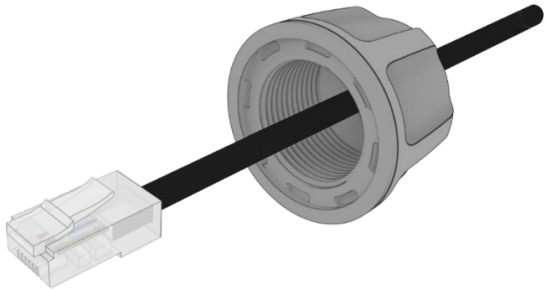


Figure 15 - Nut placed over Ethernet cable

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

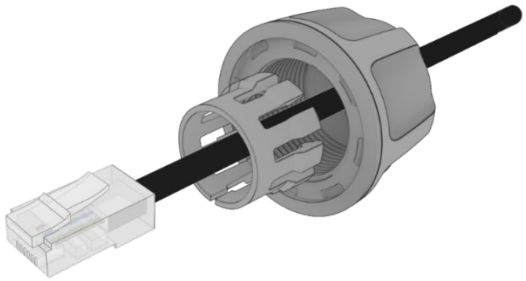


Figure 16 - Ferrule placed over Ethernet cable

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.

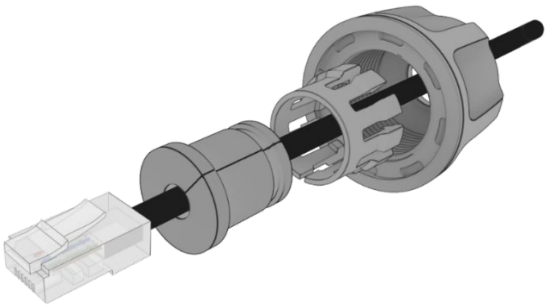


Figure 17 - Rubber seal placed over Ethernet cable

© Casa Systems 2020

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

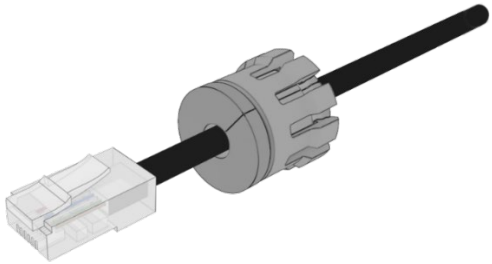


Figure 18 - Ferrule placed over rubber seal

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.

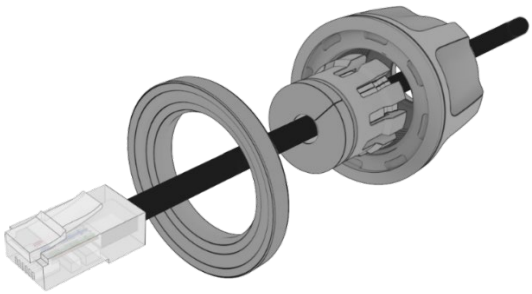


Figure 19 - Washer seal placed over Ethernet cable

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

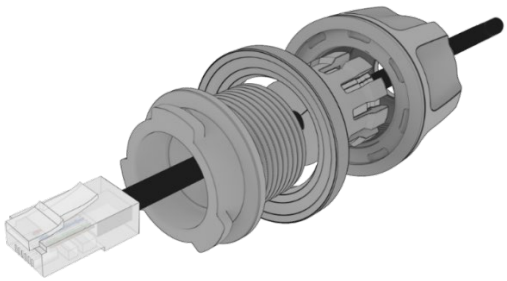


Figure 20 - Neck placed over Ethernet cable

© Casa Systems 2020

10 Plug the Ethernet cable into the Ethernet port.

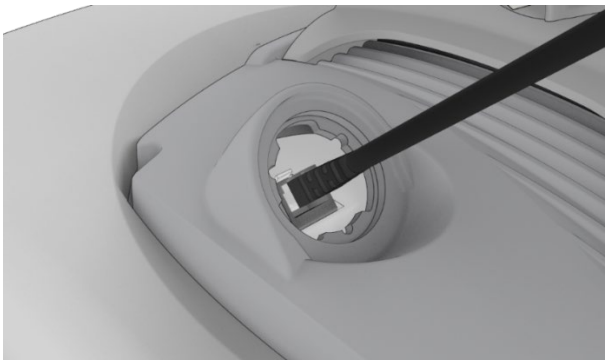


Figure 21 - Plugging in the Ethernet cable

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.

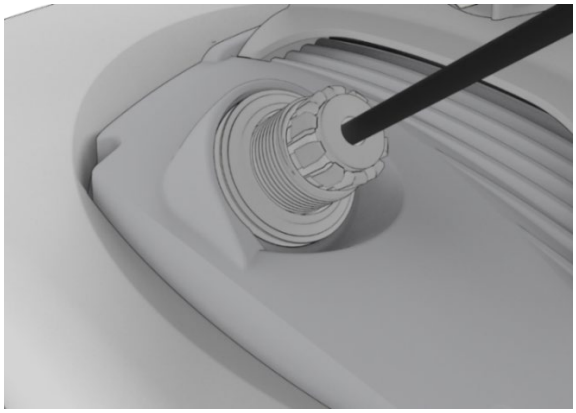


Figure 22 - Rubber seal and ferrule inserted into neck

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.

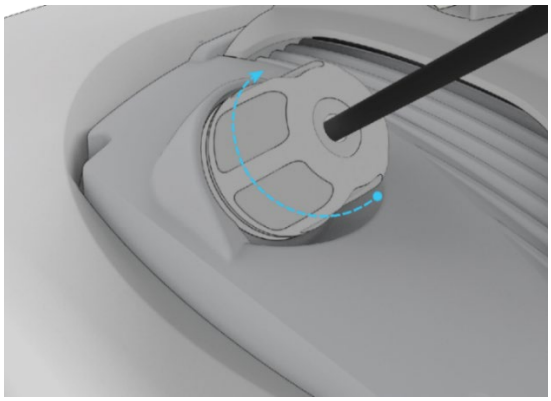


Figure 23 - Turning the nut clockwise

© Casa Systems 2020

PoE-03 power supply

Use the PoE-03 power supply to power your CFW-2182:

1. Connect the Antenna Power Supply (POE-03) to a dedicated AC power outlet away from running water, steam and excessive heat.
   a. 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 CFW 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 CFW.

Table 3 - POE-02 LED indicators

© Casa Systems 2020

Installation

The positioning and installation of the CFW-2182 antenna is achieved by a trained technician using the Casa Systems Smart Antenna Tool.

Details about the Smart Antenna Tool and the complete CFW-2182 installation process are fully described in the **CFW-2182 Installation Guide** (doc no IG1225).

Typical CFW antenna installation

The image below illustrates a typical installation of the CFW-2182 CBRS 4G Outdoor UE on the side of a building.

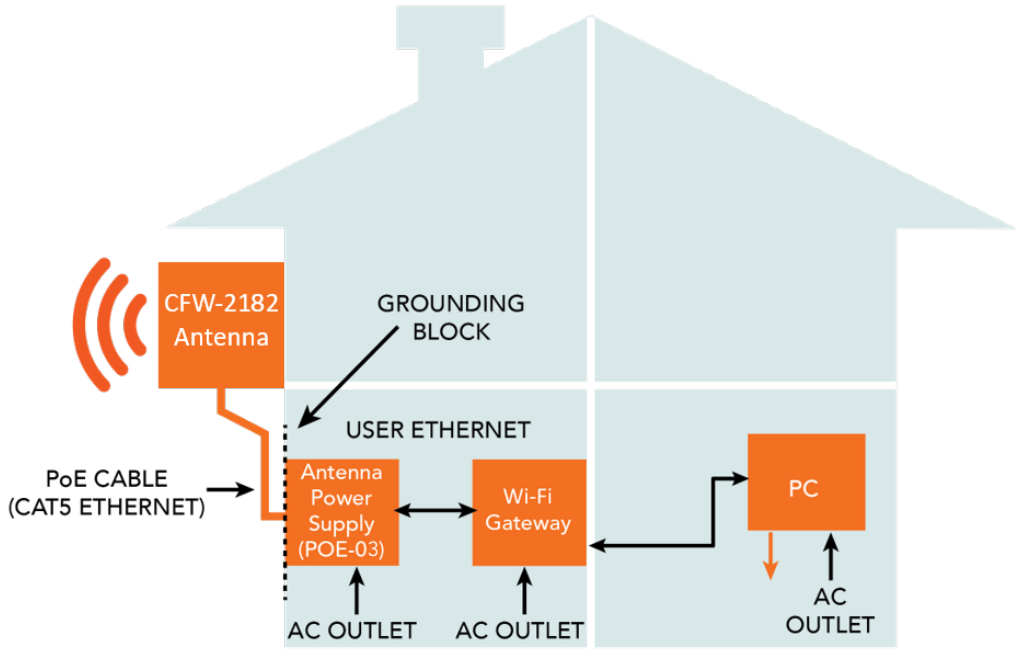


Figure 24 – Typical CFW-2182 CBRS 4G Outdoor UE Installation

Note that this User Guide relates to the CFW-2182's physical components and its web user interface.

Normally only the installing technician would require access to the CFW-2182'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.

© Casa Systems 2020

CFW-2182 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 CFW-2182.

Advanced configuration

For advanced configuration, log in to the web-based user interface of the CFW-2182.

A full suite of settings is available to customise the configuration of your wireless network connection.

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.

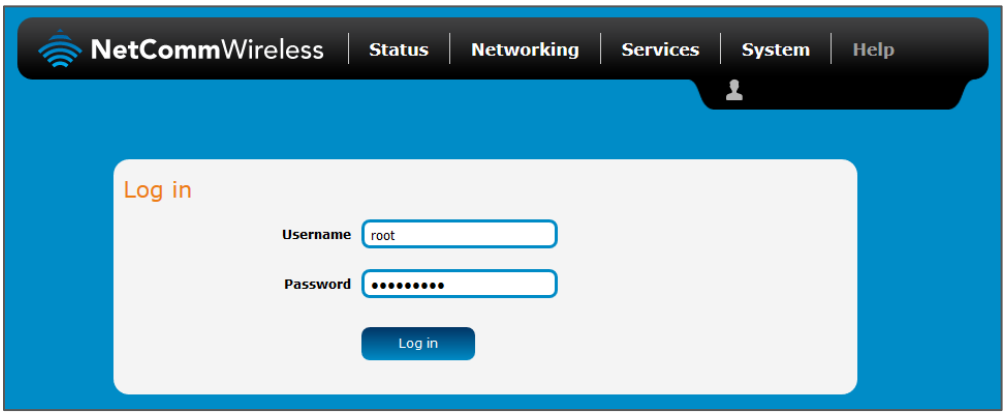


Figure 25 – Log in prompt for the web-based user interface

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

Admin manager account	
Username	root
Password	*****

Table 4 - Management account login details – Admin manager

© Casa Systems 2020

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.

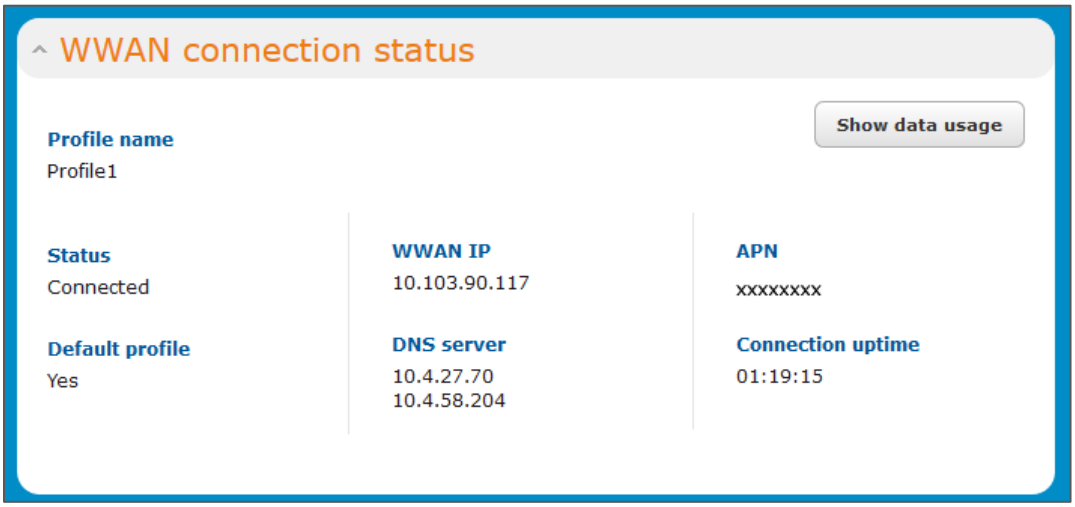


Figure 26 - WWAN connection status section

© Casa Systems 2020

Status

The **Status** page of the web interface provides system related information and is displayed when you initially log in to the CFW-2182 management console.

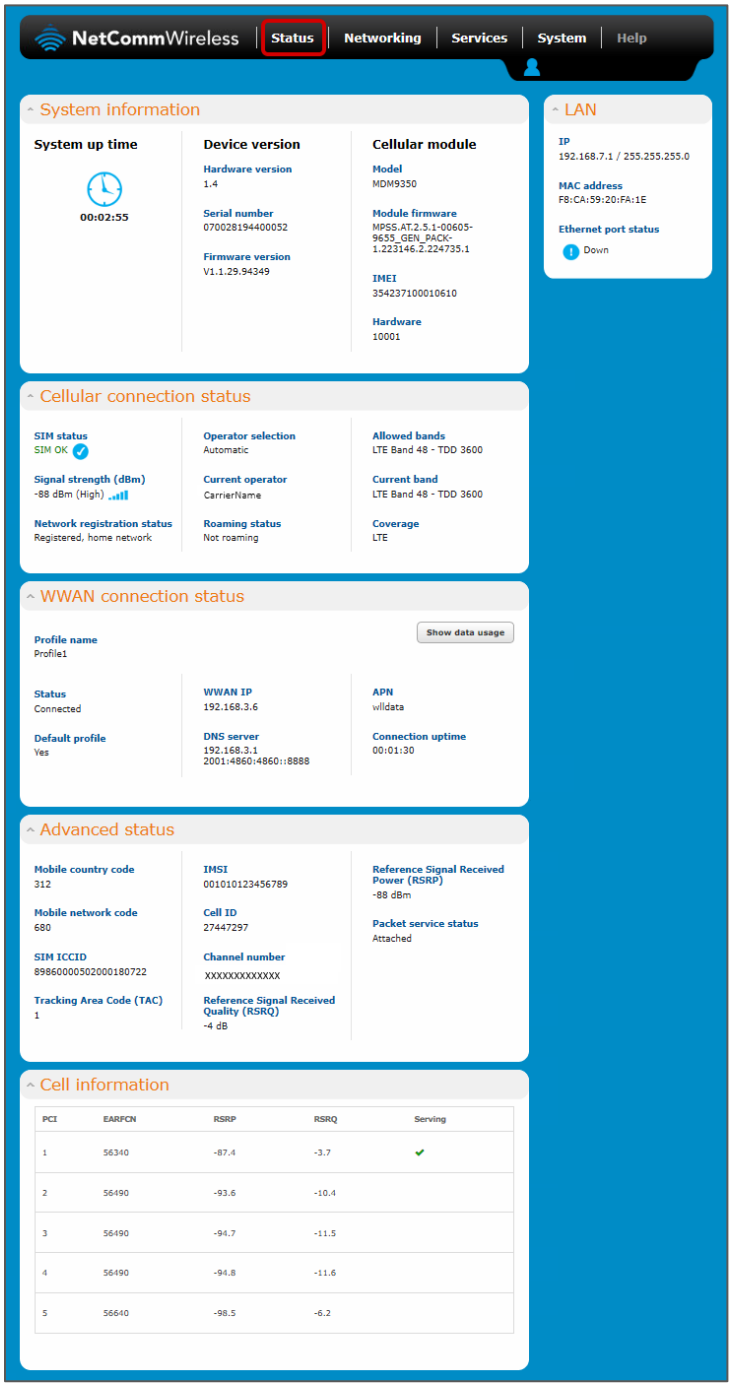


Figure 27 – Status page

© Casa Systems 2020

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
System information	
System up time	The current uptime of the CFW.
Hardware version	The hardware version of the CFW.
Serial Number	The serial number of the CFW.
Firmware version	The firmware version of the CFW
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.
LAN	
IP	The IP address and subnet mask of the CFW.
MAC address	The MAC address of the CFW.
Ethernet port status	Displays the current status of the Ethernet port and its operating speed.
Cellular connection status	
SIM Status	Displays the activation status of the CFW on the carrier network.
Signal strength (dBm)	The current signal strength measured in dBm
Network registration status	The status of the CFW'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 CFW.
Allowed bands	The bands to which the CFW may connect.
Current band	The current band being used by the CFW.
Coverage	The type of mobile coverage being received by the CFW.

© Casa Systems 2020

Item	Definition
WWAN connection status	
Profile name	The name of the currently active profile.
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.
Advanced status	
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 CFW, 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 x 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 **Attached** or **Detached**. When APN or username/password is changed, the device detaches and reattaches to the network.
Cell Information	
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.

© Casa Systems 2020

Item	Definition
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 x RSRP / RSSI where N is the number of Physical Resources Blocks (PRBs) over which the RSSI is measured.
Serving	A ✓ green check mark indicates that the cell location is currently functioning.

Table 5 - Status page item details

© Casa Systems 2020

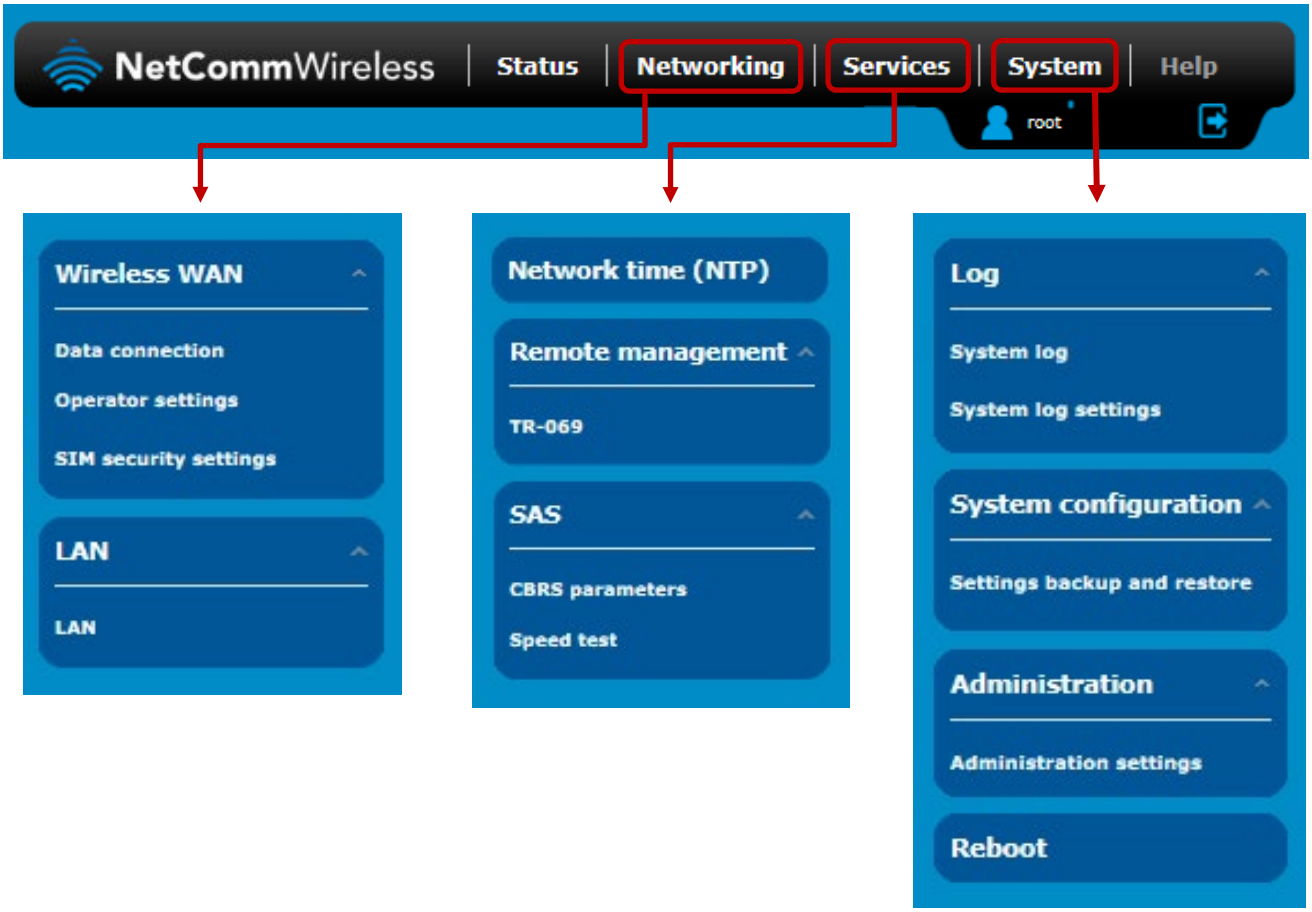
Configuration tool menus

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 **V** 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.

© Casa Systems 2020

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.

© Casa Systems 2020

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.

The is only one profile defined for the CFW-2182.

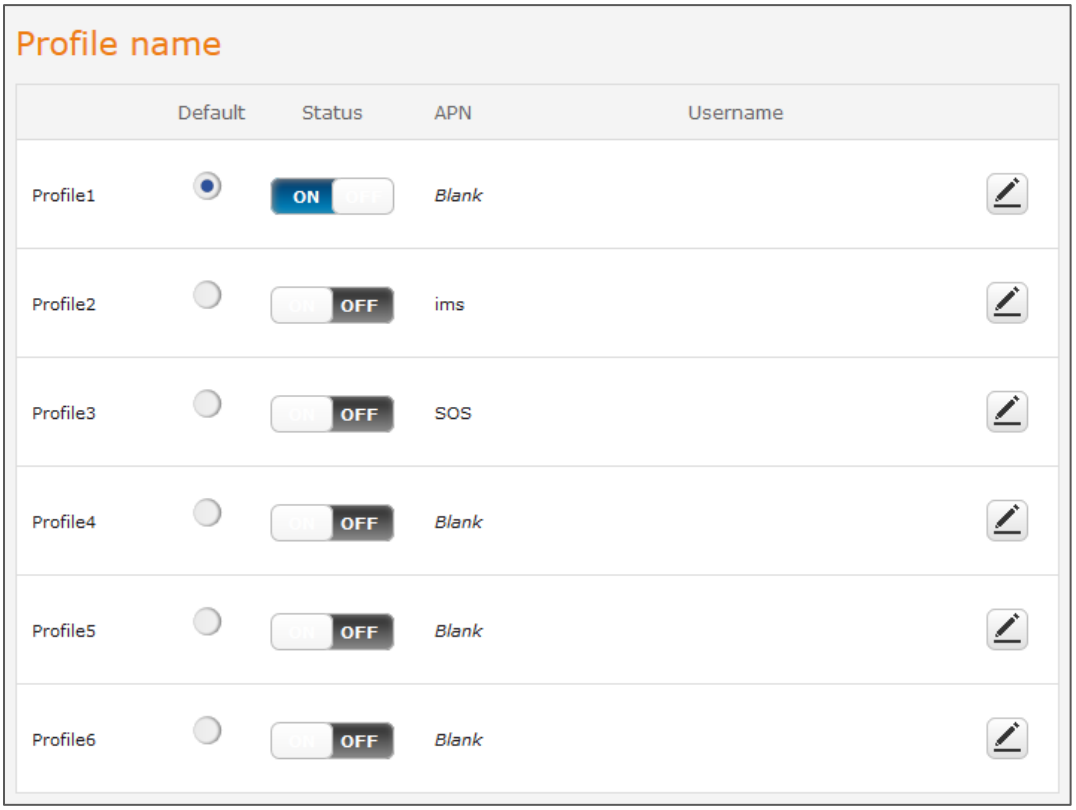


Figure 28 – Data connection settings

Item	Definition
Profile name	System reference name, cannot be changed by user.
Default	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.

© Casa Systems 2020

Status	Toggles the corresponding profile **ON** or **OFF**. Only one profile may be turned on at any time.
APN	The Access Point Name assigned to the corresponding profile.
Username	The username used to log on to the corresponding APN.
Save button	Click the **Save** 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.

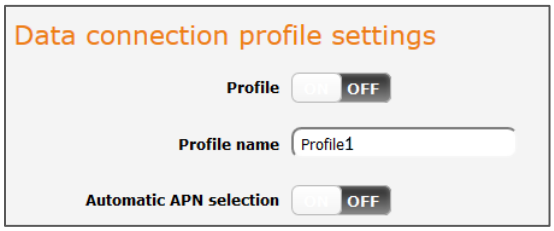


Figure 29 - Data connection profile settings

2 Click the **Profile** toggle key to turn the profile **ON**.

© Casa Systems 2020

3 Once enabled, additional profile details will display:

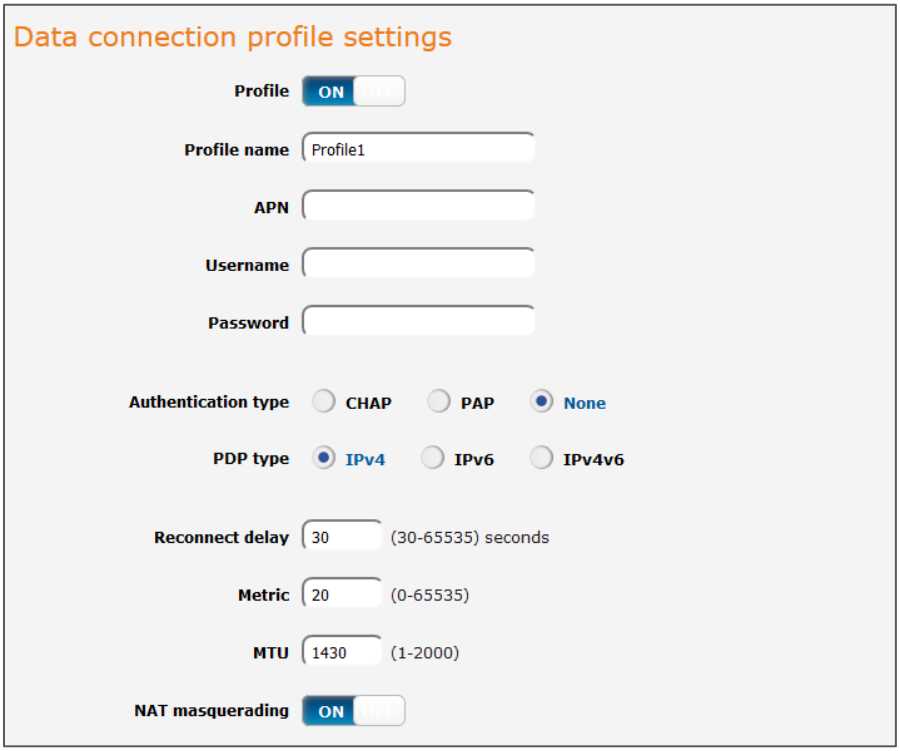


Figure 30 - Data connection settings - Profile turned on

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

© Casa Systems 2020

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.

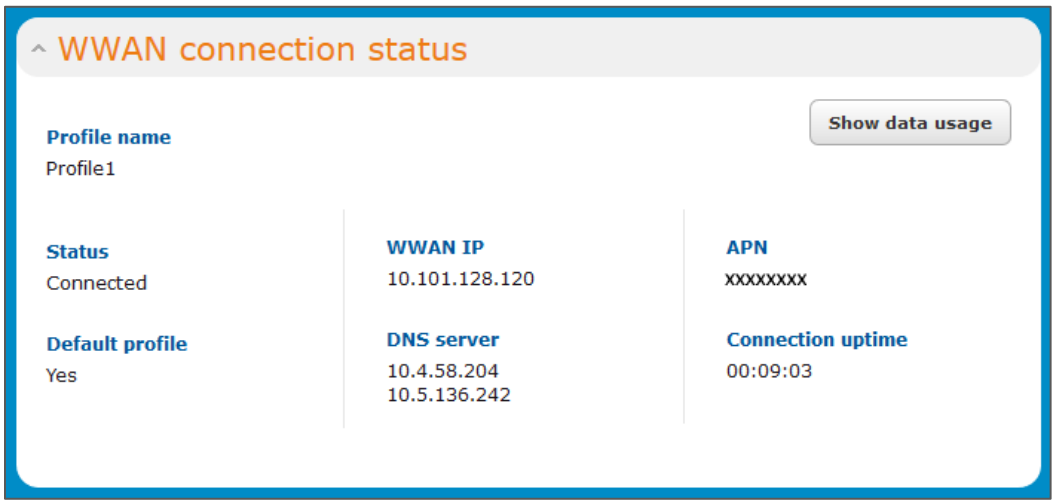


Figure 31 - WWAN connection status section

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**.

© Casa Systems 2020

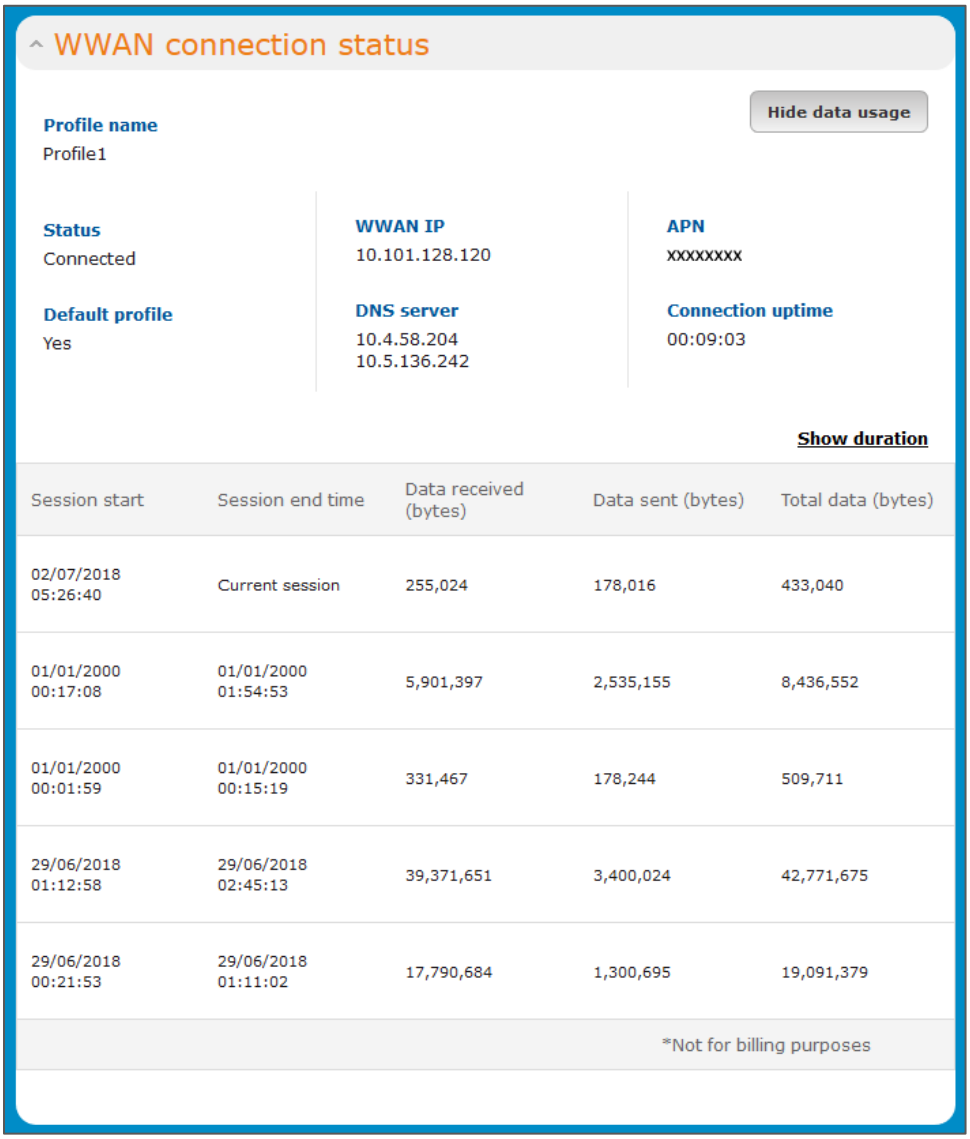


Figure 32 - Data usage

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 33 - Data usage with connection duration

© Casa Systems 2020

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.

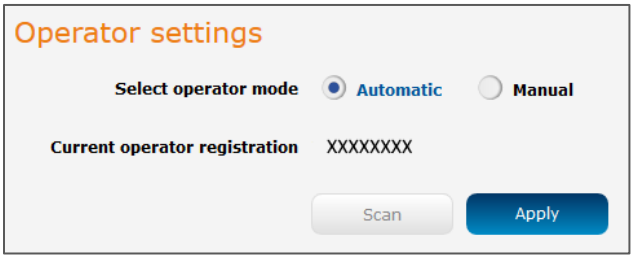


Figure 34 - Operator settings

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.

© Casa Systems 2020

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

	Operator name list	MCC	MNC	Operator status	Network type
●	Telstra	505	01	Current	LTE (4G)
○	Telstra	505	01	Available	UMTS (3G)
○	vodafone AU	505	03	Forbidden	UMTS (3G)
○	Optus AU	505	02	Forbidden	LTE (4G)
○	Optus AU	505	02	Forbidden	UMTS (3G)
○	vodafone AU	505	03	Forbidden	LTE (4G)

Figure 35 - 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.

© Casa Systems 2020

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**.

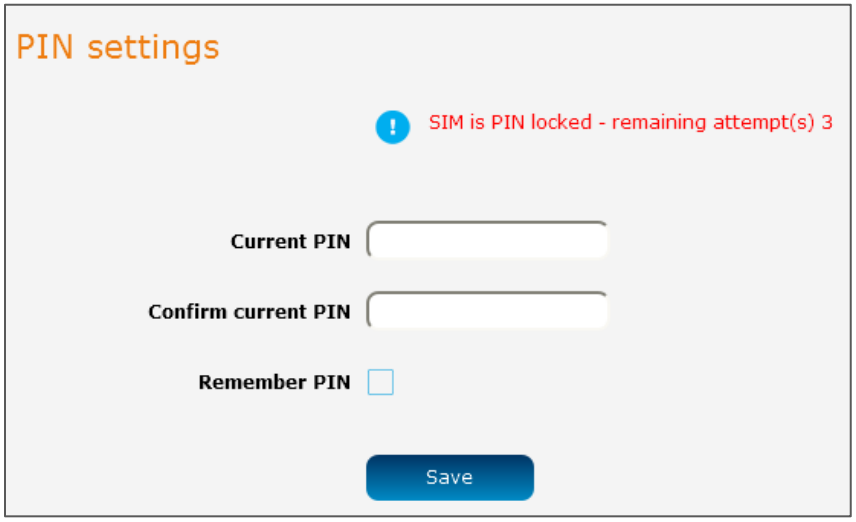


Figure 36 - SIM security settings - SIM PIN locked

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.

5 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.

6 Click the **Save** button.

© Casa Systems 2020

If successful, the antenna displays the following screen:

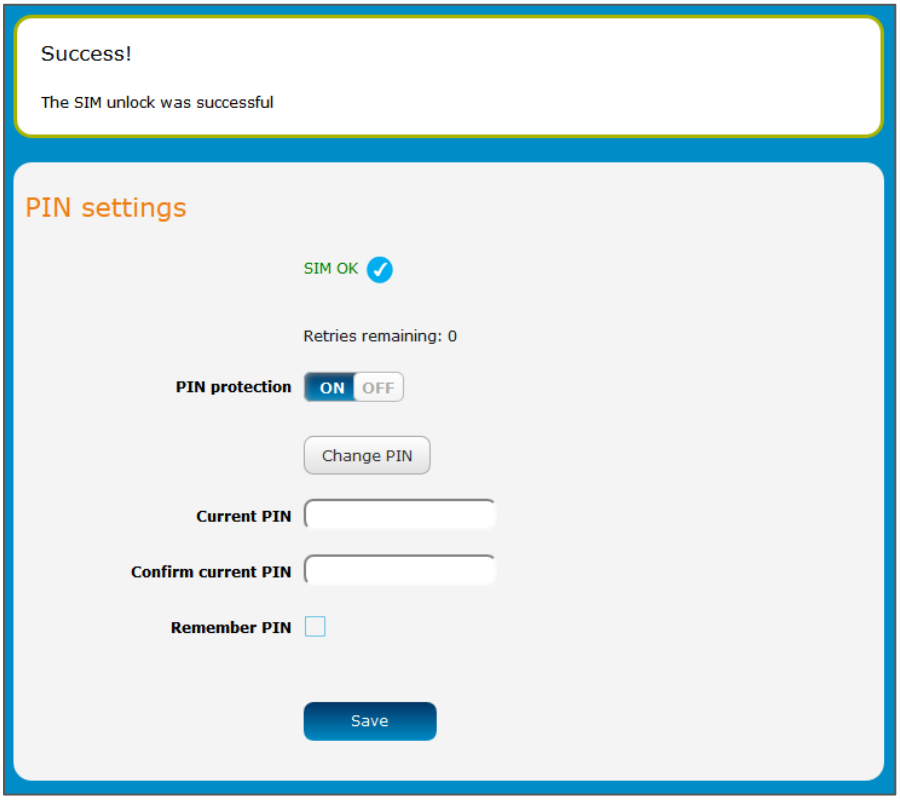


Figure 37 - SIM security settings - SIM unlock successful

Enabling/Disabling SIM PIN protection

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

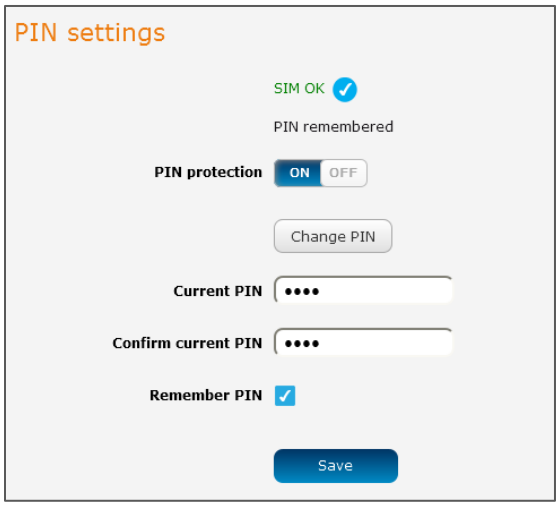


Figure 38 - PIN Settings

© Casa Systems 2020

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.

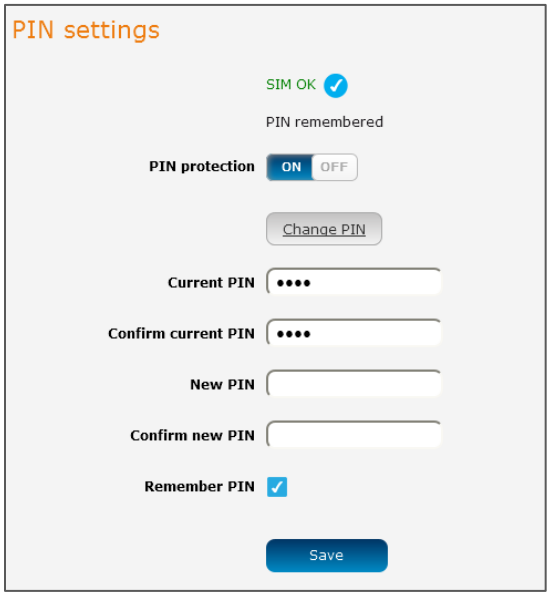


Figure 39 - PIN settings - Change PIN

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

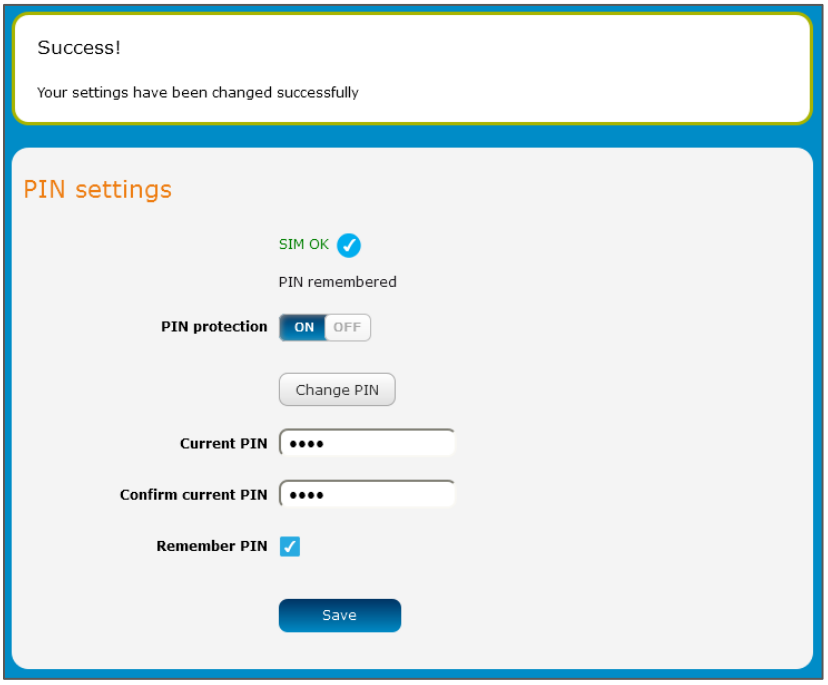


Figure 40 - SIM security settings – PIN unlock successful

© Casa Systems 2020

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.

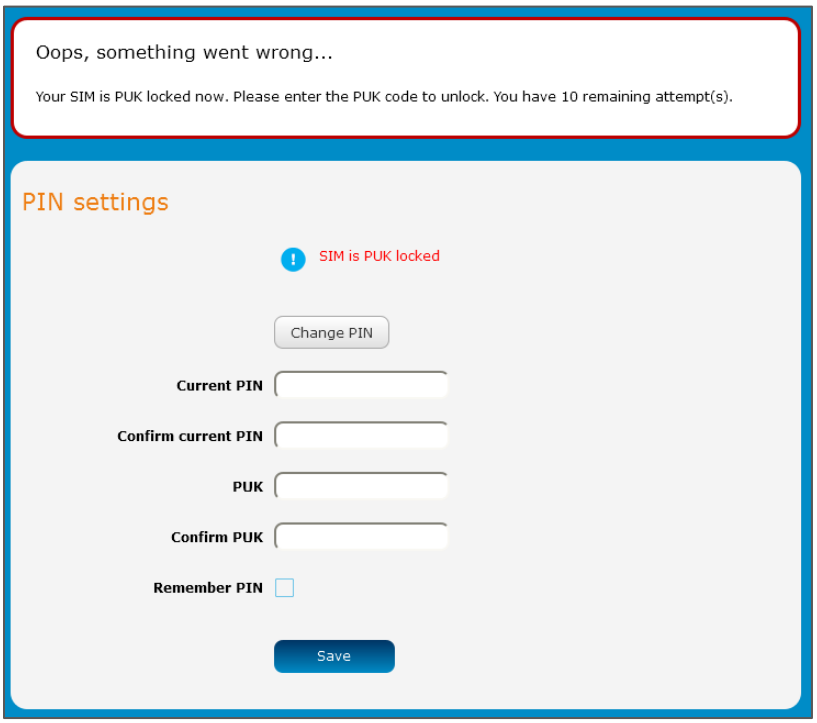


Figure 41 - SIM security - SIM PUK locked

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.

© Casa Systems 2020

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.

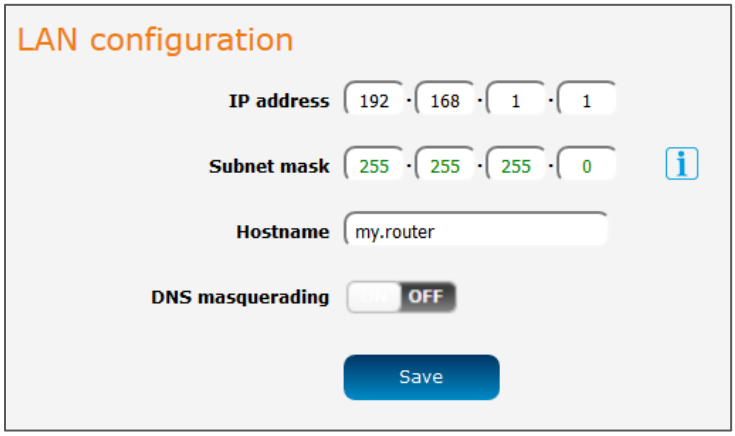


Figure 42 – LAN configuration settings

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-2182 antenna.

© Casa Systems 2020

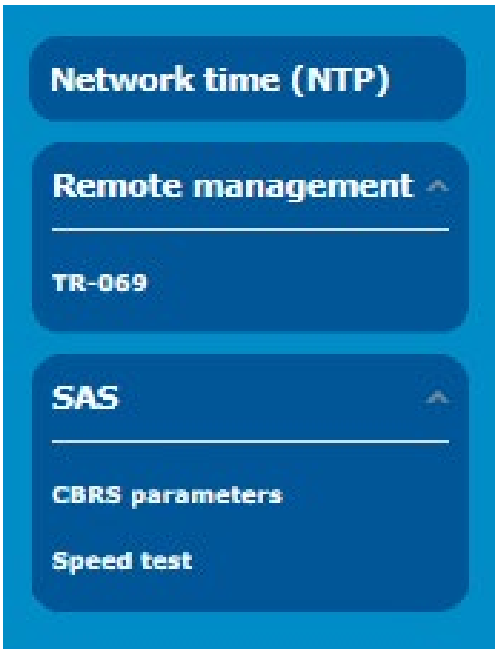
With DNS masquerading **ON**, the DHCP server embedded in the CFW-2182 antenna hands out its own IP address (e.g. 192.168.0.1) as the DNS server address to LAN clients. The downstream clients then send DNS requests to the CFW-2182 antenna which proxies them to the upstream DNS servers.

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.

© Casa Systems 2020

Services



The **Services** tool group provides configuration options for features that support extended utilisation of your CFW-2182 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-2182 antenna's internal clock with a global Internet time server.

SAS supports CBRS registration required to access 150 MHz wide broadcast band channels in a particular geographic area.

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

© Casa Systems 2020

Network time (NTP)

The NTP (Network Time Protocol) settings page allows you to configure the CFW-2182 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.

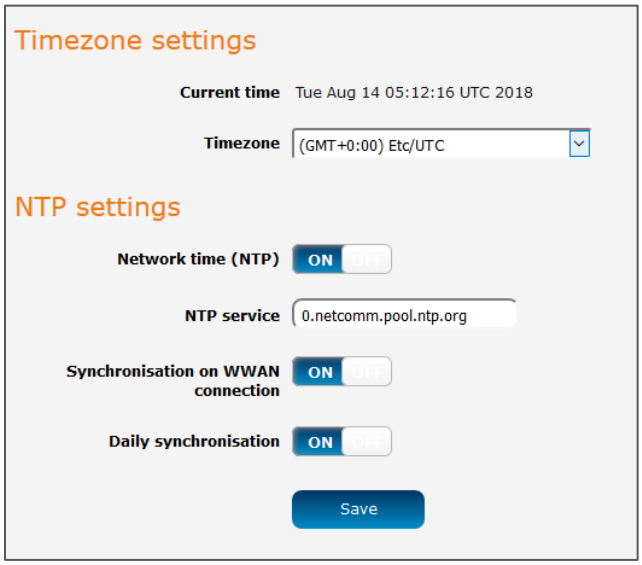


Figure 43 - NTP settings

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.

© Casa Systems 2020

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.

© Casa Systems 2020

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.

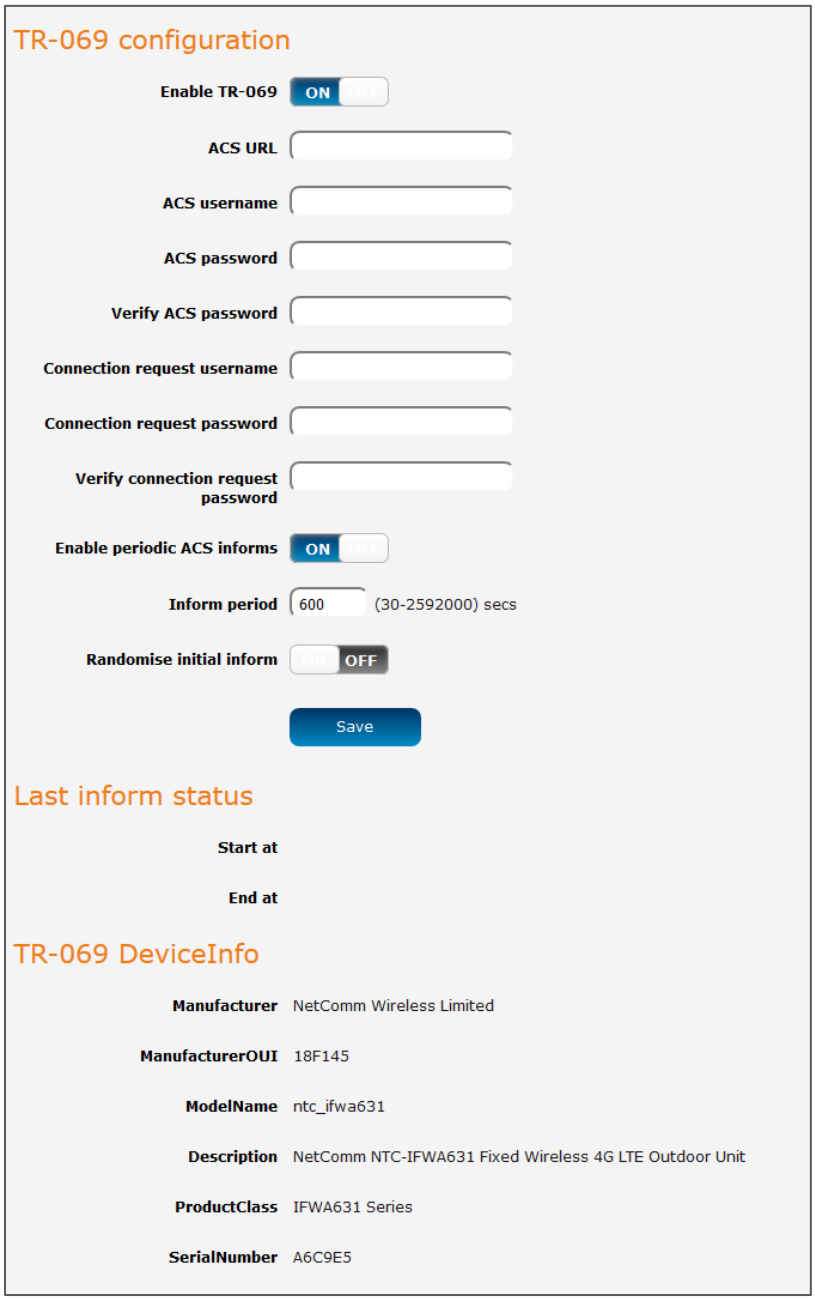


Figure 44 - TR-069 configuration

To configure TR-069:

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

© Casa Systems 2020

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.

© Casa Systems 2020

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-2182 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.

CBRS Registration Status

To see the CFW-2182's current **CBRS Registration Status** open the **Services** menu, drop down the **SAS** submenu and select **CBRS parameters**.

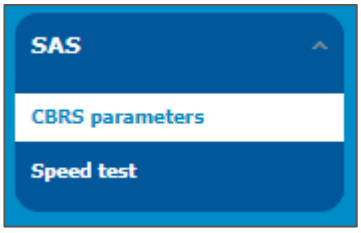


Figure 45 – Select CBRS parameters from SAS submenu

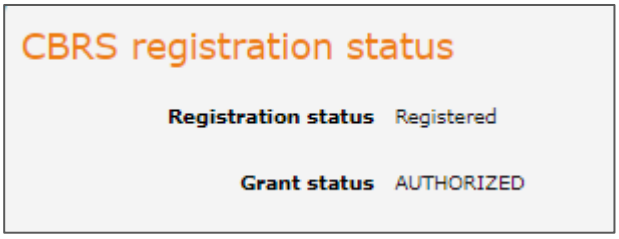


Figure 46 – CBRS Registration Status details

The **Registration Status** will be indicated as either: **Registered** or **Unregistered**

The **Grant status** will also be specified. It may be: **AUTHORIZED, PENDING, GRANTED** or blank

Speed Test

To see the CFW-2182'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-2182 and those respective servers.

© Casa Systems 2020

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.

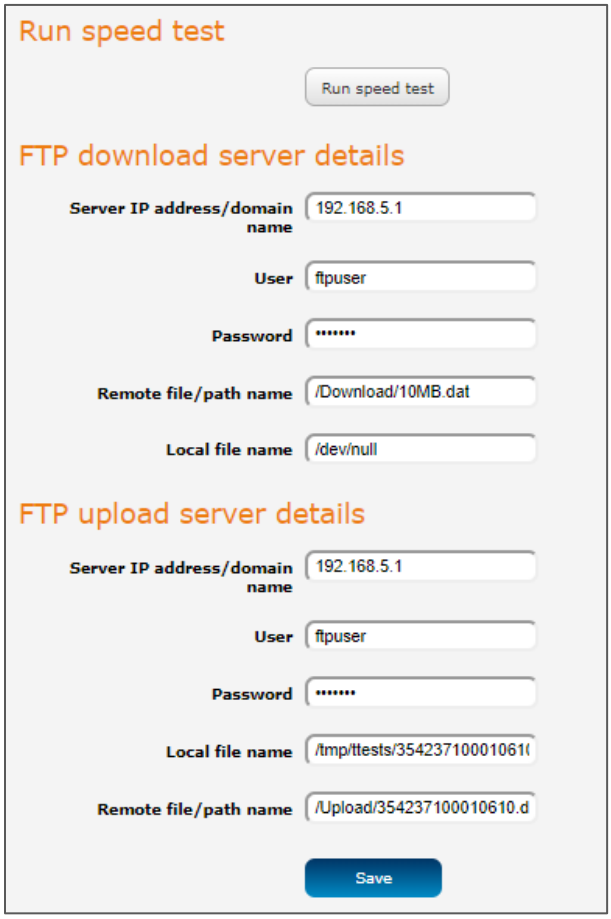


Figure 47 – Speed test parameters

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

Option	Description
Server IP address/ domain name	Enter the IP address or domain name that the FTP server is running on.
User	If an account is required, enter the username here, otherwise leave this blank.
Password	If an account is required, enter the password here, otherwise leave this blank.

© Casa Systems 2020

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

Table 7 - Speed test parameter details

Test results

Click the **Run speed test** button to check the current speeds between the CFW-2182 and the download and upload servers.

A list of results will appear on the page:

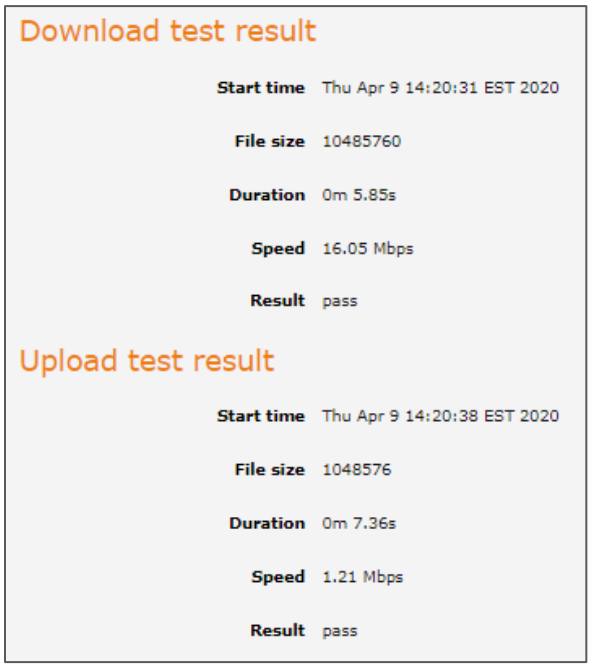


Figure 48 – Speed Test results display

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

Option	Description

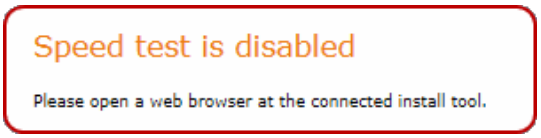
© Casa Systems 2020

Start time	The date and exact time the download or upload part of the speed test began.
File size	The size of the file used to measure the speed.
Duration	Time in seconds taken to successfully transfer the full file.
Speed	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-2182 you cannot connect to these setting through this interface.

Important –



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

© Casa Systems 2020

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-2182.

© Casa Systems 2020

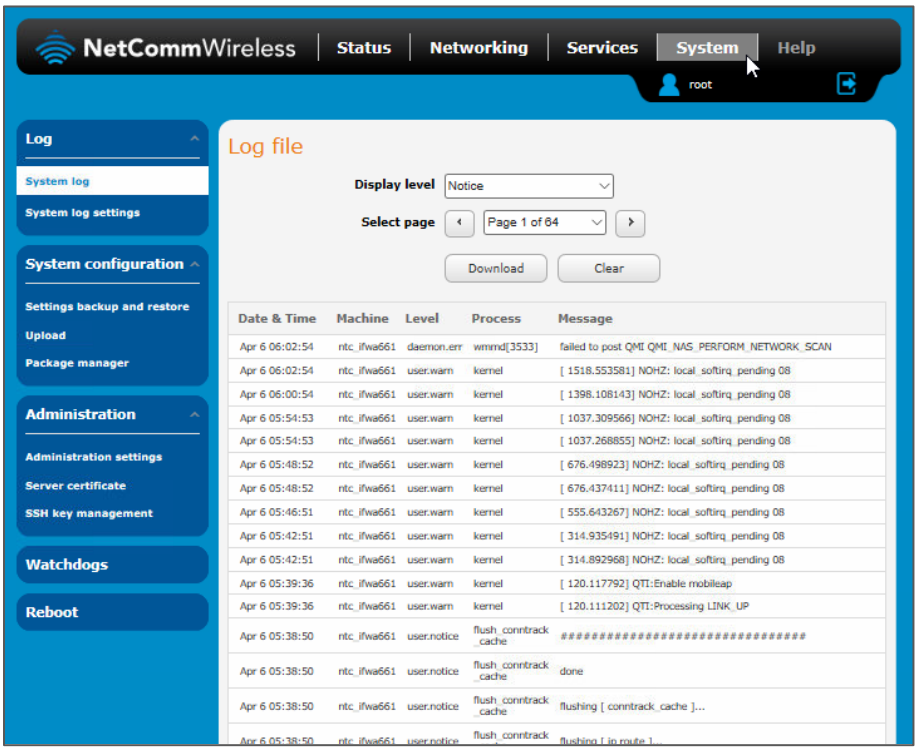
Log

The Log pages are used to display or download the System log on the CFW.

System log

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

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



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

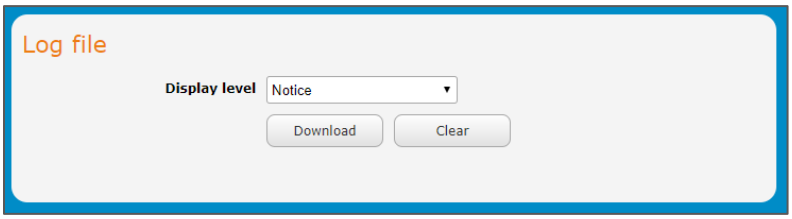


Figure 49 - System log file

© Casa Systems 2020

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

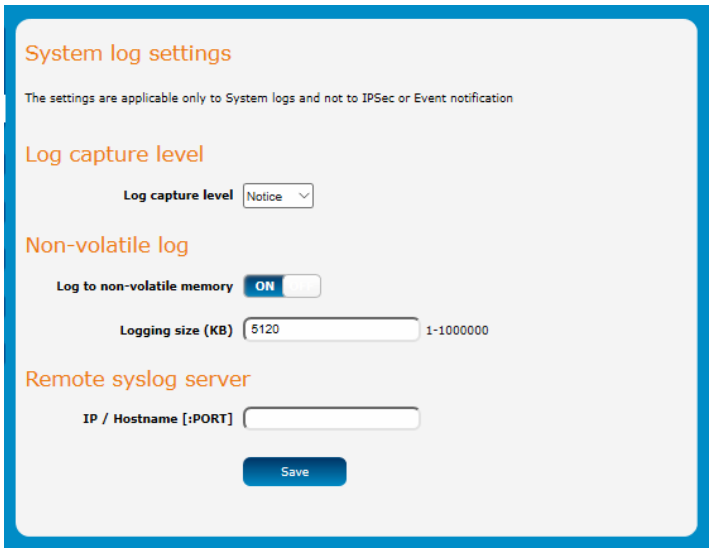


Figure 50 - System log settings

© Casa Systems 2020

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

Table 10 - System log capture levels

Non-volatile log

When the CFW is configured to log to non-volatile memory, the log data is stored in flash memory, making it accessible after a reboot of the CFW. 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 CFW 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 CFW-2182 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 CFW will use the default UDP port 514.
3. Click the **Save** button to save the configuration.

© Casa Systems 2020

Figure 51 – 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.

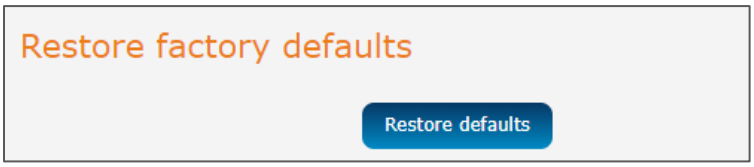


Figure 52 – Restore factory defaults button

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.

© Casa Systems 2020

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

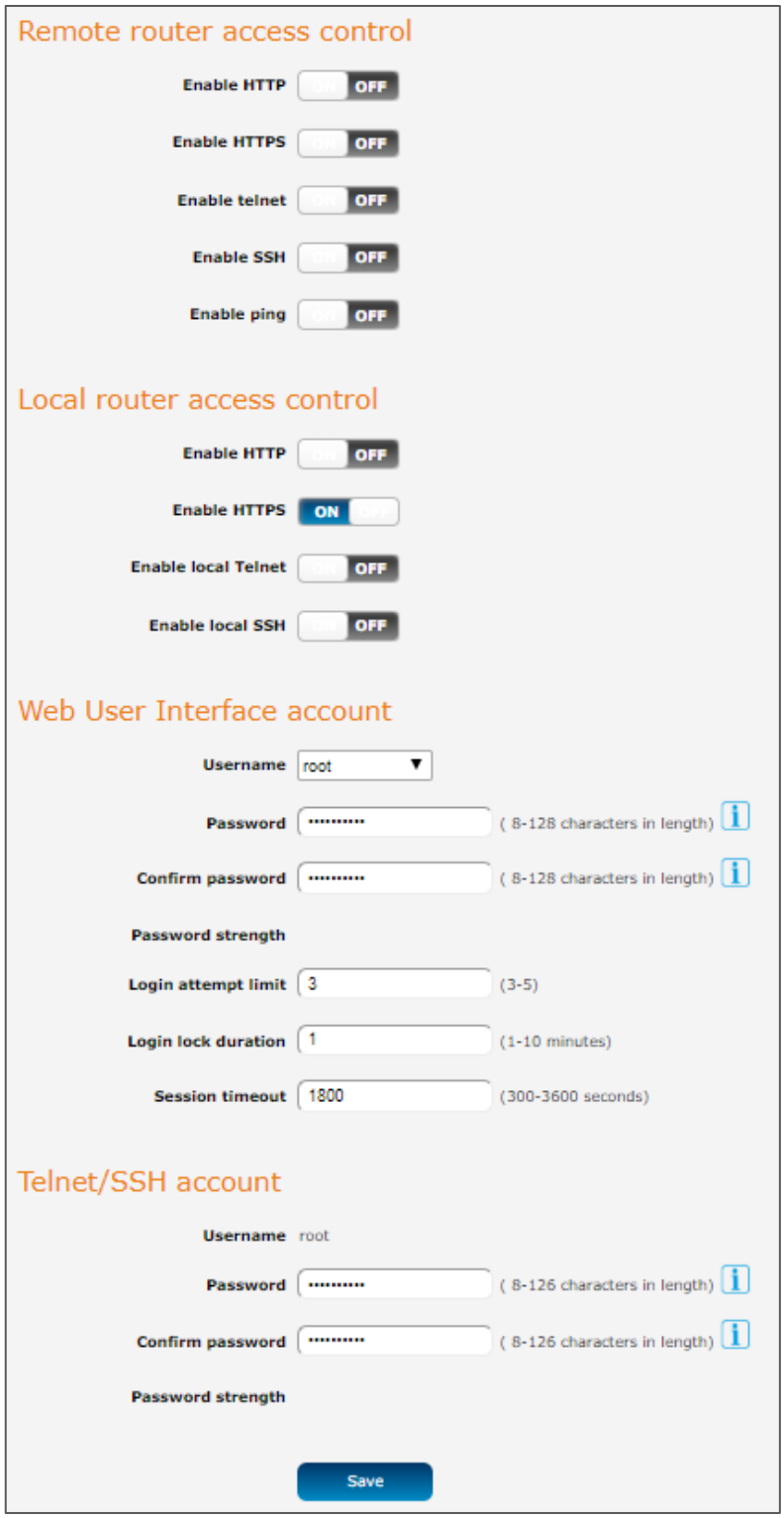
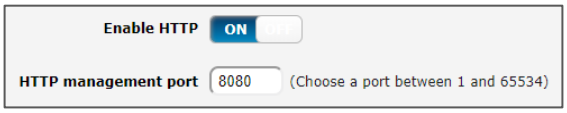
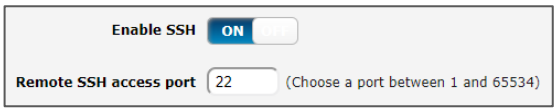


Figure 53 - Administration page

© Casa Systems 2020

Option	Definition
Remote router access control Note that all remote router access control settings are disabled by default.	
Enable HTTP	Enable or disable remote HTTP access to the antenna.
HTTP management port	When HTTP is enabled (see previous) you can set the HTTP management port.  Enter a port number between 1 and 65534 to use when accessing the antenna remotely.
Enable SSH	Enable or disable Secure Shell on the antenna.
Remote SSH Access Port	When SSH is enabled (see previous) you can set the remote SSH access port.  Enter the port number for remote SSH access. The port number must be between 1 and 65534.
Enable Ping	Enable or disable remote ping responses on the WWAN connection.
Local router access control	
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.
Web User Interface account	
Username	Use the drop-down list to select the root or user account to change its web user interface password.
Password	Enter the desired web user interface password. 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.
Password strength	The CFW-2182 antenna includes algorithms to ensure that the password you enter is strong. Any password configured on the router must now meet the following criteria:

© Casa Systems 2020

	• Be a minimum of eight characters and no more than 128 characters in length. • Contain at least one upper case, one lower case character and one number. • Contain at least one special character, such as: `~!@#$%^&*()-_=+[{]}\\|;:'",<.>/?. Additionally, the password must also satisfy an algorithm which analyses the characters as you type them, searching for commonly used patterns, passwords, 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).
Telnet/SSH account	
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**.

© Casa Systems 2020

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.

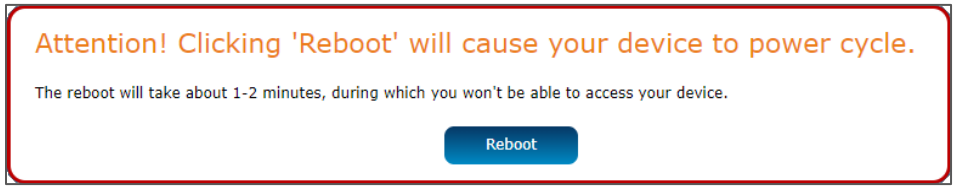


Figure 54 - Reboot confirmation

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.

© Casa Systems 2020

Appendix A – Default Settings

The following tables list the default settings of the CFW.

LAN (Management)

IP Address	192.168.1.1
Subnet Mask:	255.255.255.0

Table 12 - LAN Management Default Settings

© Casa Systems 2020

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. This equipment must be installed and operated with a minimum distance of eight (8) inches or twenty (20) centimeters between the radiator & your body.

FCC Statement

This device must be professionally installed.

FCC compliance

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

FCC regulations

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device 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:

© Casa Systems 2020

- 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

Product details

Product: CBRS 4G High Gain Outdoor CPE

Model No: CFW-2182

© Casa Systems 2020