



CONFIGURATION GUIDE

cnWave™ 5G Fixed

Release 3.3



Reservation of Rights

Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium recommends reviewing the Cambium Networks website for the latest changes and updates to products. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems ("High Risk Use").

This product is not restricted in the EU. Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Contents

Contents	3
About This Guide	6
Purpose	6
Cross references	6
Feedback	6
Warnings, cautions, and notes	6
Warnings	6
Cautions	6
Notes	7
Important regulatory information	7
Application software (firmware)	8
Ethernet networking skills	8
Lightning protection	9
Specific expertise and training for professional installers	9
Legal and Open-Source Software statements	9
Problems and warranty	9
Reporting problems	9
Repair and service	9
Hardware warranty	9
Security advice	10
Caring for the environment	10
In EU countries	10
In non-EU countries	10
Preparing for Configuration	11
Basic information about the products	11
Safety precautions	11
Regulatory compliance	11
Prerequisite tasks	12
Connecting and configuring the BTS or the CPE device	12

Configuring the management PC	13
Accessing the B1000 UI	14
The B1000 Dashboard	18
UI Controls	18
Viewing the B1000 dashboard	20
General	20
Device	22
Radio	25
GNSS	27
Accounts	30
Configuring B1000 (BTS)	30
Configuring system settings	30
Viewing Subscriber (CPE) Data	61
Configuring tools	74
The C100 Dashboard	94
Accessing the C100 UI	94
Viewing the C100 (CPE) dashboard	97
Configuring C100 (CPE)	107
Configuring system settings	107
Configuring tools	132
Setting up a wizard	141
Appendix 1: cnMaestro X Configuration	144
Prerequisite tasks	144
Configuring cnMaestro X	144
Managing BTS and CPEs	148
Dashboard	149
Notifications	149
Configuration	152
Details	154
CPEs	155
Performance	156

Software Upgrade	157
Tools	159
Assists X	160
Generating data reports	161
Appendix 2: Acronyms and Abbreviations	165
Cambium Networks	167

About This Guide

This document explains how to configure the **cnWave™ 5G Fixed** platform of products. It is intended for use by the system designer, system installer, and system administrator.

Purpose

Documents specific to the cnWave™ 5G Fixed platform of products are intended to instruct and assist personnel in the operation, installation, and maintenance of the Point-to-MultiPoint (PMP) equipment (Cambium Networks) and ancillary devices of cnWave™ 5G Fixed platform of products. It is recommended that all personnel engaged in such activities must be properly trained.

Cambium Networks disclaims all liability, whatsoever, implied or express - for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf - to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into topics that are divided into sections. Sections are not numbered and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. To provide feedback, visit the Cambium Networks [Support](#) site.

Warnings, cautions, and notes

The following sections describe how warnings, notes, and cautions are used in this document and in all documents of Cambium Networks:

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:



Warning

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:



Caution

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:



Note

Note text.

Important regulatory information

The cnWave™ 5G Fixed platform of products are certified as an unlicensed device in frequency bands where it is not allowed to cause interference to licensed services (called primary users of the bands).

Complying with rules for the country of operation

USA specific information



Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.



Note

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference 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.

Canada specific information



Caution

This device complies with ISED's license-exempt RSSs. Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device. This device must accept any interference, including interference that may cause undesired operation of the device.



Note

Certification note from industry Canada: While this equipment meets the technical requirements for its operation in its rated paired block arrangement, this block arrangement is different than the 40 + 40 MHz block arrangement prescribed in documents RSS-191 and SRSP-324.25. The operation of this equipment IS NOT permitted if the out-of-band and spurious emission limits are not met at the edge of any contiguous licensed spectrum. It should be noted that all current relevant spectrum policies, licensing procedures, and technical requirements are still applicable. For additional information, contact the local Industry Canada office.

Renseignements spécifiques au Canada



Note

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- L'appareil ne doit pas produire d'interférences; et
- L'utilisateur de l'appareil doit accepter toute interférence radioélectrique, même si elle est susceptible d'en compromettre le bon fonctionnement.

European specific information

The cnWave™ 5G Fixed platform of products are compliant with applicable European Directives required for CE marking:

- 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC; Radio Equipment Directive (RED).
- 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS Directive).

EU Declaration of Conformity

Hereby, Cambium Networks declares that the Cambium Networks cnWave™ 5G Fixed Series of Wireless Ethernet Bridge complies with the essential requirements and other relevant provisions of Directive 2014/53/EU. The declaration of conformity may be consulted at <https://www.cambiumnetworks.com/>.

Application software (firmware)

Download the latest cnWave™ 5G Fixed products' software and install it in the Base Transceiver System (BTS) and Customer Equipment Premise (CPE) before deploying the equipment. Instructions for installing software are provided in the *cnWave™ 5G Fixed Planning and Installation Guide* (available at <https://support.cambiumnetworks.com/files/28cnwave/>).

Ethernet networking skills

The installer must have the ability to configure the IP address on a PC and to set up and control products using a web user interface (UI).

Lightning protection

To protect outdoor radio installations from the impact of lightning strikes, the installer must be familiar with the normal procedures for site selection, bonding, and grounding. Installation guidelines for the cnWave™ 5G Fixed platform of products are available in the Lightning Protection Units (LPUs) section in the *cnWave™ 5G Fixed Planning and Installation Guide*.

Specific expertise and training for professional installers

To ensure that the cnWave™ 5G Fixed product series are installed and configured in compliance with the requirements of EU, ISEDC, and the FCC, installers must have the radio engineering skills and training described in this section.

Use the [Training](#) link to access the technical training programs (from Cambium Networks).

Legal and Open-Source Software statements

Refer to the cnWave™ 5G Fixed Legal and Open-Source Guide for:

- Cambium Networks end user license agreement and
- Open-Source Software Notices.

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the [Support](#) site of Cambium Networks.
3. Ask for assistance from the Cambium Networks product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the [Support](#) site.

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from the date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced products will be subject to the original warranty period but not less than thirty (30) days.

To register PMP and PTP products or activate warranties, visit the support website. For warranty assistance, contact the reseller or distributor. The removal of the tamper-evident seal will void the warranty.



Caution

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium Networks recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium Networks makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium Networks equipment in EU countries.

Disposal of Cambium equipment

European Union (EU) Directive 2012/19/EU Waste Electrical and Electronic Equipment (WEEE).

Do not dispose the Cambium Networks equipment at landfill sites. For disposal instructions, refer to <https://www.cambiumnetworks.com/support/compliance/>.

Disposal of surplus packaging

Do not dispose the surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Preparing for Configuration

This section provides basic information about the cnWave™ 5G Fixed platform of products and prerequisite tasks. This information helps you to set up the system before proceeding with the configuration of the cnWave™ 5G Fixed products and antenna alignment tasks.

This section covers the following topics:

- [Basic information about the product](#)
- [Safety precautions](#)
- [Regulatory compliance](#)
- [Prerequisite tasks](#)

Basic information about the products

The cnWave™ 5G Fixed platform of products (from Cambium Networks) are a high-end Point-to-Multipoint (PMP) system providing easy, fast, and cost-effective wireless Gigabit connectivity for edge access solutions at a significantly lower cost than fiber infrastructure.

The cnWave™ 5G Fixed platform consists of a B1000 Base Transceiver Station (BTS), which serves one or more C100 Customer Premises Equipment (CPE).

With the cnWave™ 5G Fixed platform of products, operators and service providers have access to Gigabit for business and residential connectivity and backhaul for Wi-Fi access. These products enable carriers and service providers to offer high-speed broadband connectivity to subscribers in areas not reachable through full-fiber networks.

For more information about the product description and installation (including frequency bands and hardware requirements), refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

Safety precautions

All national and local safety standards must be followed while configuring the units and aligning the antennas.



Warning

Ensure that the personnel is not exposed to unsafe levels of RF energy. The units start to radiate RF energy as soon as they are powered up. Respect the safety standards defined in Legal and Open Sources Guide, in particular the minimum separation distances.

Observe the following guidelines:

1. Never work in front of the antenna when the Outdoor Unit (ODU) is powered.
2. Always power down the Power Supply Unit (PSU) before connecting or disconnecting the drop cable from the PSU, ODU, or Lightning Protection Unit (LPU).

Regulatory compliance

All BTS and CPE specific radio regulations must be followed while configuring the units and aligning the antennas. For more information, refer to the Compliance with radio regulations section in the Legal and Open Sources Guide.

Prerequisite tasks

Before performing the configuration tasks, ensure that you have met the following hardware requirements (for example):

- A personal computer (PC) or laptop if you want to connect directly to either B1000 BTS or C100 CPE.
- B1000 BTS or C100 CPE with IP address configured (as described in the [Configuring the management PC](#) section).
- A RADIUS Server for CPE authentication and provisioning.

For more information about the main hardware requirements, cabling, and power related tasks, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.



Note

In the later sections of this guide, the term BTS is used to refer to B1000 BTS and the term CPE to refer to C100 CPE.

To put the whole system together, you must perform the following prerequisite tasks:

1. [Connecting and configuring the BTS or the CPE device](#)
2. [Configuring the PC to set up the IP address for the BTS or the CPE](#)
3. [Accessing the user interface \(UI\)](#)

These prerequisite tasks help you to ensure that each component of the system is working before the final integration.

Connecting and configuring the BTS or the CPE device

Using a laptop or PC, perform the following steps to configure the BTS or the CPE device:

1. Connect the 56V 240W PSU to the MAIN port on the BTS or the PC (in the case of CPE). For more details, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.
2. For BTS, connect an Ethernet cable between the network port of the PC and MAIN from the BTS. In case of the CPE, connect an Ethernet cable between the PoE data port and the CPE data port.
3. Configure the Network adapter card of the PC or laptop to connect to the BTS or the CPE.

The BTS or the CPE can be accessed by using the default IP address (169.254.1.1). For information about configuring the IP address, refer to the [Configuring the management PC](#) section.



Note

For detailed information about assembling, connecting, and powering up the *cnWave™ 5G Fixed* products (BTS or CPE), refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

Configuring the management PC

You must configure the PC (for example, using Windows PC) or laptop to set up the IP address (169.254.1.1) for the BTS. This configuration enables the PC to communicate with the BTS and CPEs.



Note

For information on how to connect cables and connect to power, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

To configure the PC, perform the following steps:

1. On Windows PC, click **Start > Settings > Network & Internet**.

The **Network Status** page appears with multiple options on the left navigation column.

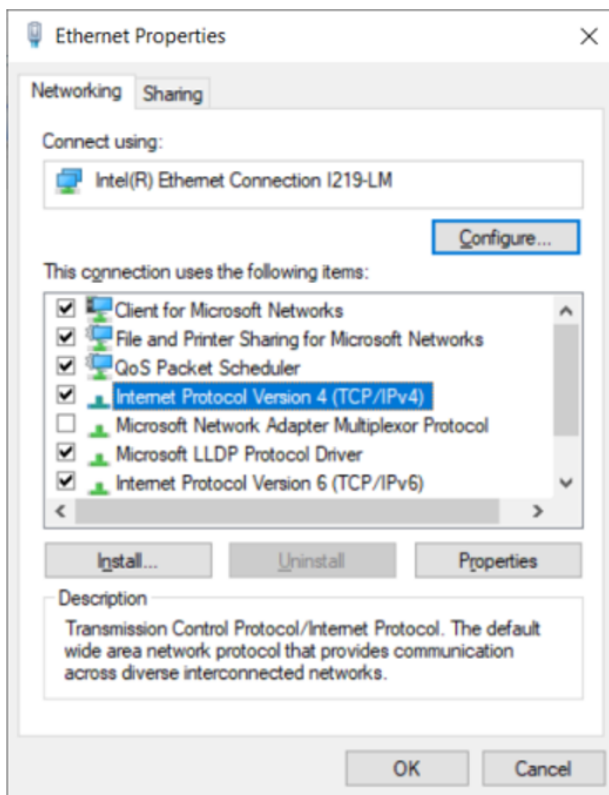
2. Select **Ethernet > Change adapter settings**.

The **Network Connections** page appears.

3. Select **Ethernet** and right-click to select **Properties**.

The **Ethernet Properties** dialog box appears with the **Networking** and **Sharing** tabs, as shown in [Figure 1](#).

Figure 1: The Ethernet Properties dialog box

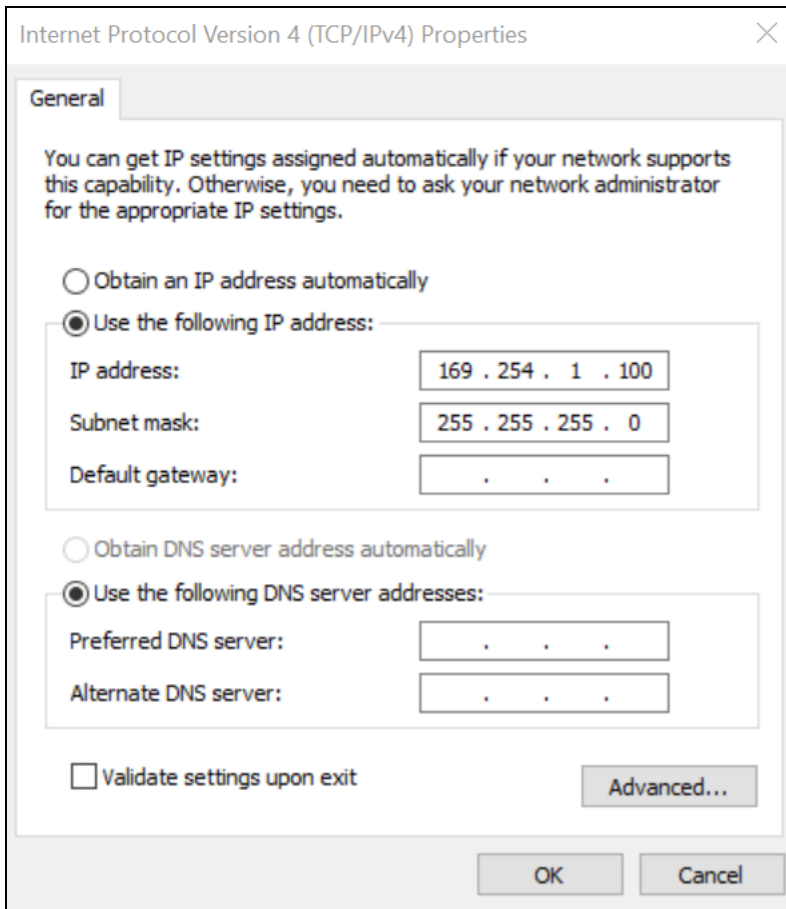


By default, the **Networking** tab is selected.

4. Select **Internet Protocol Version 4 (TCP/IPv4)** from the available list of connections (as shown in [Figure 1](#)).
5. Click **Properties**.

The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box appears, as shown in [Figure 2](#).

Figure 2: *The Internet Protocol Version 4 Properties dialog box*



6. In the **Use the following IP address** section, type an appropriate IP address in the **IP address** text box.
Example: 169.254.1.1

If you are using 169.254.1.1 as the default address, you must avoid using 169.254.0.0 and 169.254.1.1 IP addresses.

7. In the **Subnet mask** text box, type 255.255.255.0.
8. Leave the **Default gateway** text box blank and click **OK**.
9. Ensure that you can communicate with the BTS by running a continuous PING session at a command prompt.

Example: You must run a command prompt and type `Ping -t 169.254.1.1`. If the PING is successful, you can access the login page of B1000 (BTS) using the `http://169.254.1.1` URL.

Accessing the B1000 UI

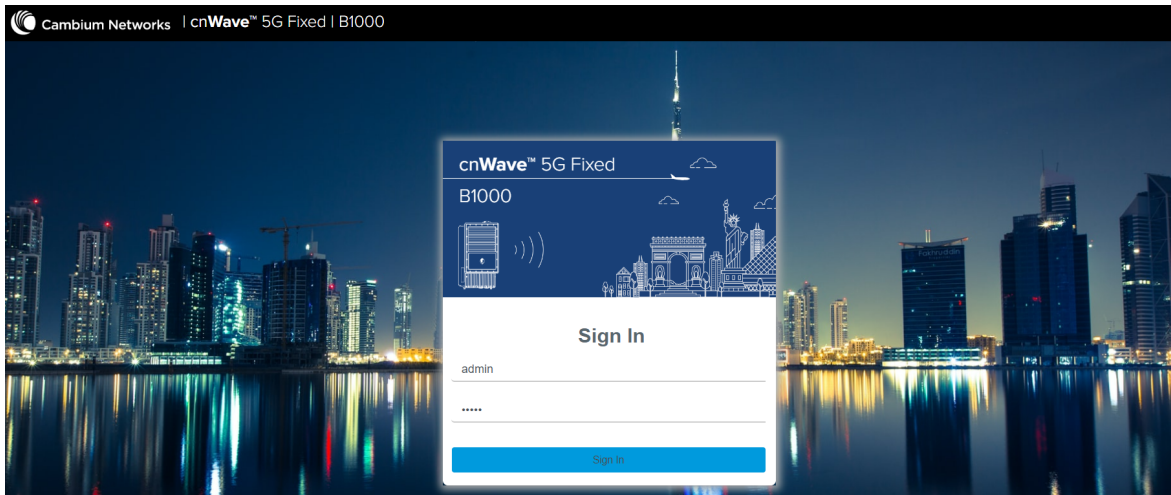
To access the B1000 UI, perform the following steps:

1. Use the default IP address (169.254.1.1) to connect to the BTS setup.
2. Ensure that your PC is set up to communicate with the required range of IP addresses.

3. Open a web browser and type the URL - <http://169.254.1.1> - to access the B1000 UI.

The **Sign In** page appears, as shown in [Figure 3](#).

Figure 3: *The Sign In page for B1000 UI*



4. Type an appropriate username and password.

Default username: admin

Default password: admin

5. Click **Sign In**.

The **Profile** page appears, as shown in [Figure 4](#). This page allows you to change the password.

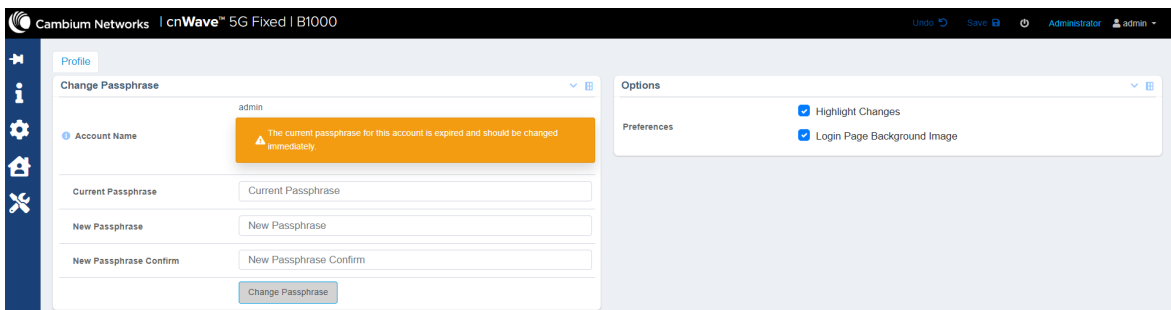


Note

Do not change the password every time when the **Profile** page appears. You must change the password only when it is required.

You can also access the **Profile** page by selecting **Profile** from the **admin** drop-down list on the top right side of the B1000 UI.

Figure 4: *The Profile page*



[Table 1](#) lists and describes the parameters available on the **Profile** page.

Table 1: List of parameters in the Profile page

Parameter	Description
Change Passphrase	
Account Name	The default name of the user account required for accessing the B1000 UI. This is read-only parameter.
Current Passphrase	The default password used for the first time log in or the old password used for the previous access. Enter the current password in the text box. Default password: <code>admin</code>
New Passphrase	Enter a new password in the text box. Note: The maximum character limit for the password is eight.
New Passphrase Confirm	Reenter the new password in the text box to confirm.
Change Passphrase	An option to change the current password. Click Change Passphrase to change the current password.
Options Used for the engineering purpose.	
Preferences	An option to set your preferences in the UI. Following options are supported: <ul style="list-style-type: none"> • Highlight Change: Use this option to easily identify the new changes, which are highlighted in light yellow color on UI pages. These highlighted values help you in quickly monitoring the system changes. Example: The System > Interface UI page displays the highlighted values in light yellow color. • Login Page Background Image: Use this option to set the background image on the Sign In page of UI (as shown in Figure 3). Select the check boxes, if required.

6. On changing the password, log on to the B1000 UI using admin (username) and the new password (which you set on the **Profile** page).

The **Profile** page appears, as shown in [Figure 4](#).

7. To view the main B1000 dashboard, click the  icon (Dashboard) on the left navigation pane.

The **Dashboard** page appears. For more information about the B1000 dashboard page, refer to the [Viewing the B1000 dashboard](#) section.



Note

To log out from the UI, select **Logout** from the **admin** drop-down list at the top right side of the UI.

To change the password, select **Profile** from the **admin** drop-down list. For more information on changing the password and setting preferences, refer to [Table 1](#).

When you log on to the B1000 UI, you can use the required UI controls (as described in [Table 1](#)) for configuring and managing BTS.



Note

For information on how to access the C100 (CPE) UI, refer to the [Accessing the C100 UI](#) section.

The B1000 Dashboard

This section provides information about UI controls and the main B1000 dashboard page. It also explains how to configure BTS using the B1000 UI.




This section covers the following topics:












- [UI Controls](#)
- [Viewing the B1000 Dashboard](#)
- [Configuring B1000 \(BTS\)](#)

UI Controls

Before configuring the UI of B1000 and C100, familiarize yourself with the UI controls (as described in [Table 2](#)). These UI controls are required for adding, viewing, and managing B1000 and C100 configurations.

Table 2: List of UI controls

UI Control	UI Control name	Description
	Dashboard	To open the main dashboard page of the required product. Applicable to both B1000 and C100 UIs.
	System	To configure the required system settings of cnWave™ 5G Fixed platform of products. For BTS: <ul style="list-style-type: none">• General• Management• Radio• Interface• CPE Provisioning• Synchronisation For CPE: <ul style="list-style-type: none">• General• Management• Radio• Interface• Session• RADIUS Authentication Applicable to both B1000 and C100 UIs.
	Subscribers	To view (read-only) all the data related to CPE subscribers.

UI Control	UI Control name	Description
		Applicable only to the B1000 UI.
	Tools	To update firmware and reboot the unit. Applicable to both B1000 and C100 UIs.
	Setup Wizard	To configure the CPE (for example, frequencies, power, polarisation, and other configurations). Applicable only to the C100 UI.
Other common UI controls:		
	Expand or collapse	To expand or collapse the options in the left navigation column of the dashboard.
	Expand	To expand the parameters of a section.
	Collapse	To collapse the parameters of a section.
	Table	To view the parameters in a column format.
	Revert	To go back to the previous option.
	Undo	To undo the changes.
	Save	To save the changes.
	Power	To restart or reboot the system from the UI.
	admin	To change the password of the UI and log out from the UI.

Viewing the B1000 dashboard

When you log on to the B1000 UI (as described in the [Accessing the B1000 UI](#) section), the main B1000 dashboard page appears as shown in [Figure 5](#).


Figure 5: The B1000 dashboard

The B1000 dashboard provides a simple representation of the number of CPEs connected and registered with BTS, and the connection status of CPEs. Example: [Figure 5](#) shows the B1000 dashboard, which indicates the number of CPEs that are registered to and connected with BTS.



Note

Currently, the B1000 BTS device can support up to 120 CPE connections.

You can also use the **Dashboard**  icon to view the main B1000 dashboard page. The main B1000 dashboard page contains the following tabs:

- [General](#)
- [Device](#)
- [Radio](#)
- [GNSS](#)
- [Accounts](#) (visible and applicable only to engineer user roles)

General

The **General** page provides a summary (read-only) of the connected and registered devices. It also displays the subscriber status and other system-related details. [Table 3](#) lists and describes parameters available on the **General** page.


Table 3: List of parameters on the General page

Parameter	Description
Device	Indicates the Electronic Serial Number (ESN) of the hardware device and its run time.
Sessions	Total number of currently connected and registered CPEs.
Device Summary	
Product Name	Name of the device that you have deployed. Example: cnWave 5G Fixed Base Transceiver Station (BTS)
Release Name	Release number of the operational software.
System Description	A brief description of the system (device).
System Name	An administratively assigned name of the device. When using DNS, this name must be the device's fully qualified domain name (FQDN).
System Location	The physical location of the device node.
System Contact	Contact details of the device administrator.
System Time	Date and time (in YYYY-MM-DD 24-hour format) that are configured in the system.
NTP Synchronized	Determines whether BTS is using Network Time Protocol (NTP) to receive time from a reference clock. If the check box is selected, then the BTS is using NTP. You can set NTP on the Synchronisation page. For more details, refer to the Synchronisation section. Note: NTP is a networking protocol that allows you to automatically sync your system date and time with a remote server. NTP sets the reference time and date in the BTS.
cnMaestro Connection Status	Indicates the connection status of cnMaestro™ (a network management platform). For more information on configuring cnMaestro, refer to the cnMaestro Configuration section.
Subscribers	
Connected CPEs	Number of CPEs that are currently connected to the BTS.
Registered CPEs	Number of CPEs that are currently registered and authenticated with the BTS.
Network	
MAC	The Ethernet Media Access Control (MAC) address that is assigned to the network interface and used for the device management.
IP Address	The IP address that is assigned to the network interface and used for the device management.
Prefix	The IP network prefix that is assigned to the network interface and used for the device management.
Default	The IP address of the default gateway (if any) that is used for the device management.

Parameter	Description
Gateway	
VLAN	
Management VID	<p>The VLAN ID used to communicate with BTS and CPE for the management purpose.</p> <p>The default value of this parameter is 1, which implies that there is no VLAN in the system.</p> <p>You can set the VID value between 2 and 4094 on the General page. For more details, refer to the Configuring system settings section.</p>
Management VID Priority	The priority value that is set for the management VLAN ID.
VLAN Enabled	<p>Determines whether the VLAN functionality for the BTS and all linked CPEs is enabled.</p> <p>Default value: Disabled</p> <p>For more details, refer to the Configuring system settings section.</p>
Q-in-Q Ether Type	<p>The Ether types for Q-in-Q (802.1ad) and outer tags (S-Tag).</p> <p>Example: 0x88a8</p> <p>You can configure this Ether type using the System > General page of the B1000 UI.</p>
Radio	
Calibration Status	<p>Indicates the unit calibration status.</p> <p>The calibrated status implies that BTS has been tested and calibrated for all the frequency ranges.</p> <p>Note: A production unit showing an uncalibrated or a persistent uncalibrated state indicates a problem that requires factory repair.</p>
Tx State	<p>Specifies the status of transmit control (Tx).</p> <p>This is a read-only parameter. By default, this parameter is enabled.</p> <p>Note: If the engineering keys (used for troubleshooting and support) are enabled, then this parameter displays a message (highlighted in orange) indicating that transmit control is overridden by the Engineering key. For more information about the engineering keys, refer to the Engineering section.</p>



Note

The Power icon () on the top right side of the page, allows you to restart (reboot) B1000 from the UI.

Device

The **Device** page displays information (read-only) about the device identifiers, system reboot, and the boot loader as shown in [Figure 6](#).

Figure 6: The Device page

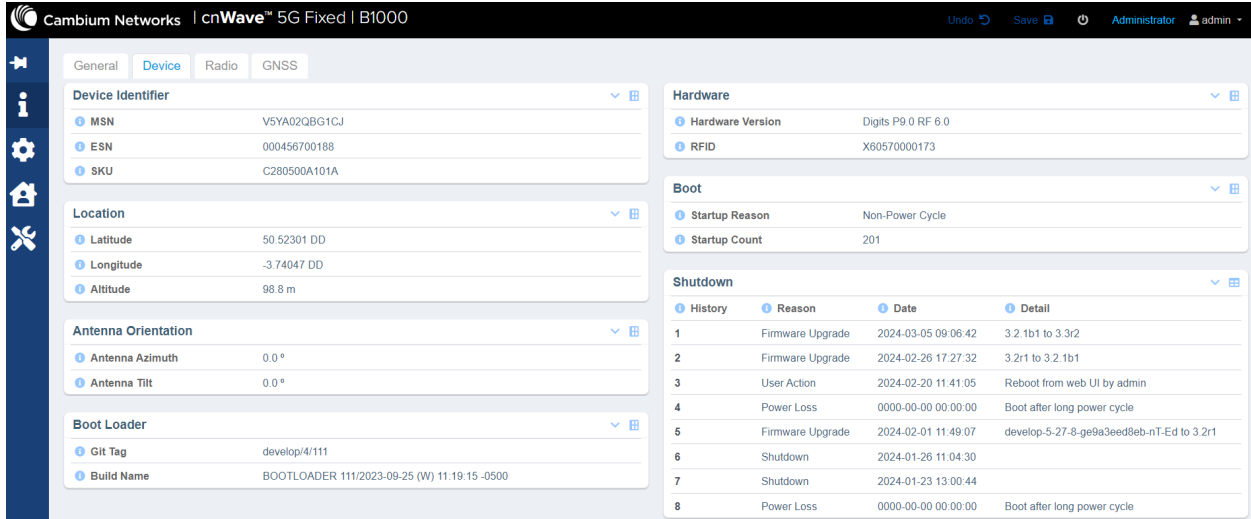


Table 4 lists and describes parameters available on the Device page.

Table 4: Parameters on the Device page

Parameter	Description
Device Identifier	
MSN	Manufacturer Serial Number (MSN) of the device that is used for device identification.
ESN	Electronic Serial Number (ESN) of the device.
SKU	Stock Keeping Unit (SKU) of the device.
Location	
Latitude	Latitude (in DD) of the geographical location where the BTS device is located. Note: Decimal degrees (DD) indicates latitude and longitude geographic coordinates in decimal fractions of a degree. Example: A positive latitude is north of the equator and a negative latitude is south of the equator. A DD to five decimal places is precise to approximately one metre.
Longitude	Longitude (in DD) of the geographical location where the BTS device is located. Example: A positive longitude is east of the Prime Meridian and a negative longitude is west of the Prime Meridian.
Altitude	Altitude (in m) of the geographical location relative to mean sea level (MSL).
Antenna Orientation	
Antenna Azimuth	The direction in azimuth that the BTS is pointing towards. 0.0, 90.0, 180.0, and 270.0 values (in degrees) correspond to magnetic North, East, South, and West, respectively. Note: The radio does not use this value but reports the value to cnMaestro.
Antenna Tilt	The tilt angle (in degrees) of the BTS antenna.

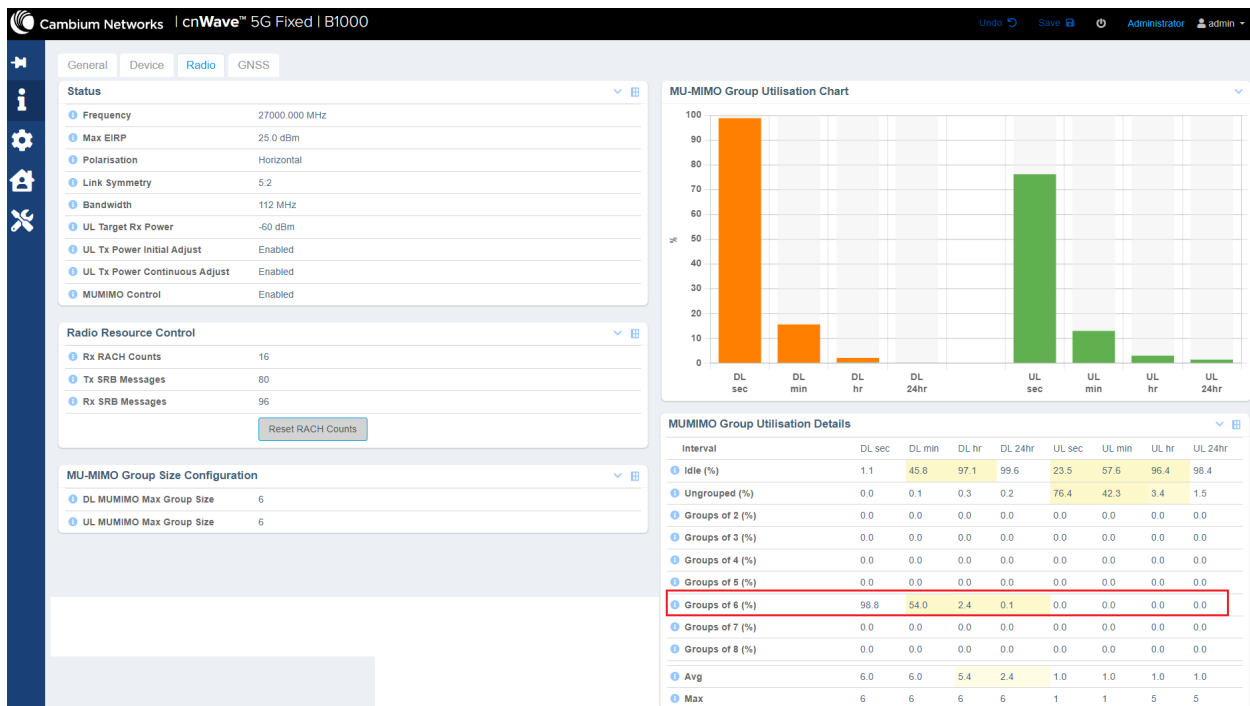
Parameter	Description
	A positive value indicates that the antenna is pointing above the horizon. Note: The radio does not use this value but reports the value to cnMaestro.
Boot Loader	
Git Tag	ID of the software build version.
Build Name	Build name of the BTS software.
Hardware	
Hardware Version	Hardware version of the BTS device.
RFID	The radio frequency (RF) module ID.
Boot	
Startup Reason	Indicates the reason for the previous system reboot. The following reasons are supported: <ul style="list-style-type: none"> • Non-Power Cycle: The device was reset without a power cycle. • Short Power Cycle: Power to the device was briefly interrupted. • Long Power Cycle: Power to the device was interrupted.
Startup Count	Indicates the counter that is incremented each time the device starts up.
Shutdown - Provides details of the boot history.	
History	Index of the boot history. The history for the most recent system reboot is always available in the first row.
Reason	Reasons specified for each boot history. The following boot reasons are supported: <ul style="list-style-type: none"> • Unspecified: The shutdown was not planned (for example, power loss or Watchdog reset). • Shutdown: Shutdown due to a user action. • Firmware Upgrade: A firmware upgrade requiring a reboot to complete. • Configuration Change: A configuration change requiring a reboot to complete. • User Action: A user action requiring a reboot. • Watchdog: A managed shutdown due to a fatal system fault. • Application Fatal: A managed shutdown due to an application managed error. • Application Panic: A managed shutdown due to an application fatal error.

Parameter	Description
Date	Date and time at which the system was rebooted.
Detail	A brief description of the reboot.

Radio

The **Radio** page displays information (read-only) about the key radio settings (as shown in [Figure 7](#)) configured using the **System > Radio** page. For more details about configuring the key radio settings, refer to the [Radio settings](#) section.

Figure 7: The Radio page



In [Figure 7](#), the DL MUMIMO utilisation in groups of six is shown as an example. The utilisation is expressed as the percentage of the available link capacity that has been utilised by the downlink scheduler. The measurement is updated every minute and shows the utilisation for the last second, one minute, one hour, and day (24 hours).

[Table 5](#) lists and describes parameters available on the **Radio** page.

Table 5: Parameters on the Radio page

Parameter	Description
Status	
Frequency	The operating frequency (in MHz) of the radio bearer. For more details on this parameter, refer to Table 10 .
Max EIRP	The maximum Effective Isotropic Radiated Power (EIRP) value in milliwatts (dBm). For more details on this parameter, refer to Table 10 .

Parameter	Description
Polarisation	Determines the antenna polarisation settings. For more details on this parameter, refer to Table 10 .
Link Symmetry	The downlink (DL) or uplink (UL) ratio (symmetry) that is used for controlling the usage of signal slots. For more details on this parameter, refer to Table 10 .
Bandwidth	Indicates the bandwidth (in MHz) of the radio channel spacing. For more details on this parameter, refer to Table 10 .
UL Target Rx Power	The UL target receive power in dBm. For more details on this parameter, refer to Table 10 .
UL Tx Power Initial Adjust	Determines the initial power adjust mode of CPEs. For more details on this parameter, refer to Table 10 .
UL Tx Power Continuous Adjust	Determines the continuous power adjust mode of CPEs. For more details on this parameter, refer to Table 10 .
MUMIMO Control	Determines the Multiple User Multiple Input Multiple Output (MUMIMO) control mode of CPEs. For more details on this parameter, refer to Table 10 .
Radio Resource Control	
Rx RACH Counts	Number of registration requests received on uplink Random Access Channel (RACH). An increase in the number of requests indicates that at least one CPE is requesting to attach to the BTS.
Tx SRB Messages	Number of Signalling Radio Bearer (SRB) request messages that are transmitted by the BTS. An increase in the number of messages indicates that at least the BTS is sending data bearer establishment messages to at least one CPE.
Rx SRB Messages	Number of SRB response messages that are received by the BTS. An increase in the number of messages indicates that at least the BTS is receiving data bearer establishment response messages from at least one CPE.
Reset RACH Counts	An option to reset the Rx RACH count from the Dashboard > Radio page.
MU-MIMO Group Size Configuration	
DL MUMIMO Max Group Size	Maximum size of the downlink Multiple User Multiple Input Multiple Output (MUMIMO) group. This size indicates the number of data streams that can be formed in the downlink direction simultaneously.
UL MUMIMO Max Group Size	Maximum size of the uplink MUMIMO group. This size indicates the number of data streams that can be formed in the uplink direction simultaneously.
MU-MIMO Group Utilisation Chart - This section displays a chart that indicates the percentage of DL and UL MUMIMO group utilisation observed in the last second, minute, one hour, and day (24 hours).	

Parameter	Description
Note: When you place the cursor on the chart, you can view the details of the MUMIMO group utilisation.	
MUMIMO Group Utilisation Details	
Idle (%)	Percentage of idle or management slots observed in the last second, minute, one hour, and day (24 hours).
Ungrouped (%)	Percentage of ungrouped slots observed in the last second, minute, one hour, and day (24 hours).
Groups of 2 (%)	The MUMIMO utilisation (in percentage) for the group size of two observed in the last second, minute, one hour, and day (24 hours).
Groups of 3 (%)	The MUMIMO utilisation (in percentage) for the group size of three observed in the last second, minute, one hour, and day (24 hours).
Groups of 4 (%)	The MUMIMO utilisation (in percentage) for the group size of four observed in the last second, minute, one hour, and day (24 hours).
Groups of 5 (%)	The MUMIMO utilisation (in percentage) for the group size of five observed in the last second, minute, one hour, and day (24 hours).
Groups of 6 (%)	The MUMIMO utilisation (in percentage) for the group size of six observed in the last second, minute, one hour, and day (24 hours).
Groups of 7 (%)	The MUMIMO utilisation (in percentage) for the group size of seven observed in the last second, minute, one hour, and day (24 hours).
Groups of 8 (%)	The MUMIMO utilisation (in percentage) for the group size of eight observed in the last second, minute, one hour, and day (24 hours).
Avg	The MUMIMO utilisation (in percentage) for the average group size observed in the last second, minute, one hour, and day (24 hours).
Max	The MUMIMO utilisation (in percentage) for the maximum group size observed in the last second, minute, one hour, and day (24 hours).

GNSS

The **GNSS** page displays satellite information (read-only) for the BTS device such as number of satellites that are in use, sky view details, and sky map (location of satellites in different directions).

Using this information (as shown in [Figure 8](#)), you can monitor the satellites and ensure the BTS installation in a clear sky for optimal GPS synchronisation.



Note

You can configure GNSS using the **System > Synchronisation** page of the B1000 UI. For more information, refer to the [Synchronisation](#) section.

For information on checking the BTS installation using satellite details, refer to the *cnWave 5G Fixed Planning and Installation Guide*.

Figure 8: The GNSS page

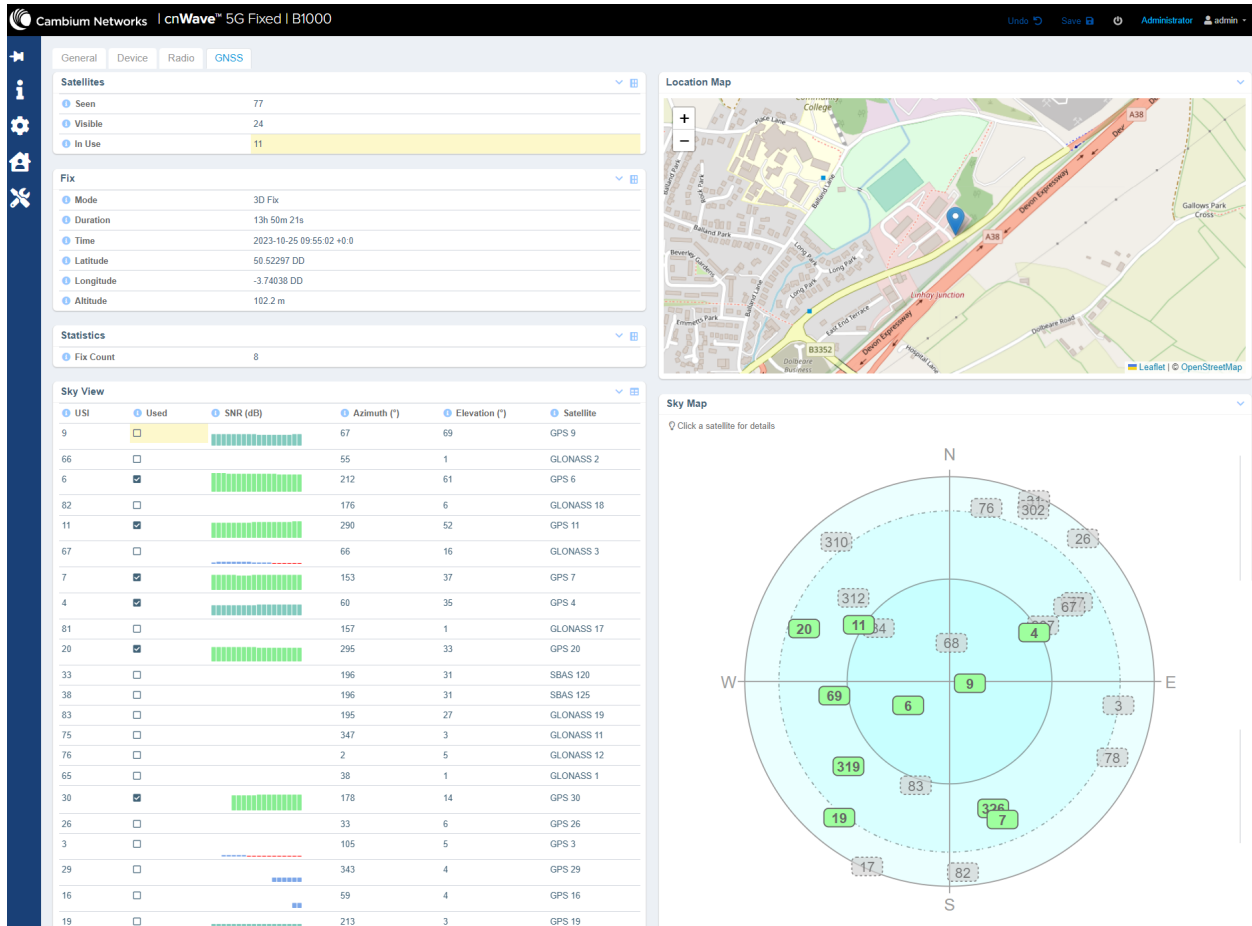


Table 5 lists and describes parameters available on the GNSS page.

Table 6: Parameters on the GNSS page

Parameter	Description
Satellites	
Seen	Total number of individual GNSS satellites that have been detected by this BTS device. This also indicates the number of satellites, which are currently visible or have previously been visible to this device in the last five days. This total number corresponds to the number of rows in the Sky View table. Note: GNSS stands for Global Navigation Satellite System.
Visible	Number of individual GNSS satellites that are currently visible to this BTS device.
In Use	Number of GNSS satellites that are in use by the device to calculate its latitude, longitude and the elevation (with a 3D fix).
Fix	
Mode	Indicates the GPS fix mode.

Parameter	Description
	A 2D fix is sufficient for the calculation of latitude and longitude. A 3D fix is required for the calculation of altitude.
Duration	Indicates the time elapsed since Fix Mode transitioned to or from No Fix (s) . This time duration is presented as a number of days, hours, minutes, or seconds (where only the significant two of these options are displayed).
Time	The GPS reference clock time that is accompanying the latest fix.
Latitude	Latitude (in DD) of the geographical location where the device is located. Note: Decimal degrees (DD) indicates latitude and longitude geographic coordinates in decimal fractions of a degree. Example: A positive latitude is north of the equator and a negative latitude is south of the equator. A DD to five decimal places is precise to approximately one metre.
Longitude	Longitude (in DD) of the geographical location where the device is located. Example: A positive longitude is east of the Prime Meridian and a negative longitude is west of the Prime Meridian. A DD to five decimal places is precise to approximately one metre.
Altitude	Altitude (in m) of the geographical location relative to the mean sea level (MSL).
Statistics	
Fix Count	A count of the number of times a GPS Fix has been achieved since the system start-up. This value increments each time when Fix Mode transitions from No Fix to either 2D Fix or 3D Fix.
Sky View - This section displays the following Space Vehicle (SV) related details for the satellites:	
USI	A Universal Satellite Identifier (USI), which is unique to each SV. For this device, GNSS ID and PRN code are combined to form a USI. Note: The SV timing signal is modulated by a pseudo-random noise (PRN) code, which is unique to each SV within its GNSS system. These PRN code numbers overlap between different systems.
Used	Indicates whether the timing information from this Space Vehicle (SV) has been used to calculate the fix information. This timing information is not used if SNR is too low.
SNR (dB)	The signal-to-noise ratio (SNR) of the timing signal from this SV (in dB). The signal cannot be used if the SNR is too low. A value above 20 is a good SNR.
Azimuth (°)	The compass angle of the SV measured clockwise starting with 0 at due North (°).
Elevation (°)	The elevation angle of the SV relative to the horizontal where 90° is directly above the zenith (°).
Satellite	The GNSS identifier and the SV identifier.

Parameter	Description
Location Map	Displays the location of the device on a map. You can use the map settings to view the location.
Sky Map	Displays the location of satellites on the sky in different directions. Green color indicates the satellites that are in use. When you click on any satellite, this section displays USI, satellite ID, azimuth, elevation, and SNR details for the selected satellite.

Accounts

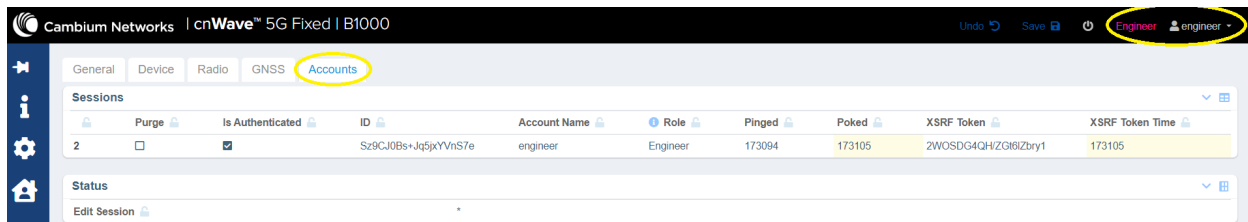


Note

The **Accounts** tab appears only when you log in with an engineer user role. This tab is not visible to other user roles on the B1000 UI.

The **Accounts** page displays information specific to sessions and status of the session, which are used by engineers only. Example: Session related details such as account name, ID, and role. [Figure 9](#) is an example of the Accounts page.

Figure 9: The Accounts page for engineer user roles




Configuring B1000 (BTS)

Using the B1000 UI, you can configure, view, and manage the BTS configurations. This section covers the following topics:

- [Configuring system settings](#)
- [Viewing subscriber data](#)
- [Configuring tools](#)

Configuring system settings

The **System** page in the B1000 UI allows you to configure the required settings for the device such as network, IP addresses of BTS, radio parameters, interfaces, and network services. You must use the **System** icon () to configure, view, and manage the system settings.

The **System** page contains the following tabs:

- [General](#)
- [Management](#)
- [Radio](#)
- [Interfaces](#)
- [CPE Provisioning](#)
- [Synchronisation](#)

General

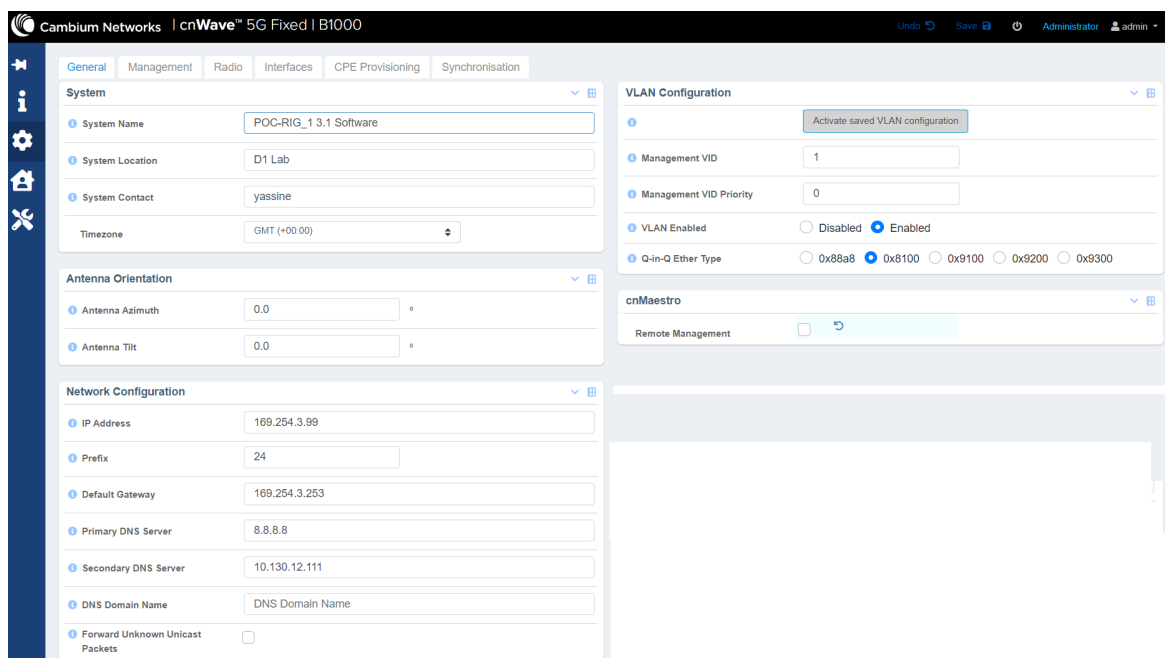
The **General** page allows you to configure generic system settings such as system name, its location, contact details, IP, and other network-related settings.

To access and configure the system settings, perform the following steps:

1. Log on to the B1000 UI (as described in [Accessing the B1000 UI](#)).
The main B1000 dashboard page appears (as shown in [Figure 1](#)).
2. On the left navigation column, click the **System** icon (⚙️).

A system setting-specific page appears, as shown in [Figure 10](#). By default, the **General** tab is selected.

Figure 10: *The System page*



3. Set the values for each parameter, as described in [Table 7](#).

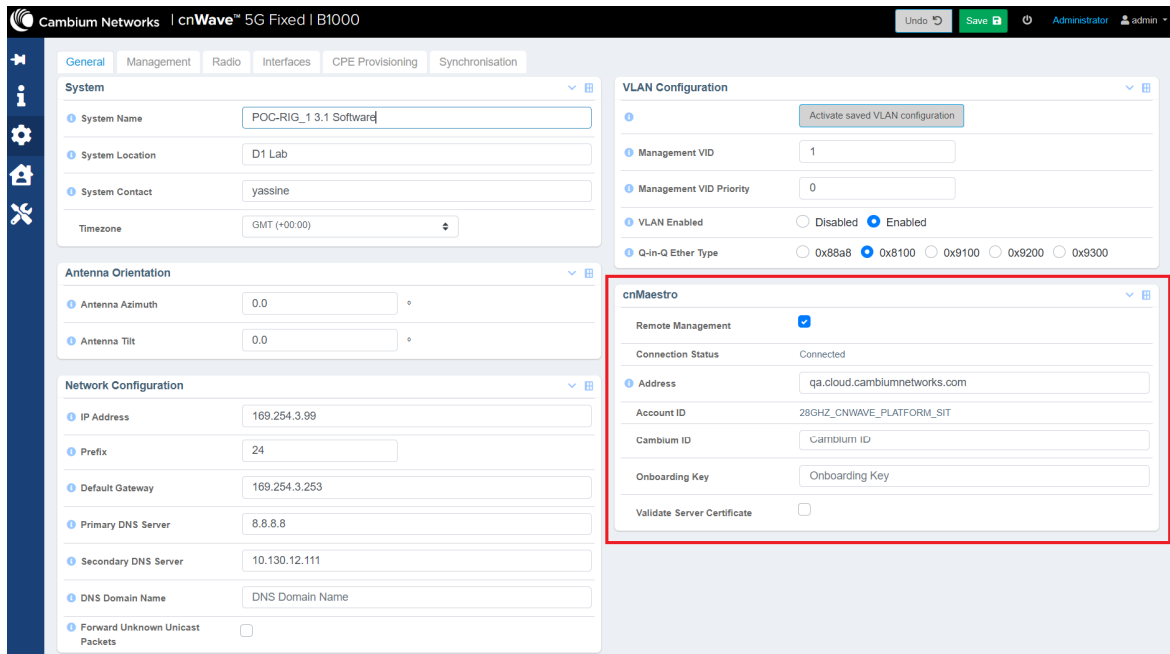
Table 7: List of parameters in the General page

Parameter	Description
System	
System Name	An administratively assigned name of the device. When using DNS, this name must be the device's fully qualified domain name (FQDN). Provide an appropriate name in the text box for the system.
System Location	The physical location of the device node. Provide appropriate location details in the text box.
System Contact	Contact details of the device administrator. Enter appropriate details in the text box.
Timezone	Time zone that you want to set for the system. Select the required time zone from the drop-down list. Example: GMT (+00:00)
Antenna Orientation	
Antenna Azimuth	The direction in azimuth that the BTS is pointing towards. 0.0, 90.0, 180.0, and 270.0 values (in degrees) correspond to magnetic North, East, South, and West, respectively. Note: The radio does not use this value but reports the value to cnMaestro.
Antenna Tilt	The tilt angle (in degrees) of the BTS antenna. A positive value indicates that the antenna is pointing above the horizon. Note: The radio does not use this value but reports the value to cnMaestro.
Network Configuration	
IP Address	The IP address that is assigned to the network interface. This IP address is used for managing the device. Type an appropriate value in the text box.
Prefix	The IP network prefix that is assigned to the network interface. This prefix is used for managing the device. Type an appropriate value in the text box. Example: 24
Default Gateway	The IP address of the default gateway (if any), which is used for managing the device. Type an appropriate value in the text box.
Primary DNS Server	The IP address that is assigned to the primary Domain Name System (DNS) Server (if any). This IP address is used for managing the device. Type an appropriate value in the text box.

Parameter	Description
Secondary DNS Server	<p>The IP address that is assigned to the secondary DNS Server (if any). This IP address is used for managing the device.</p> <p>Type an appropriate value in the text box.</p>
DNS Domain Name	<p>The domain name that is used for configuring the management DNS. This domain name may be concatenated to the DNS names configured for the management interface.</p> <p>Type an appropriate value in the text box.</p>
Forward Unknown Unicast Packets	<p>Determines whether the BTS forwards the Ethernet packets to CPEs on receiving the packet with a unicast destination address.</p> <p>By default, the check box is not selected. This indicates that the BTS does not forward the Ethernet packets to any CPE on receiving the packet with a unicast destination address, which the BTS has not learned.</p> <p>If you select the check box, then the BTS forwards the Ethernet packets to all registered CPEs on receiving the packet with a unicast destination address, which the BTS has not learned.</p>
VLAN Configuration	
Activate saved VLAN configuration	<p>An action that updates the live VLAN configuration for using the currently saved settings unless they are overridden by RADIUS.</p> <p>Note: If you have changed Management VID, then you will lose contact with the device until you make the corresponding changes.</p>
Management VID	<p>The VLAN ID that is used to communicate with BTS and CPE for the management purpose.</p> <p>Default value: 1 - which implies that there is no VLAN in the system.</p> <p>You can set up an ID value between 2 and 4094.</p> <p>Type an appropriate value in the text box.</p> <p>To understand the concept of VLAN, refer to the VLAN section.</p>
Management VID Priority	<p>The priority value that is set for the management VLAN ID.</p>
VLAN Enabled	<p>Determines whether the VLAN functionality for the BTS and all linked CPEs is enabled.</p> <p>Default value: Disabled</p> <p>Select the required option.</p> <p>If you change the value of this parameter, reboot the device for applying the change.</p> <p>Note: If this parameter is disabled, then you cannot configure VLAN-related parameters on the C100 UI (CPE).</p>
Q-in-Q Ether Type	<p>The Ether type values used for Q-in-Q (802.1ad) and outer tag (S-Tag).</p> <p>Following values are supported:</p> <ul style="list-style-type: none"> • 0x88a8

Parameter	Description
	<ul style="list-style-type: none"> • 0x8100 • 0x9100 • 0x9200 • 0x9300 <p>Default value: 0x88a8</p> <p>Select the required Ether type tag.</p> <p>If you change the value of this parameter, reboot the device for applying the change.</p> <p>Note: Generally, the Ether Type field in Ethernet frames is used to specify the protocol or format of the encapsulated data. With Q-in-Q (for instance, where you have an outer VLAN and inner VLAN), the Ether Type is used to distinguish the outer tag and the inner tag. For more information, refer to the Q-in-Q section.</p>
<p>Note: Before enabling cnMaestro in the B1000 UI, ensure that cnMaestro is deployed and configured with a Cambium ID. For more details, refer to the cnMaestro Configuration section.</p>	
<p>cnMaestro</p>	
Remote Management	<p>Determines whether the remote management of the BTS system through cnMaestro X is enabled.</p> <p>Select the check box if you want to manage the BTS system, remotely, through cnMaestro X.</p> <p>When you select the check box, cnMaestro X-specific parameters appear as shown in Figure 11.</p>

Figure 11: *cnMaestro-specific parameters*



Following parameters (as listed in Table 8) appear only if you select the **Remote Management** check box in the **cnMaestro** section:

Table 8: Parameters required for the **cnMaestro** configuration

Parameter	Description
cnMaestro	
Connection Status	<p>Indicates the connection status of the BTS device with the cnMaestro X server.</p> <p>When you select the Remote Management check box, the BTS device tries to connect to the required cnMaestro X server and onboard automatically.</p> <p>During this connecting and onboarding process, this parameter displays the connection status messages, as described:</p> <ul style="list-style-type: none"> When BTS tries to connect to the cnMaestro X server, this parameter displays the status as Connecting. When BTS connects to the cnMaestro X server and waits for an approval to onboard, then this parameter displays the status as Device Approval Pending. When BTS connects to the cnMaestro X server and receives an approval to onboard, this parameter displays the status as Onboarding. When BTS disconnects or cannot connect to the cnMaestro X server, then this parameter displays the status as Disconnected.

Parameter	Description
	<ul style="list-style-type: none"> When BTS connects to the cnMaestro X server and onboards successfully, then this parameter displays the status as Connected.
Address	<p>The IP address or the domain name of the required cnMaestro X server.</p> <p>Type an appropriate address in the text box.</p> <p>Note: The address can be either an IP or URL of the On-Premise cnMaestro.</p>
Account ID	<p>The account ID of the required cnMaestro X server.</p> <p>This is a read-only parameter that displays the value when BTS connects to the required cnMaestro X server.</p>
Cambium ID	<p>The user account ID that is assigned and associated with the cnMaestro X server.</p> <p>You can set a Cambium ID for a user using the Onboard > Settings page of the cnMaestro UI. For more information, refer to the cnMaestro Configuration section.</p> <p>Type an appropriate value in the text box.</p>
Onboarding Key	<p>The license key (or a password) that is set on purchasing the BTS device.</p> <p>You can set the onboarding key using the Onboard > Settings page of the cnMaestro UI. For more information, refer to the cnMaestro Configuration section.</p> <p>Type an appropriate value in the text box.</p>
Validate Server Certificate	<p>Indicates whether a server certificate is installed at the customer site for the validation purpose.</p> <p>Select the check box if the server certificate is installed at the customer site.</p>

- Click **Save** (located at the top right side of the page) to save the configuration changes.

VLAN

A **Virtual Local Area Network (VLAN)** is a networking technology that allows you to segment a physical network into multiple virtual networks. VLANs are primarily used for improving network efficiency, security, and management. Using the VLAN technology, you can perform the following functions:

- Segment a single physical network logically into multiple smaller networks.
- Isolate the traffic.
- Control the broadcast domains.
- Organize devices in a flexible manner and enhance security.
- Add the VLAN tags to the Ethernet frame header by following tagging protocols, such as IEEE 802.1Q.

When data packets move between switches, the VLAN to which the packet belongs must be identified. In such cases, VLAN tagging is helpful.

Q-in-Q

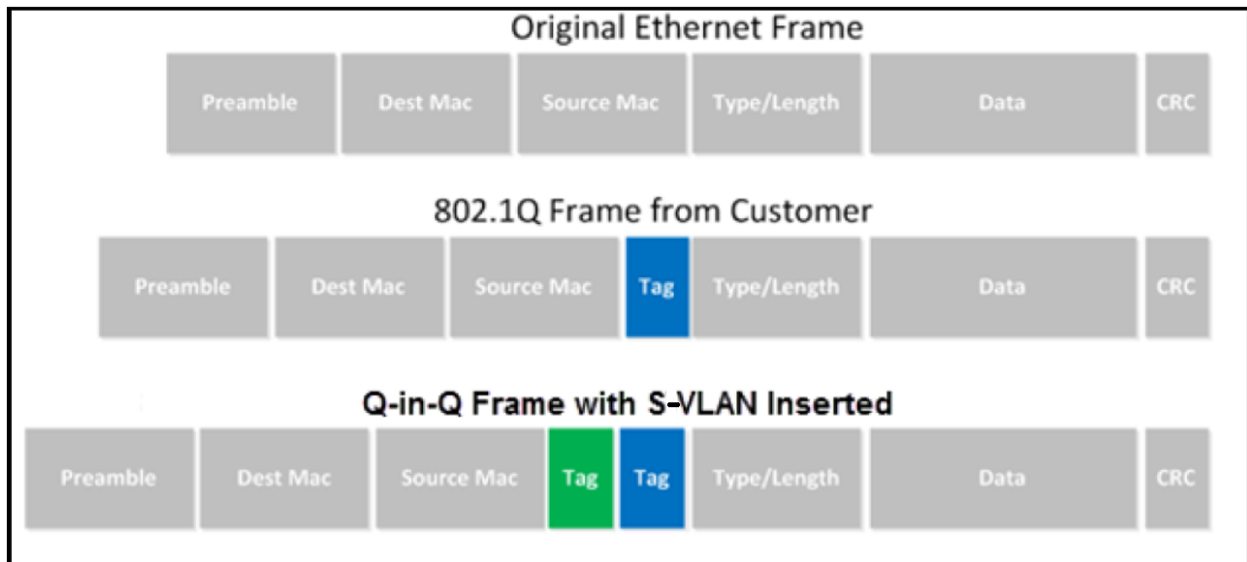
Q-in-Q (also known as double tagging or 802.1ad) is a networking technology that extends the capabilities of VLAN tagging. It's used for addressing some limitations of standard VLAN tagging, especially when dealing with service provider networks or complex network architectures.

In a normal scenario where a standard VLAN setup is using IEEE 802.1Q tagging, each Ethernet frame has a single VLAN tag added to its header. This tag contains information about the VLAN to which the frame belongs. In some scenarios where multiple VLAN domains have to be maintained within a single VLAN network or when passing VLAN traffic through service provider networks, a single VLAN tag might not be sufficient. This is where Q-in-Q is helpful.

Q-in-Q encapsulates a VLAN-tagged frame within another VLAN-tagged frame. This implies that two levels of VLAN tags are used. The outer tag represents a customer's VLAN, while the inner tag represents the VLAN of the service provider's network. This process allows for better isolation and segregation of traffic between different customers or network segments.

Q-in-Q allows service providers to create a Layer 2 Ethernet connection between two customer sites. Service providers can segregate different customers' VLAN traffic on a link (for example, if a customers use overlapping VLAN IDs) or bundle different customer VLANs into a single service VLAN. Data centers can use Q-in-Q to isolate customer traffic within a single site or to enable customer traffic flows between cloud data centers in different geographic locations. Q-in-Q adds a service VLAN tag (802.1Q based) before the customer's 802.1Q VLAN tags.

Figure 12: Q-in-Q Frame format



When a packet travels from a customer VLAN (C-VLAN) to a service provider's or data center VLAN (S-VLAN), another 802.1Q tag for the appropriate S-VLAN is added before the C-VLAN tag. The C-VLAN tag remains and is transmitted through the network. As the packet leaves the S-VLAN in the downstream direction, the S-VLAN 802.1Q tag is removed.

Management

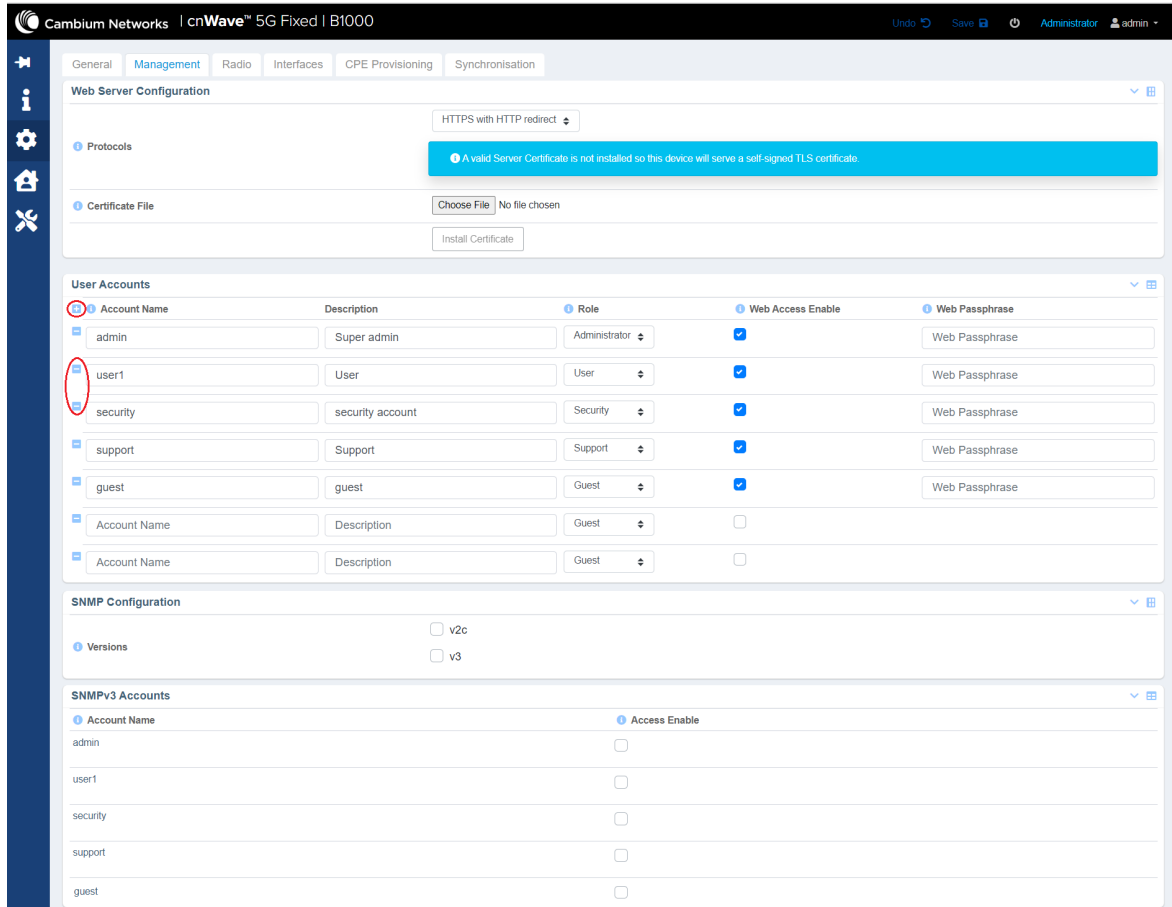
The **Management** page allows you to set multiple user accounts and SNMP configuration related information. This configuration allows the users to manage the B1000 dashboard (web UI) and BTS using SNMP.

To view and configure the management settings, perform the following steps:

1. From the main B1000 dashboard page, navigate to **System > Management**.

The **Management** page appears, as shown in [Figure 13](#).



Figure 13: The Management page



2. Set the values for each parameter, as described in [Table 9](#).

Table 9: List of parameters in the Management page

Parameter	Description
Web Server Configuration	
Protocols	<p>Type of protocol that must be configured for accessing and managing the web UI of BTS.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • HTTP Only: Indicates that only HTTP is available. • HTTPS Only - Indicates that only HTTPS is available.

Parameter	Description
	<ul style="list-style-type: none"> • HTTP and HTTPS: Indicates that both HTTP and HTTPS are available. • HTTPS with HTTP redirect: Indicates that both HTTP and HTTPS are available, but an incoming HTTP connection is automatically redirected to HTTPS. <p>Default value: HTTPS with HTTP redirect</p> <p>Select the required protocol from the drop-down list.</p> <p>Note: Except for the HTTP option, a message is visible for the rest of the options. The message indicates that a valid server certificate is not installed, and the device serves a self-assigned TLS certificate.</p>
Certificate File	<p>An option to browse and upload a certificate file (.PEM) from a location locally. This certificate file must contain a device private key and matching certificate that is signed by the trusted certificate authority (CA).</p> <p>To upload a certificate file (.PEM) from the desired location locally, perform the following steps:</p> <ol style="list-style-type: none"> Click Choose File. <p>A file folder appears.</p> <ol style="list-style-type: none"> Browse the location where you have saved the required certificate file (.PEM) on your machine. Click Open. <p>The certificate file is selected, and the file name appears next to the Choose File button.</p> <ol style="list-style-type: none"> Click Install Certificate. <p>The selected certificate file is installed, which is authenticated and encrypted.</p>
User Accounts	
Account Name	<p>Name of the account used for administering the BTS device. This name must be unique and start with a letter. An account name can contain lower case letters, numbers, and hyphens.</p> <p>Provide an appropriate name in the text box. Example: admin or user1</p> <p>The account name can belong to a guest, an administrator, an engineer, a support team member, or a user. You can add multiple names to the user account using the text boxes.</p> <p>Note: To add a new user account row, use the  icon located beside the Account name parameter (as shown in Figure 13). To delete a user account, use the  icon located beside the corresponding account name.</p>

Parameter	Description
Description	<p>A brief description of the account.</p> <p>Provide a brief description for the user account that you want to add. Example: Super admin</p>
Role	<p>Specifies the role of the user who wants to access the device.</p> <p>This parameter supports the following roles, which have different capabilities and server different functions:</p> <ul style="list-style-type: none"> • Guest: This role has limited, read-only access to the device configuration and status. All fields in the web UI are read-only and some of them are also not available for guest roles. The guest roles have limited SNMP access with a read-only view of MIB-II. • User: This role has limited access to the device configuration and status. Some UI fields are read-only and some fields are not available on the web UI. The user roles cannot change any parameters on the UI. • Administrator: This role has visibility of the device configuration and status. These role can view, configure, and change everything in the UI, but cannot access the sensitive security information. • Security: This role (for example, a security officer) has visibility of the device configuration and status, including sensitive security information. • Support: This role (for example, a support agent) can access diagnostics information for the product support purpose. • Engineer: This role (for example, an engineer) has privileged write access to specific engineering settings and read access to engineering status information. • Factory: This role (for example, a factory operator) has privileged write access to the device customisation settings such as ESN and SKU. <p>Select an appropriate option from the drop-down list.</p>
Web Access Enable	<p>Determines whether the access for web UI of the BTS device is enabled for the selected role.</p> <p>Select the check box if you want to enable the web access for the required user role.</p> <p>Note: Multiple users are allowed to access the UI simultaneously.</p>
Web Passphrase	<p>The passphrase (password) that is assigned to the user role of this account for accessing the web UI.</p> <p>Type an appropriate password in the text box.</p>

Parameter	Description
SNMP Configuration	
Versions	<p>The version of the SNMP protocol that is supported by the agent running on this BTS device.</p> <p>The following SNMP protocol versions are supported:</p> <ul style="list-style-type: none"> • V2c : This is an obsolete version with weak security. • V3 <p>Choose the required check box.</p> <p>Note: A message is visible in this field, providing an option to download the SNMP Management Information Base (MIB) files directly from the device (as shown in Figure 14). Using the SNMP MIB files, you can access VLAN and QoS attributes of the device.</p>
Port	<p>This parameter appears only when you select an SNMP version (V2c or V3).</p> <p>Indicates the network port number assigned to the SNMP agent, which is running on the device.</p> <p>Default value: 161</p> <p>Provide an appropriate value in the text box.</p>
The following parameters appear only when you set V2c in the Versions field, as shown in Figure 14 .	
Read-Only Community	<p>Name of the SNMP V2c community for read-only access to the device.</p> <p>Provide an appropriate value in this text box.</p>
Read/Write Community	<p>Name of the SNMP V2c community for read-write access to the device.</p> <p>Provide an appropriate value in this text box.</p>
SNMPv3 Accounts - This section is applicable only when you set V3 in the Versions field.	
Account Name	<p>The account name that is used for authentication to the BTS device.</p> <p>This is read-only parameter that contains account names, which you added in the User Accounts section.</p>
Access Enable	<p>Determines whether the permission is set for this account name to access the BTS device using SNMPv3 credentials (which are configured in this SNMPv3 Accounts section).</p> <p>Select the check box for the required account name. This setting permits the user account to access the BTS device using SNMP.</p> <p>Note: To modify this parameter, you must enable V3 using the Versions parameter in the SNMP Configuration section.</p>
When you enable the access for the account names using the Access Enable parameter, the following parameters specific to authentication appear (as shown in Figure 15):	

Parameter	Description
Authentication Type	<p>Indicates the authentication type to use.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • None MD5 • SHA1 <p>Select the required option from the drop-down list.</p>
Authentication Passphrase	<p>The authentication passphrase that is assigned to the user role.</p> <p>This passphrase must be same as the one that is set at the SNMP site for this user role.</p> <p>The value of this parameter can contain any combination of ASCII characters. The value must consist of eight characters in length.</p> <p>Type a valid value in the text box.</p>
Privacy Protocol	<p>The protocol that must be used for account privacy.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • None • DES • AES <p>Select the required option from the drop-down list.</p>
Privacy Passphrase	<p>The privacy passphrase that is assigned to the user role. This passphrase must be same as the one that is set at the SNMP site for this user.</p> <p>The value of this parameter can contain any combination of ASCII characters. Also, the value must consist of eight characters in length.</p> <p>Type a valid value in the text box.</p> <p>Note: If you do not provide any privacy passphrase in this text box, then the value is assumed to be same as the authentication passphrase.</p>

When you select V2c in the **Versions** field, Read-Only Community and Read/Write Community parameters appear as shown in [Figure 14](#).

Figure 14: SNMP configuration settings

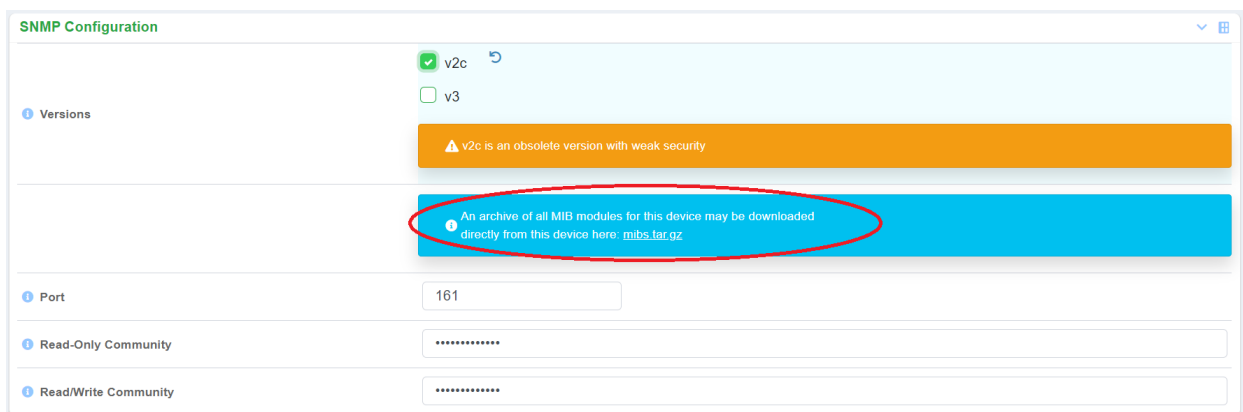
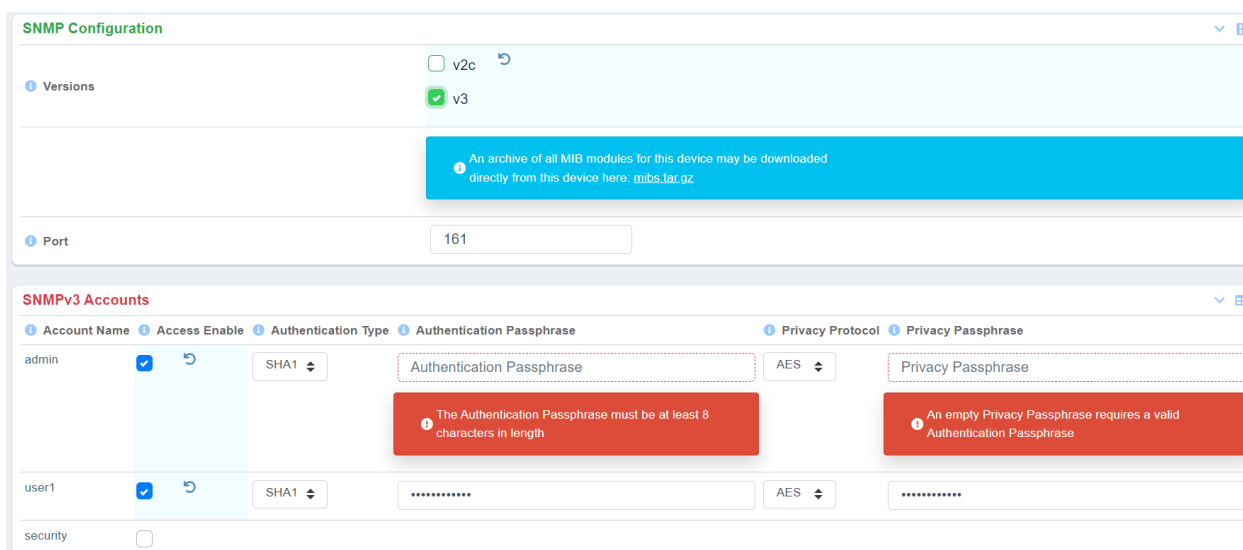


Figure 15 is an example of configuring the **User Accounts** section in the Management page.

Figure 15: The User Accounts section settings



3. Click **Save** to apply the settings.

Radio

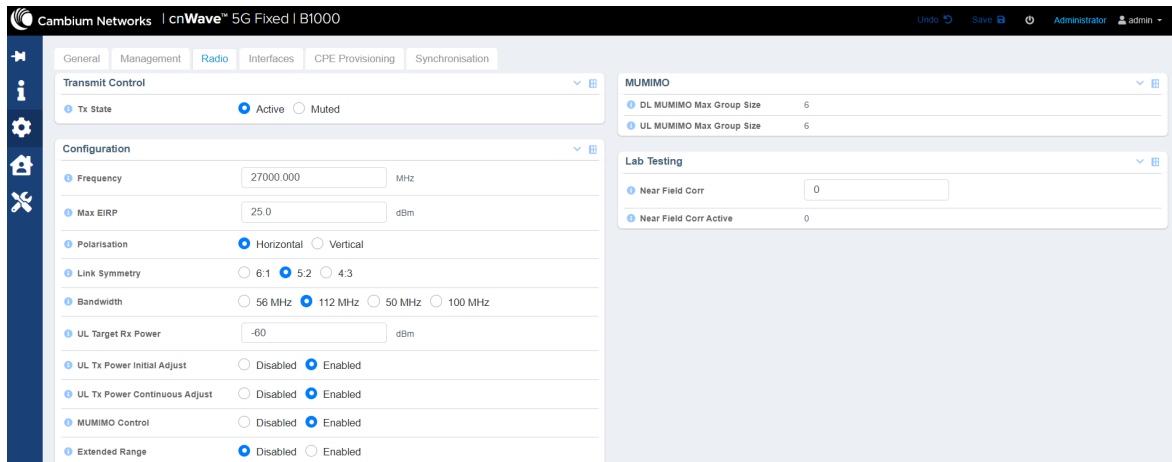
The Radio page allows you to configure transmit control and other radio settings. You can also enable or disable Multi-user Multiple Input Multiple Output (MU-MIMO) and Extended Range parameters.

To view and configure the key radio settings, perform the following steps:

1. From the main B1000 dashboard page, navigate to **System > Radio**.

The **Radio** page appears, as shown in Figure 16.

Figure 16: The Radio page



2. Set the values for each parameter, as described in Table 10.

Table 10: List of parameters in the Radio page

Parameter	Description
Transmit Control	
Tx State	<p>Determines whether the transmitter is active or muted on the BTS.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> Active Muted <p>If you select the Muted option, the transmitter is disabled allowing the BTS to be in a standby mode of operation. Then, all CPEs lose the connection with the BTS.</p> <p>Select the required option.</p>
Configuration	
Frequency	<p>The operating frequency (in MHz) of the radio bearer.</p> <p>Type an appropriate value in the text box.</p> <p>Note: Ensure that the value must be greater than or equal to 24250.000 MHz (or 24.25 GHz).</p>
Max EIRP	<p>The maximum Effective Isotropic Radiated Power (EIRP) value in milliwatts (dBm). This depends on the regulatory conditions of the country of operation.</p> <p>Type an appropriate value in the text box.</p> <p>Note: Ensure that the value is greater than 20 or equal to 48.</p>
Polarisation	<p>Determines the antenna polarisation settings.</p> <p>This parameter supports the following polarisation settings:</p>

Parameter	Description
	<ul style="list-style-type: none"> • Horizontal • Vertical <p>Select the required polarisation for the antenna.</p> <p>When you configure and save the polarisation settings, CPE connects to the BTS using a similar polarization scan feature implemented in the cnWave™ 5G Fixed system. For more information about the CPE's polarisation scan feature, refer to the Radio section.</p> <p>Note: When you change the value of this parameter, the connected CPEs get disconnected and prompts you to reboot the system.</p>
Link Symmetry	<p>The downlink (DL) or uplink (UL) ratio (symmetry) used for controlling the usage of signal slots.</p> <p>BTS and CPE exchange data with each other by using the defined link symmetry.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • 6.1: Indicates 6 DL slots, 1 DL-to-UL transition, 1 UL slots • 5.2: Indicates 5 DL slots, 1 DL-to-UL transition, 2 UL slots • 4.3: Indicates 4 DL slots, 1 DL-to-UL transition, 3 UL slots <p>Select the required symmetry option.</p> <p>Note: When you change the value of this parameter, the Enable Reboot parameter appears.</p>
Bandwidth	<p>Indicates the bandwidth (in MHz) of the radio channel spacing.</p> <p>Set the required bandwidth value.</p> <p>This parameter supports the following values.</p> <ul style="list-style-type: none"> • 50 MHz • 56 MHz • 100 MHz • 112 MHz <p>Select the required bandwidth value.</p> <p>Note: When you change the value of this parameter, the connected CPEs get disconnected and prompts you to reboot the system.</p>
UL Target Rx Power	<p>The UL target receive power in dBm.</p> <p>Type an appropriate value in the text box.</p>

Parameter	Description
	This parameter supports values between -120 and 0. Typically, the best value for this parameter is -50.
UL Tx Power Initial Adjust	<p>Determines the initial power adjust mode of CPEs.</p> <p>This parameter supports the following modes:</p> <ul style="list-style-type: none"> • Disabled • Enabled <p>Select the required mode.</p> <p>Note: In case of first installation, it is recommended to select Enabled.</p>
UL Tx Power Continuous Adjust	<p>Determines the continuous power adjust mode of CPEs.</p> <p>This parameter supports the following modes:</p> <ul style="list-style-type: none"> • Disabled • Enabled <p>Select the required mode.</p> <p>Note: It is recommended to set to Enabled.</p>
MUMIMO Control	<p>Determines the multi user-multiple input and multiple output (MU-MIMO) control mode of CPEs.</p> <p>This parameter supports the following modes:</p> <ul style="list-style-type: none"> • Disabled • Enabled <p>Select the required mode.</p> <p>Note: When you enable this parameter, the B1000 UI provides DL utilisation during the MUMIMO operation.</p>
Extended Range	<p>Determines whether the maximum distance range between a CPE and the BTS is extended up to 10 Km.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Disabled: Indicates that the maximum distance range supported between a CPE and the BTS is five Km. By default, this option is selected. • Enabled: Indicates that the maximum distance range between a CPE and the BTS is extended up to 10 km. <p>Select the required option.</p>
Enable Reboot	<p>An option to reboot the system when you change polarisation, bandwidth, and link symmetry parameters.</p> <p>Select the check box to enable the system reboot.</p>

Parameter	Description
	When the system reboots, the configuration changes that you made are effective.
MUMIMO	
DL MUMIMO Max Group Size	Maximum size of the downlink Multiple User Multiple Input Multiple Output (MUMIMO) group. This size indicates the number of data streams that can be formed in the downlink direction simultaneously.
UL MUMIMO Max Group Size	Maximum size of the uplink MUMIMO group. This size indicates the number of data streams that can be formed in the uplink direction simultaneously.
Lab Testing - This section is controlled by engineering only in lab environments at a short range.	
Near Field Corr	Indicates the phase in degrees of edge columns. This is a one-time setting, and this parameter resets to default on each reboot.
Near Field Corr Active	Indicates the phase in degrees of edge columns. This parameter displays the currently active near field correction setting.

3. Click **Save** to apply the settings.

Interfaces

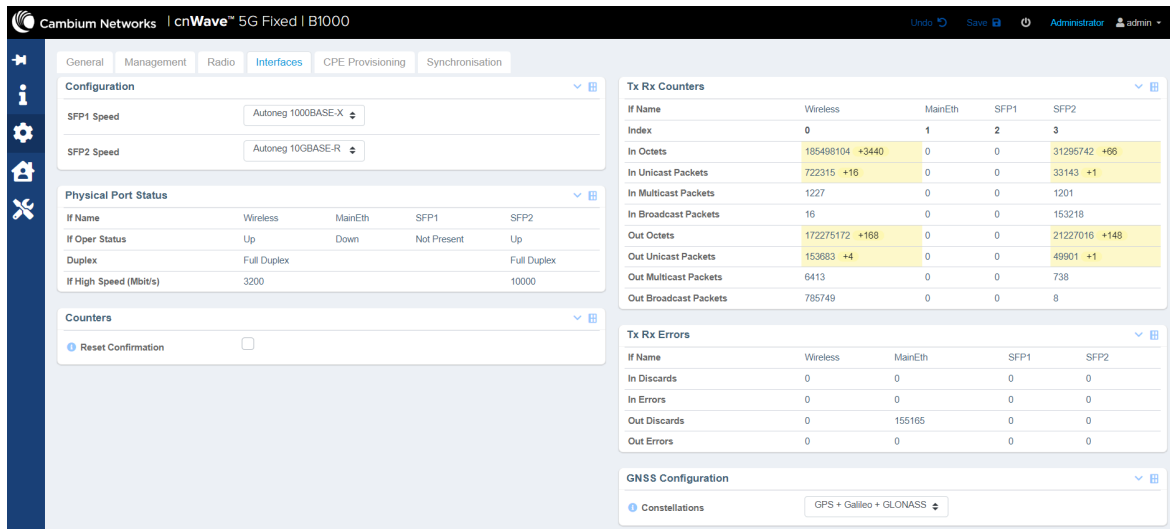
The **Interfaces** page provides statistical information on all the BTS interfaces (for example, Copper or RJ45 MAIN, Small form-factor pluggable (SFP), Global Positioning System (GPS), and Power ports). The page also allows you to configure GNSS.

To view the interface settings, perform the following steps:

1. From the main B1000 dashboard page, navigate to **System > Interfaces**.

The **Interfaces** page appears, as shown in [Figure 17](#).

Figure 17: The Interfaces page



2. View or monitor the data statistics of different interfaces.

Table 11 lists and describes each parameter in the **Interfaces** page.

Table 11: List of interface related parameters

Parameter	Description
Configuration	
SFP1 Speed	<p>The fiber port data speed (1 Gbps).</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Autoneg 1000BASE-X • Forced 1000BASE-X • Autoneg 10GBASE-R <p>Select the required option from the drop-down list.</p>
SFP2 Speed	<p>The fiber port data speed (10 Gbps).</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Autoneg 1000BASE-X • Forced 1000BASE-X • Autoneg 10GBASE-R <p>Select the required option from the drop-down list.</p>
Physical Port Status	
If Oper Status	<p>Indicates the working status (up or down) of wireless, Main Ethernet, or fiber ports for BTS.</p>

Parameter	Description
Duplex	Indicates the capability mode of wireless and Main Ethernet ports to send and receive data.
If High Speed (Mbit/s)	Indicates the data transmission speed of wireless and Main Ethernet ports (in Mbits per second).
Counters	
Reset Confirmation	An option to reset the SNMP MIB-II interface counters. Select the check box if you want to reset. Note: When you select the check box, the Reset Counters button is available. You can use this button to reset the SNMP MIB-II interface counters.
<p>Tx Rx Counters - Applicable to all data ports and wireless.</p> <p>The data report is listed in the following columns:</p> <ul style="list-style-type: none"> • Wireless - Indicates all the data transmitted on the wireless link when it is up. • MainEth - Indicates the data that is entering the Main Ethernet port. • SFP1 - Indicates the data that is entering the SFP1 port. • SFP2 - Indicates the data that is entering the sFP2 port. 	
Index	Index number assigned to each counter column.
In Octets	Number of data bytes received by the BTS from the CPEs.
In Unicast Packets	Number of data packets received by the BTS from a specific CPE.
In Multicast Packets	Number of data packets received by the BTS from specific two or more CPEs.
In Broadcast Packets	Number of data packets received by the BTS from all the connected CPEs.
Out Octets	Number of data bytes sent by the BTS to the CPEs.
Out Unicast Packets	Number of data packets sent by the BTS to a specific CPE.
Out Multicast Packets	Number of data packets sent by the BTS to specific two or more CPEs.
Out Broadcast Packets	Number of data packets sent by the BTS to all the connected CPEs.
<p>Tx Rx Errors - Applicable to all data ports and wireless. The data report is listed in columns, as described in Tx Rx Counters.</p>	
In Discards	Number of incoming data packets discarded by the BTS.
In Errors	Number of incoming data packets that contain errors.
Out Discards	Number of outgoing data packets (from BTS) that are marked or labelled as discarded by the BTS.

Parameter	Description
Out Errors	Number of outgoing data packets (from BTS) that contain errors.
GNSS Configuration	
Constellations	<p>An option to choose the suitable combination of GNSS satellite constellation for the location of this device.</p> <p>Several combinations of GNSS satellite constellations can be used.</p> <p>Select the required combination from the drop-down list.</p> <p>Note: You can monitor the satellites using the GNSS tab on the B1000 dashboard page. For more information, refer to the GNSS section.</p>
<p>Following parameters specific to GNSS configuration are visible only to engineers who log in to the B1000 UI with an engineer user role:</p> <ul style="list-style-type: none"> • Timing only Fix • Anti Jamming Mask • Anti Jamming Threshold 	
GNSS Stats - This section is visible only to engineers.	
Corrupt ZDA Count	Count of the number of times a corrupt ZDA GPS message has been received.
Corrupt GGA Count	Count of the number of times a corrupt GGA GPS message has been received.

CPE Provisioning

The **CPE Provisioning** page provides options to:

- Configure the RADIUS server and other network settings for CPEs.

A RADIUS server is used for remote authentication, provisioning, and configuration of users (CPEs). The cnWave™ 5G Fixed BTS application supports (currently) up to three RADIUS authentication servers. The network RADIUS server contains one entry for each authorized CPE. For each entry, the CPE is identified by its IMSI. For each authorized CPE, the RADIUS contains configuration settings such as IP address, mask, gateway, QoS details, VLAN details, and forwarding of tag and/or untagged traffic.

Using the **CPE Provisioning** page in the B1000 UI, you can configure the RADIUS authentication server for CPEs.

- View and download logs specific to authentication.
- Enable and set the DHCP Option 82 configuration.

You can enable DHCP option 82 (also known as the DHCP relay agent information option) on cnWave™ 5G fixed devices while operating in the L2 bridge mode. This implementation helps to protect the cnWave™ 5G fixed devices against attacks, such as DHCP IP address starvation and spoofing (forging) of IP addresses and MAC addresses. The Option 82 standard This standard defines how the DHCP server can use the location of a DHCP client when assigning IP addresses or other parameters to the client.



Note
 For more information about the DHCP relay agent information option, check <http://tools.ietf.org/html/rfc3046>.

When you enable the DHCP Option 82 feature using the **CPE Provisioning** page, the system intercepts DHCPv4 REQUEST and DISCOVER packets, and inserts the Option 82 fields. When Option 82 is implemented on a switching device, it comprises the following sub options (which are fields in the packet header):

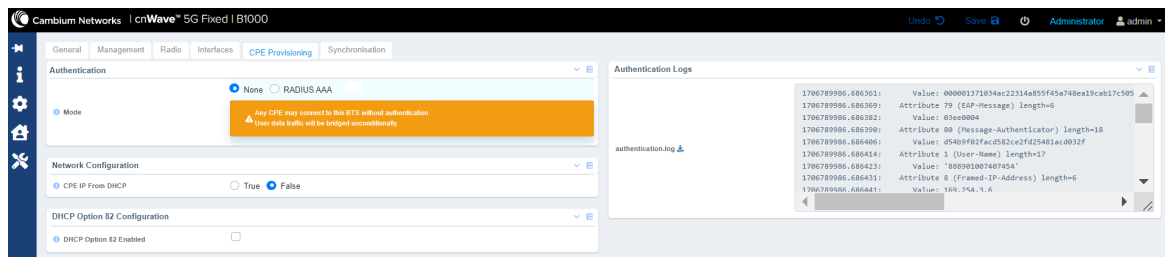
- Circuit ID: Used for identifying the circuit (for example, interface or VLAN) on the node on which the request is received.
- Remote ID: Used for identifying the remote device that sends the DHCP request.

To configure the RADIUS server and other provisioning related parameters, perform the following steps:

1. From the main B1000 dashboard page, navigate to **System > CPE Provisioning**.


The **CPE Provisioning** page appears, as shown in [Figure 18](#) (if RADIUS AAA settings are not set).

Figure 18: The CPE Provisioning page with no RADIUS AAA settings




2. Set the required parameter, as described in [Table 12](#).

Table 12: List of parameters in the CPE Provisioning page

Parameter	Description
Authentication	
Mode	<p>Determines the connection mode of CPEs.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • None: In this mode, any CPE can connect to BTS without authentication. Therefore, user data traffic is bridged unconditionally. By default, this option is selected. • RADIUS AAA: In this mode, CPEs are authenticated by a RADIUS Server (back-end server). User traffic is not bridged until the CPEs are authenticated. <p>Choose the required mode.</p> <p>You can use  to revert to None from the RADIUS AAA mode.</p>
Network Configuration	
CPE IP From DHCP	Determines whether the CPE's IP network configuration is supplied by a DHCP server.

Parameter	Description
	<p>The following values are supported:</p> <ul style="list-style-type: none"> • True: If enabled, the DHCP server supplies the CPE's IP network configuration. • False: If disabled and the Authentication Mode is RADIUS AAA, the configured RADIUS server supplies the CPE's IP network configuration. <p>If disabled and the Authentication Mode is None, the CPE's IP network configuration is set locally at each CPE.</p> <p>Select the required option.</p>
CPE Use Local VLAN Config	<p>Determines whether the CPE uses the local VLAN configuration or the RADIUS-supplied VLAN settings.</p> <p>This parameter is applicable only when you choose RADIUS AAA as the authentication mode.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • True: The CPE uses the local VLAN configuration. This control is applicable when the Authentication Mode is None and this control has no effect as CPEs always install their local VLAN configuration. • False: The CPE installs the RADIUS-supplied VLAN settings. This control is applicable when the Authentication Mode is RADIUS AAA. <p>Select the required option.</p>
CPE Use Local QoS Config	<p>Determines whether the CPE uses the local QoS configuration or the RADIUS-supplied QoS settings.</p> <p>This parameter is applicable only when you choose RADIUS AAA as the authentication mode.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • True: The CPE uses the local QoS configuration. This control is applicable when the Authentication Mode is None and this control has no effect as CPEs always install their local QoS configuration. • False: The CPE installs the RADIUS-supplied QoS settings. This control is applicable when the Authentication Mode is RADIUS AAA. <p>Select the required option.</p>
DHCP Option 82 Configuration	
DHCP Option 82 Enabled	<p>Determines whether the DHCP Option 82 feature is enabled.</p> <p>When this parameter is enabled, the system intercepts DHCPv4 REQUEST and DISCOVER packets, and inserts the Option 82 fields (Circuit ID and Remote ID information) to the packet header.</p>

Parameter	Description
	<p>Select the check box if you want to enable this feature.</p> <p>Note: When you enable the DHCP Option 82 parameter, the following Option 82- specific fields appear (as shown in Figure 19):</p> <ul style="list-style-type: none"> • Circuit ID • Remote ID
Circuit ID	<p>The circuit ID used for identifying the circuit (for example, interface or VLAN) on the node on which the request is received.</p> <p>When the DHCP Option 82 Enabled parameter is enabled, the system inserts this Circuit ID to the packet header.</p> <p>Default value: \$btsMAC\$</p> <p>Note: Use the following wildcards to configure Circuit ID and Remote ID fields:</p> <ul style="list-style-type: none"> • \$btsMAC\$: MAC address of the BTS in ASCII format without colons. \$btsMAC\$ is the default value of the Circuit ID field. • \$cpeMAC\$: MAC address of the CPE in ASCII format without colons. \$cpeMAC\$ is the default value of the Remote ID field. • \$cpeIMSI\$: IMSI of the CPE. • \$btsSystemName\$: The configured system name of the BTS device. • \$cpeSystemName\$: The configured system name of the CPE device. <p>You can combine multiple wildcards. The total length of the option (after replacing wildcards with corresponding values) must not exceed 255 characters. You can also configure a custom string, which must not start with a \$ character.</p>
Remote ID	<p>The remote ID used for identifying the remote device that sends the DHCP request.</p> <p>When the DHCP Option 82 Enabled parameter is enabled, the system inserts this Remote ID to the packet header.</p> <p>Default value: \$cpeMAC\$</p> <p>For information about the supported wildcards, check the Circuit ID field description.</p> <p>Note: You can combine multiple wildcards. The total length of the option (after replacing wildcards with corresponding values) must not exceed 255 characters. You can also configure a custom string, which must not start with a \$ character.</p>
DHCP Option 82 Statistics	<p>Displays the count of DHCP Option 82-specific requests and replies that are received, discarded, and relayed, including other message discards.</p>

Parameter	Description
	<p>This section appears only when you select the DHCP Option 82 Enabled check box.</p> <p>This section displays the following statistics:</p> <ul style="list-style-type: none"> • Requests Received: Number of DHCP requests received by DHCP Option 82 Relay. • Requests Relayed: Number of DHCP requests relayed by DHCP Option 82 Relay. • Requests Discarded: Number of DHCP requests discarded by DHCP Option 82 Relay. • Replies Received: Number of DHCP replies received by DHCP Option 82 Relay. • Replies Relayed: Number of DHCP replies relayed by the DHCP Option 82 Relay. • Replies Discarded: Number of DHCP replies discarded by DHCP Option 82 Relay. • Untrusted Discards: Number of untrusted messages discarded by DHCP Option 82 Relay. • Max Hop Discards: Number of messages discarded by DHCP Option 82 Relay due to exceeded max hop. • Packet Too Big: Number of messages forwarded without relay information by DHCP Option 82 Relay when the relay information exceeded the maximum message size. • Invalid Packet Discards: Number of messages discarded by DHCP Option 82 Relay due to invalid or corrupted packet.
Authentication Logs	
authentication.log	<p>An option to view and download the authentication logs from the UI.</p> <p>Click the  icon to download the authentication logs.</p>
Following parameters appear only when you select the RADIUS AAA mode (as shown in Figure 20):	
RADIUS Configuration	
Accounting	<p>Used for billing purposes.</p> <p>When the CPE authentication mode is set to RADIUS AAA, this RADIUS accounting-specific parameters are enabled in the RADIUS Accounting Server section (as shown in Figure 20).</p> <p>You must set these RADIUS accounting-specific parameters with appropriate values by configuring with at least one primary accounting server (as shown in Figure 20).</p>
RADIUS Accounting Server - This section appears only when you select the Accounting check box.	

Parameter	Description
Role	<p>An option to designate one RADIUS server as primary and the others (if required) as secondary accounting servers.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Primary • Secondary • None <p>Select the required option from the drop-down list.</p> <p>Note: Ensure to configure at least one primary accounting server (as shown in Figure 20).</p>
Inet Address	<p>The IP address assigned to the server that performs RADIUS accounting.</p> <p>Type an appropriate value in the text box.</p>
Port	<p>The network port assigned to the server that performs RADIUS accounting.</p> <p>Default value: 1813</p>
Secret	<p>The shared secret that is used to authenticate transactions between the BTS device and the RADIUS accounting server.</p> <p>Provide an appropriate value in the text box.</p>
RADIUS Authentication Server	
Role	<p>An option to designate one RADIUS server as primary and the others (if required) as secondary authentication servers.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Primary • Secondary • None <p>Select the required value from the drop-down lists.</p>
Inet Address	<p>The IPv4 address of the RADIUS server used for identifying in standard dot notation.</p> <p>Type an appropriate value in the text box.</p>
Port	<p>The destination port used by the device for RADIUS communication, authorization, and configuration.</p> <p>Default value: 1812</p>
Secret	<p>The shared secret value that must contain up to 32 ASCII printable characters. These characters are used to authenticate transactions between the BTS and the RADIUS Authentication Server.</p>

Parameter	Description
	<p>The shared secret(s) must match with those shared secret(s) configured in the RADIUS server(s) <code>clients.conf</code> file. For more information about the <code>clients.conf</code> file settings, refer to An example of configuring an Authentication Server.</p> <p>Provide an appropriate value in the text box.</p>

Figure 19 shown the parameters specific to the DHCP Option 82 configuration.

Figure 19: DHCP Option 82 configuration and statistics

DHCP Option 82 Configuration

1 DHCP Option 82 Enabled
↻

1 Circuit ID

1 Remote ID

DHCP Option 82 Statistics

1 Requests Received	0
1 Requests Relayed	0
1 Requests Discarded	0
1 Replies Received	0
1 Replies Relayed	0
1 Replies Discarded	0
1 Untrusted Discards	0
1 Max Hop Discards	0
1 Packet Too Big	0
1 Invalid Packet Discards	0

Figure 20 is an example of the CPE Provisioning page when the CPE connection mode is set to RADIUS AAA.

Figure 20: Parameters specific to the RADIUS AAA mode

3. Click **Save** to apply the changes.

An example of configuring an Authentication Server

This section explains an example of configuring FreeRADIUS 3.0 as an Authentication Server.

Use the `clients.conf` file to configure the credentials required for enabling the RADIUS server to authenticate the data flow from BTS to CPE or CPE to BTS. The default location of the file is `/etc/freeradius/3.0/` (in a Linux-based PC).

Following is an example of a configuration:

```
client hawking-auth {
    ipaddr = 10.10.10.150/24
    secret = phn_shared_secret
    shortname = hawking_auth
}
```

Dictionary files:

Each dictionary file contains a list of Vendor Specific Attribute (VSAs) and values. The RADIUS server uses these VSAs and values to map descriptive names and on-the-wire data.

Default location of directories: `/etc/freeradius/3.0/`

To add `dictionary.canopy` and `dictionary.hawking`, add the following to the default dictionary file:

```
$INCLUDE dictionary.canopy
$INCLUDE dictionary.hawking
```

Ensure that all dictionaries are available in the default location.

Authorize file:

The authorize file within a FreeRADIUS server determines the network access and configuration for each user.

Default location of the authorize file: `/etc/freeradius/3.0/mods-config/files/`

Figure 21 is a screenshot of a section taken from an authorize file for a CPE with an IMSI - 208920007405736.

Figure 21: A sample configuration for a RADIUS Server

```
# CPEs 1
# Fixed IMSIs
208920007405736          Cleartext-Password := "networks"
    Framed-IP-Address      = "192.168.192.31",      # Assigned CPE Management IP Address
    Framed-IP-Netmask      = 255.255.255.0,          # Assigned Management Netmask
    Cambium-Canopy-Gateway = 10.10.10.254,          # The IP address acting as a gateway
    Cambium-Canopy-VLMGVID = 1,                    # VLAN Management VLAN ID
    Cambium-Canopy-VLSMMGPASS = 0,                  # VLAN SM Management Passthrough
                                                # Enable(1=enable,0=disable)
    Cambium-Canopy-HPENABLE = 0,                    # High Priority Channel Enable (1=enable,0=disable)
    Cambium-Canopy-ULBR    = 3072,                  # Uplink Bit Rate/Sustained Uplink Rate (kbps)
    Cambium-Canopy-ULBL    = 6144,                  # Uplink Bit Limit/Uplink Burst Allocation (kbps)
    Cambium-Canopy-DLBR    = 30720,                 # Downlink Bit Rate/Sustained Downlink Rate (kbps)
    Cambium-Canopy-DLBL    = 61440,                 # Downlink Bit Limit/Downlink Burst Allocation (kbps)
    Cambium-Canopy-BCASTMIR = 100,                  # Broadcast Traffic Maximum Information Rate (kbps)
    Cambium-Canopy-ULMB    = 6144,                  # Max Burst Uplink Rate (kbps)
    Cambium-Canopy-DLMB    = 61440,                 # Max Burst Downlink Rate (kbps)
    Cambium-Canopy-LPULCIR = 1000,                  # Low Priority uplink CIR (kbps)
    Cambium-Canopy-HPULCIR = 100,                   # High Priority uplink CIR (kbps)
    Cambium-Canopy-LPDLCIR = 6000,                  # Low Priority downlink CIR (kbps)
    Cambium-Canopy-HPDLCIR = 100,                   # High Priority downlink CIR (kbps)
    Cambium-Canopy-VLLEARNEN = 0,                   # VLAN Learning Enable (1=enable, 0=disable)
    Cambium-Canopy-VLIGVID = 50,                    # VLAN Ingress VLAN ID
    Cambium-Canopy-VLFRAMES = 1,                     # Frames Types allowed(0=all/1=Tagged/2=Untagged)
    Cambium-Canopy-VLIDSET  = 103,                   # VLAN Membership (1-4094)
    Cambium-Canopy-VLIDSET  = 203                     # VLAN Membership (1-4094)
```

Figure 22 shows various fields that indicate how the CPE uses RADIUS authentication to communicate with BTS.

Figure 22: RADIUS authentication details in the C100 (CPE) dashboard

RADIUS Session	
Phase	Authenticated
Connection	Connected
IP Address	169.254.2.13
IP Netmask	255.255.255.0
Prefix	24
Default Gateway	169.254.2.88
VLMGVID	1
CPE Management VID Pass-through	Disabled
ULBR	0 kbps
ULBL	226144 kbits
DLBR	0 kbps
DLBL	2261440 kbits
LPULCIR	0 kbps
MPULCIR	0 kbps
HPULCIR	0 kbps
UHPULCIR	0 kbps
LPDLCIR	0 kbps
MPDLCIR	0 kbps
HPDLCIR	0 kbps
UHPDLCIR	0 kbps
VLLEARNEN	Enabled
VLGETO	25
VLIGVID	50
VLFRAMES	Tagged Frames
Bts_version	3-1-0-0

Details of RADIUS authentication-specific parameters (as shown in Figure 22) are described in Table 32 (in the [Viewing the C100 \(CPE\) dashboard](#) section).

Synchronisation

The **Synchronisation** page displays parameters required to configure and manage the TDD synchronization by using either an internal GPS or an external GPS source.

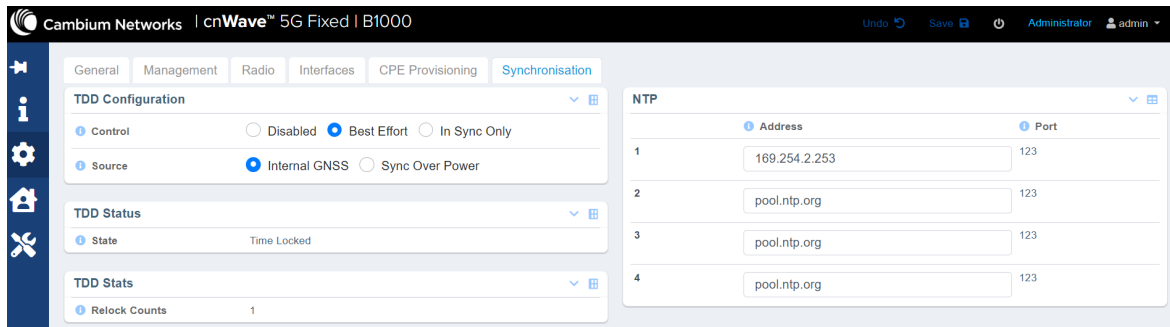
For more information about the TDD Synchronization and how to check the BTS installation using satellite details, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

To view the TDD synchronisation related settings, perform the following steps:

1. From the main B1000 dashboard page, navigate to **System > Synchronisation**.



The **Synchronisation** page appears, as shown in Figure 23.

Figure 23: The Synchronisation page



2. Set the value of each parameter, as described in Table 13.

Table 13: List of parameters in the Synchronisation page


Parameter	Description
TDD Configuration	
Control	<p>Determines the use of internal or external reference signal for TDD synchronisation.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Disabled: Indicates that an internal reference is used. • Best Effort: Indicates that an external one pulse per second (PPS) reference is used. • In Sync Only: Indicates that Tx is turned off when TDD is not in sync. <p>Select the required option. For example, the Best Effort option indicates that the BTS device uses the satellite signal for the reference. Even if all satellites go down, the BTS device uses the reference time for a specific period (for example, 5 minutes) before it loses the reference signal.</p> <p>Note: When you select Best effort or In Sync only, the  icon appears indicating to select the Disabled option.</p>
Source	<p>The sync source for TDD.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Internal GNSS: Indicates that the BTS device uses an integrated GPS as a reference for the operation of TDD. • Sync Over Power: Not supported in this release. <p>Select the required option.</p> <p>Note: When you select Sync Over Power, the  icon appears indicating to select the Internal GNSS option.</p>

Parameter	Description
TDD Status	
State	<p>Indicates the state of TDD synchronisation process, which is reported by TDD Sync state.</p> <p>The BTS device can be synchronised to a one PPS source. The synchronisation process involves detecting of a valid one PPS reference signal, acquiring frequency lock, and then acquiring and maintaining time lock.</p> <p>When a PPS is detected, the frequency is locked and the TDD is synchronized (which is indicated by the Time Locked state).</p> <p>Note: The Local state indicates that the local reference is used, and no PPS input is detected.</p>
TDD Stats	
Relock counts	Indicates the number of times the TDD Sync has entered the locked condition.
<p>NTP - Stands for Network Time Protocol (NTP).</p> <p>A networking protocol that allows you to automatically sync your system date and time with a remote server. NTP sets the reference time and date in the BTS.</p>	
Address	<p>IP address of the NTP server or a Domain Name System (DNS) name (using which the device is configured to use DNS).</p> <p>Enter the required addresses or DNS names of the system in the text boxes.</p>
Port	<p>The network port number that is assigned to the NTP server.</p> <p>Note: The 0 value is not valid.</p>

3. Click **Save** to apply the changes.

Viewing Subscriber (CPE) Data

This section describes how to view the CPE (device) performance for managing subscribers.

The **Subscribers** () icon in the B1000 dashboard page allows you to access the CPE subscriber list and data. Using the B1000 UI, you can view the following subscriber management-related data:

- [CPE status](#)
- [CPE device data](#)
- [CPE radio data](#)
- [CPE configuration data](#)
- [CPE QoS configuration data](#)
- [CPE wireless port statistics](#)
- [CPE Ethernet port statistics](#)

CPE status

The **CPE Status** page provides information about the number of CPEs registered with BTS and their connection state.

To view the CPE status data, perform the following steps:

1. Log on to the B1000 UI, by using the appropriate username and password.

The main B1000 dashboard page appears, as shown in [Figure 2](#).

2. From the left navigation column, select the **Subscribers** (🏠) icon.

A page appears with multiple tabs such as CPE Status, CPE Radio, CPE Auth, CPE Cfg, and CPE Data. By default, the **CPE Status** tab is selected (as shown in [Figure 24](#)).

Figure 24: The CPE Status page

Sys Name	C-RNTI	Registration State	Registration Count	Link Uptime	IP Address	DL Rx Power (dBm)	DL MCS	DL EVM (dB)	UL Rx Power (dBm)	UL MCS	UL EVM (dB)
CPE Release 3.1.1b2	14	Registered	1	4d 23h 29m	169.254.3.2	-43	23	-33.4	-61	23	-27.4
CPE Release 3.1.1b2	15	Registered	1	4d 23h 29m	169.254.3.1	-44	23	-27.1	-61	23	-27.2
CPE Release 3.1.1b2	18	Registered	1	4d 23h 26m	169.254.3.3	-42	23	-30.1	-67	23	-25.0
CPE Release 3.1.1b2	19	Registered	1	4d 23h 25m	169.254.3.4	-43	23	-28.0	-65	23	-25.6
CPE Release 3.1.1b2	20	Registered	1	4d 23h 24m	169.254.3.5	-43	23	-27.8	-65	23	-24.7
CPE Release 3.1.1b2	21	Registered	1	4d 23h 10m	169.254.3.7	-44	23	-30.1	-61	23	-28.3
CPE Release 3.1.1b2	22	Registered	1	4d 23h 8m	169.254.3.8	-41	23	-28.8	-61	23	-28.1
CPE Release 3.1.1b2	24	Registered	1	4d 23h 4m	169.254.3.6	-43	23	-34.0	-61	23	-28.1

Table 14 lists and describes parameters available on the **CPE Status** page.

Table 14: List of CPE Status parameters

Parameter	Description
Summary	
Connected CPEs	Total number of CPEs that are currently connected to BTS.
Registered CPEs	Total number of CPEs that are currently registered and authenticated with BTS.
NTP Synchronized	Indicates whether this device is using NTP to receive time from a reference clock.
CPE Status	
Sys Name	Name of the CPE system.
C-RNTI	<p>Stands for Call-Radio Network Temporary Identifier (C-RNTI).</p> <p>Unique ID used for identifying RRC connection and scheduling. Each CPE device is associated with a dedicated C-RNTI.</p> <p>BTS uses the C-RNTI to:</p>

Parameter	Description
	<ul style="list-style-type: none"> Allocate a CPE with uplink grants, downlink assignments, Physical Downlink Control Channel (PDCCH) order, and others. Differentiate uplink transmissions. Example: Physical Uplink Shared Channel (PUSCH) and Physical Uplink Control Channel (PUCCH) of a CPE from others. <p>In addition, a CPE promotes a temporary C-RNTI to permanent C-RNTI (if the CPE does not have a C-RNTI already) on completing the connection-based RFA procedure successfully.</p> <p>Note: The RNTI is allocated by the BTS on the connection of a CPE. A CPE might be allocated with a different RNTI each time whenever it connects.</p> <p>The RNTI is released when a CPE disconnects from the BTS. RNTI uniquely identifies a CPE connected to a given BTS or sector.</p>
Registration State	<p>Indicates whether the CPE has made any progress to enter to the network.</p> <p>This parameter supports the following device transition states:</p> <ul style="list-style-type: none"> Down - Indicates that the device is yet to attach to a BTS. Attaching - Indicates the device has attached to the BTS radio. Authenticating - Indicates the device is authenticating (using Radius) with the BTS. Configuring - Indicates that the CPE is being configured. Registered - Indicates that the CPE is ready to pass user traffic.
Registration Count	<p>Number of times that the CPE has successfully registered with BTS.</p> <p>The value of this parameter is reset to 0 when the system starts up.</p>
Link Uptime	<p>Time period (in seconds) at which the last successful registration of the CPE found with BTS.</p>
IP Address	<p>The IP address that is assigned to the network interface. This IP address is used for managing the device.</p> <p>Note:</p>
DL Rx Power (dBm)	<p>The downlink received signal power (in dBm).</p>
DL MCS	<p>The Modulation and Coding Scheme (MCS) index value of the downlink.</p> <p>For more information about MCS, refer to the Modulation section.</p>
DL EVM (dB)	<p>The EVM value (in dB) of the downlink.</p>
UL Rx Power (dBm)	<p>The uplink received signal power (in dBm).</p>
UL MCS	<p>The MCS index value of the uplink.</p> <p>For more information about MCS, refer to the Modulation section.</p>

Parameter	Description
UL EVM (dB)	The EVM value (in dB) of the uplink.
Following parameters are visible only to engineers who log in to the B1000 with an engineer user role:	
DL SNR (dB)	The downlink SNR (in dB). Note: SNR stands for signal-to-noise ratio.
UL SNR (dB)	The uplink SNR (in dB).

CPE device data

The **CPE Device** page provides information about the hardware device (CPE) that is connected to the BTS.

To view the CPE device data, perform the following steps:

1. From the left navigation column in the B1000 dashboard, navigate to **Subscribers < CPE Device**.

The **CPE Device** page appears, as shown in [Figure 25](#).

Figure 25: The CPE Device page

The screenshot shows the Cambium Networks B1000 dashboard. The top navigation bar includes 'CPE Status', 'CPE Device', 'CPE Radio Status', 'CPE Ctg', 'CPE QoS', 'CPE Wireless Port Stats', and 'CPE Ethernet Port Stats'. The main content area is titled 'CPE Device' and contains a table with the following data:

Sys Name	IMSI	MSN	ESN	Release Name	SKU	Drop	Reset Network Counters
CPE Release 3.1.1b2	888901007406344	V5YA01SP4QWW	000456710308	3.1.1b2	C280500C001A	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CPE Release 3.1.1b2	888901007406869	V5YA02J5X411	000456710515	3.1.1b2	C280500C001A	<input type="checkbox"/>	<input type="checkbox"/>
CPE Release 3.1.1b2	888901007406429	V5YA01PQKV2W	00045671035D	3.1.1b2	C280500C001A	<input type="checkbox"/>	<input type="checkbox"/>
CPE Release 3.1.1b2	888901007407454	V5YG01GK6DZ	0004567113F0	3.1.1b2	C280500C001A	<input type="checkbox"/>	<input type="checkbox"/>
CPE Release 3.1.1b2	888901007406893	V5YA026678KB	00045671052D	3.1.1b2	C280500C001A	<input type="checkbox"/>	<input type="checkbox"/>
CPE Release 3.1.1b2	888901007406841	V5YA01XDV62D	0004567104F9	3.1.1b3	C280500C001A	<input type="checkbox"/>	<input type="checkbox"/>
CPE Release 3.1.1b2	888901007406574	V5YA01WVRXJ4	0004567103EE	3.1.1b2	C280500C001A	<input type="checkbox"/>	<input type="checkbox"/>

Below the table is a 'Control' section with the following buttons:

- Drop Selected Sessions
- Drop All Sessions
- Reset Selected CPE Network Counters
- Reset All CPE Network Counters

2. View the data of CPE device parameters, as described in [Table 15](#).

Table 15: List of CPE device parameters

Parameter	Description
Sys Name	Name of the CPE system.
IMSI	Unique number used for identifying a subscriber (CPE user) in a cellular network. Each subscriber is associated with a unique IMSI.
MSN	MSN of the device.
ESN	ESN of the device.
Release Name	The release version of the embedded software running on the CPE

Parameter	Description
	device.
SKU	SKU of the CPE device.
Drop	An option to drop the required CPE session from the B1000 UI. If you want to drop a CPE session, select the corresponding check box and click Drop Selected Sessions . The selected CPE session is dropped and there is no need for system reboot. If you want to drop all the CPE sessions, click Drop All Sessions .
Reset Network Counters	An option to reset the required CPE network counters from the B1000 UI. If you want to drop a CPE network counter, select the corresponding check box and click Reset Selected CPE Network Counters . The selected CPE network counter is reset and there is no need for system reboot. If you want to reset all the CPE network counters, click Reset All CPE Network Counters .

CPE radio data

The **CPE Radio Status** page provides information that you can use to troubleshoot any issues with the radio link-related parameters at a deployment site.

To view the data of CPE radios, perform the following steps:

1. From the left navigation column in the B1000 dashboard, navigate to **Subscribers > CPE Radio Status**.

The **CPE Radio Status** page appears, as shown in [Figure 26](#).

Figure 26: *The CPE Radio Status page*

Sys Name	DL Rx Power (dBm)	DL EVM (dB)	DL MCS	DL Backoff (dB)	DL Spatial Frequency	DL Channel Distortion (dB)	DL Sounding State	Current EIRP (dBm)	UL Rx Power (dBm)	UL EVM (dB)	UL MCS	UL Backoff (dB)	UL Spatial Frequency	UL Channel Distortion (dB)	UL Sounding State	Range (km)	Alignment Active
CPE Release 3.1.1b2	-49	-28.1	23	10	517	-15.1	Tracking	15	-65	-25.5	23	4	514	-18.7	Tracking	0.01	<input type="checkbox"/>
CPE Release 3.1.1b2	-48	-32.5	23	11	891	-16.4	Tracking	14	-65	-25.7	23	3	892	-16.9	Tracking	0.02	<input type="checkbox"/>
CPE Release 3.1.1b2	-48	-31.8	23	11	277	-16.3	Tracking	17	-64	-25.3	23	5	280	-17.4	Tracking	0.02	<input type="checkbox"/>
CPE Release 3.1.1b2	-47	-31.9	23	10	759	-18.2	Tracking	18	-64	-25.7	23	5	757	-20.7	Tracking	0.02	<input type="checkbox"/>
CPE Release 3.1.1b2	-51	-32.4	23	8	636	-15.2	Tracking	18	-63	-25.6	23	5	633	-19.7	Tracking	0.01	<input type="checkbox"/>
CPE Release 3.1.1b2	-50	-31.5	23	9	395	-17.4	Tracking	18	-64	-26.0	23	4	397	-18.0	Tracking	0.02	<input type="checkbox"/>
CPE Release 3.1.1b2	-48	-30.4	23	11	1020	-16.9	Tracking	12	-63	-25.8	23	5	1020	-19.7	Tracking	0.01	<input type="checkbox"/>

2. View the data of CPE radio parameters, as described in [Table 16](#).

Table 16: List of CPE radio parameters

Parameter	Description
Sys Name	Name of the CPE system.
DL Rx Power (dBm)	The downlink received signal power (in dBm).
DL EVM (dB)	The EVM value (in dB) of the downlink.
DL MCS	The MCS index value of the downlink. For more information about MCS, refer to the Modulation section.
DL Backoff (dB)	Indicates the amount (in dB) of power backoff for the downlink. This is the amount by which the BTS is currently reducing its power from the maximum configured EIRP when transmitting to the CPE. The BTS uses the greatest backoff that it can achieve while still maintaining the downlink throughput required by the CPE. Note: Backing off the BTS transmit power means that the power allocation can be maximized for the CPE and also for minimizing interference.
DL Spatial Frequency	Indicates the downlink spatial frequency. Spatial frequency is the plane advance of the wavefront from one antenna column to the next, which is caused by an angle at which the wavefront impinges on the array. This frequency is represented in integer units, with 1024 equating to 360 degrees per column. The 2048 value signifies a spatial frequency that is unknown or invalid. Note: For more information on how the spatial frequency is calculated, refer to the Spatial frequency versus azimuth section.
DL Channel Distortion (dB)	Value (in dB) that indicates the distortion (or degraded) length of the downlink Multiple Input Multiple Output (MIMO) channel, with respect to a perfect state. Note: Values that are less than -10 are considered good values.
DL Sounding State	The current sounding state of the downlink MIMO channel. An over-the-air continuous sounding mechanism is used to access the MIMO channel state. This parameter supports the following values: <ul style="list-style-type: none"> • ASSESSING • TRACKING
Current EIRP (dBm)	The current Effective Isotropic Radiated Power (EIRP) in dBm.
UL Rx Power (dBm)	The uplink received signal power (in dBm).
UL EVM (dB)	The EVM value (in dB) of the uplink.
UL MCS	The MCS index value of the uplink. For more information about MCS, refer to the Modulation section.

Parameter	Description
UL Backoff (dB)	Indicates the amount (in dB) of power backoff for the uplink. The Tx Power is reduced if there is a link budget in the top modulation mode for improving spectral efficiency.
UL Spatial Frequency	Indicates the uplink spatial frequency. Spatial frequency is the plane advance of the wavefront from one antenna column to the next, which is caused by an angle at which the wavefront impinges on the array. This frequency is represented in integer units, with 1024 equating to 360 degrees per column. The 2048 value signifies a spatial frequency that is unknown or invalid.
UL Channel Distortion (dB)	Value (in dB) that indicates the distortion (or degraded) length of the uplink MIMO channel, with respect to a perfect state. Note: Values that are less than -10 are considered as the good values.
UL Sounding State	The current sounding state of the uplink MIMO channel. An over-the-air continuous sounding mechanism is used to access the MIMO channel state. This parameter supports the following values: <ul style="list-style-type: none"> • ASSESSING • TRACKING
Range (Km)	Value (in kilometers) that indicates the measured distance between BTS and CPE.
Alignment Active	Determines whether the antenna alignment mode is active. This parameter supports the following options: <ul style="list-style-type: none"> • if the check box is selected, then it implies that the antenna alignment mode is active. • if the check box is not selected, then it implies that the antenna alignment mode is not active.

Modulation

The Modulation and Coding Scheme (MCS) index values can be used in conjunction with the channel width values. This usage allows you to instantly calculate the available data rate of wireless hardware.

MCS depends on the quality of radio signals in a wireless link. If the signal quality is good, then the higher MCS is obtained. Bad signal quality results in lower MCS, which means that less useful data can be transmitted within a symbol. In other words, MCS depends on the Block Error Rate (BLER).

Table 17 contains aggregate throughputs for each MCS mode and the Line of Sight (LoS)-specific theoretical ranges for the cnWave™ 5G Fixed products.

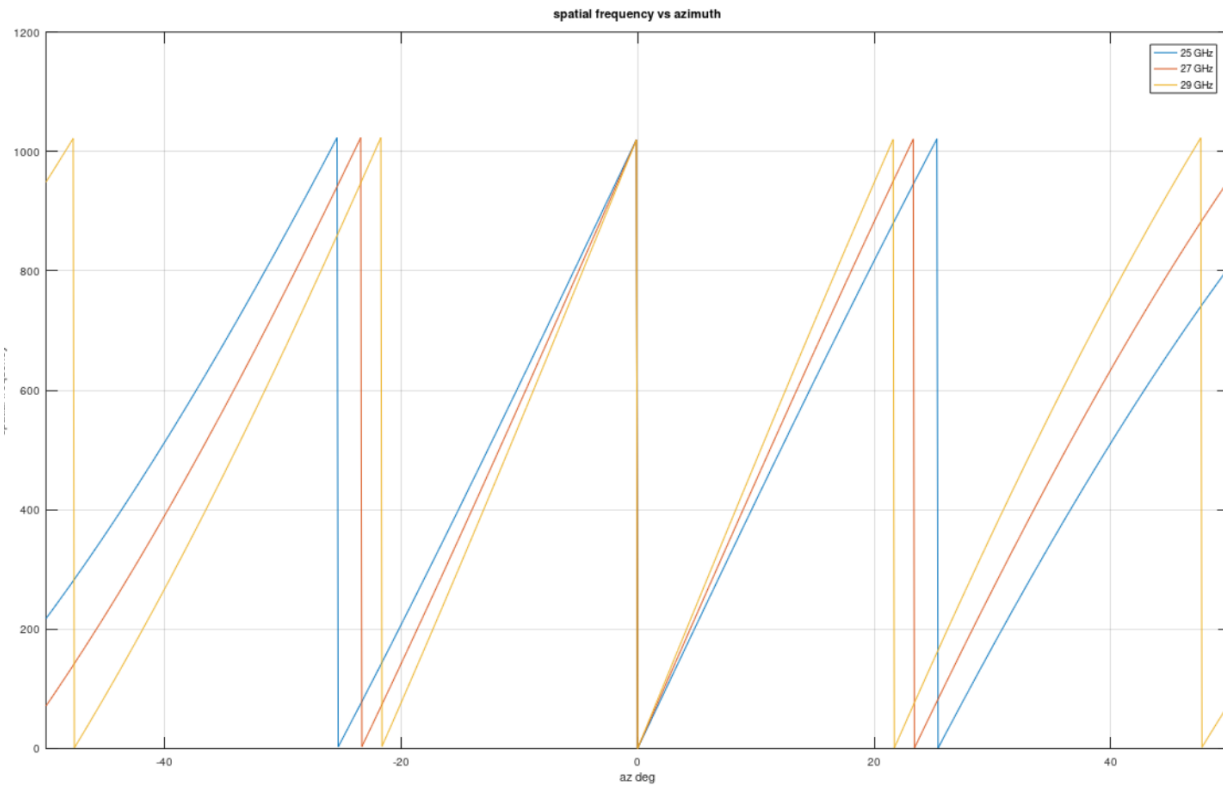
Table 17: MCS Modes and cnWave™ 5G Fixed throughputs

MCS Mode	Aggregate throughput (in Mbps)	
	BW=112 MHz	BW=56 MHz
MCS 24	-	212.9
MCS 23	408.0	
MCS 22	390.3	195.1
MCS 21	372.6	
MCS 20	354.8	177.4
MCS 19	337.1	
MCS 18	319.3	159.7
MCS 17	301.6	
MCS 16	283.9	141.9
MCS 15	266.1	
MCS 14	248.4	124.2
MCS 13	230.6	
MCS 12	212.9	106.4
MCS 11	195.1	
MCS 10	177.4	88.7
MCS 09	159.7	
MCS 08	141.9	71.0
MCS 07	124.2	
MCS 06	106.4	53.2

Spatial frequency versus azimuth

The nominal column spacing of the production Hawking BTS is 28 minutes. The calibration of the digital beamformer of a BTS associates a spatial frequency of 0 with a plane wave front on boresight. This results in the following idealized spatial versus azimuth (as shown in [Figure 27](#)).

Figure 27: Spatial frequency versus azimuth



Assuming a plane wave front incident on the BTS antenna array, the spatial frequency is a measure of the average phase difference of the front between adjacent columns. For a phase difference of $0 \leq \text{Ang} < 360$ degrees, the spatial frequency is reported as $(1024 \times \text{Ang}/360 \text{ degrees})$.

Near boresight, grating lobes appear every ~ 24 degrees. For MU-MIMO grouping, the minimum CPE spatial frequency separation is 128 and the minimum azimuth separation is approximately the grating lobe separation or columns. That is, ~ 3 degrees and columns = 8.

CPE configuration data

The **CPE Cfg** page provides information about the CPEs names and other network configuration-related data of connected and registered CPEs (subscribers).

To view the configuration data of CPEs, perform the following steps:

1. From the left navigation column in the B1000 dashboard, navigate to **Subscribers > CPE Cfg**.

The **CPE Cfg** page appears, as shown in Figure 28.

Figure 28: The CPE Cfg page

Sys Name	IP Address	IP Netmask	Default Gateway	VLMGVID	CPE Management VID Pass-through	VLLEARNEN	VLAGETO	VLIGVID	VLFRAMES
CPE Release 3.1.1b2	169.254.3.8	255.255.255.0	169.254.3.99	1	Enabled	25	50	Tagged Frames	
CPE Release 3.1.1b2	169.254.3.5	255.255.255.0	169.254.3.99	1	Disabled	Enabled	25	50	Tagged Frames
CPE Release 3.1.1b2	169.254.3.2	255.255.255.0	169.254.3.99	1	Disabled	Enabled	25	50	Tagged Frames
CPE Release 3.1.1b2	169.254.3.6	255.255.255.0	169.254.3.99	1	Disabled	Enabled	25	50	Tagged Frames
CPE Release 3.1.1b2	169.254.3.7	255.255.255.0	169.254.3.99	1	Disabled	Enabled	25	50	Tagged Frames
CPE Release 3.1.1b2	169.254.3.1	255.255.255.0	169.254.3.99	1	Disabled	Enabled	25	50	Tagged Frames
CPE Release 3.1.1b2	169.254.3.4	255.255.255.0	169.254.3.99	1	Disabled	Enabled	25	50	Tagged Frames

2. View the configuration data of CPEs, as described in [Table 18](#).

Table 18: List of CPE configuration parameters

Parameter	Description
Sys Name	Name of the CPE system.
IP Address	The IP address that is assigned to the network interface. This IP address is used for managing the device.
IP Netmask	The netmask that is corresponding to the IP address of the CPE. This netmask IP address is used for the device management.
Default Gateway	The IP address of a system (computer) in the current network that acts as a gateway. The IP address of the default gateway (if any) is used for managing the subscriber data service.
VLMGVID	VID that is used to communicate with BTS and CPE for the management purpose.
CPE Management VID Pass-through	Determines whether the Management VID traffic (VLMGVID) is allowed to or from the CPE wired interface. Default value: Enabled Note: You can configure this parameter using the System > General page of C100 UI.
VLLLEARNEN	Determines whether the CPE must add the VLAN IDs (VIDs) of upstream frames to the VID table. The parameter supports the following values: <ul style="list-style-type: none"> • Enabled: Indicates that the CPE must add the VIDs to the VID table. • Disabled: Indicates that the CPE must not add the VIDs to the VID table. Default value: Enabled Note: The CPE drops frames with VIDs that are not stored in the VID table.
VLGETO	The period (in minutes) during which the CPE must dynamically keep learning about VIDs. This parameter supports values ranging from 5 to 1440 (in minutes). Default value: 25 (in minutes) You can configure this parameter using the System > General page of C100 UI. Note: VIDs that you set for the Untagged Ingress VID and Management VID parameters do not time out.
VLIGVID	The VID that is used for untagged frames. This VID corresponds either to the Q-tag for 802.1Q frames (if VLAN Port Type is Q) or the C-tag for 802.1ad frames (if VLAN Port Type is Q-in-Q).

Parameter	Description
VLFRAMES	Type of arriving frames to which the CPE must tag using the VID (which is set in the Untagged Ingress VID parameter). Default value: All frames

CPE QoS configuration data

The **CPE QOS** page provides information about uplink and downlink related configuration data used for managing services of CPEs.

To view the quality of service (QoS)-specific configuration data of CPEs, perform the following steps:

1. From the left navigation column in the B1000 dashboard, navigate to **Subscribers > CPE QOS**.

The **CPE QOS** page appears, as shown in [Figure 29](#).

Figure 29: The CPE QOS page

Sys Name	ULBR (kbps)	ULBL (kbits)	DLBR (kbps)	DLBL (kbits)	LPULCIR (kbps)	MPULCIR (kbps)	HPULCIR (kbps)	UHPULCIR (kbps)	LPDLCIR (kbps)	MPDLCIR (kbps)	HPDLCIR (kbps)	UHPDLCIR (kbps)
CPE Release 3.1.1b2	0	0	0	0	0	0	0	0	0	0	0	0
CPE Release 3.1.1b2	0	0	0	0	0	0	0	0	0	0	0	0
CPE Release 3.1.1b2	0	0	0	0	3500	6500	12500	15000	5000	10000	15000	20000
CPE Release 3.1.1b2	0	0	0	0	0	0	0	0	0	0	0	0
CPE Release 3.1.1b2	0	0	0	0	0	0	0	0	0	0	0	0
CPE Release 3.1.1b2	0	0	0	0	2500	5000	10000	15000	10000	20000	30000	40000
CPE Release 3.1.1b2	0	0	0	0	4500	75000	10500	13500	20000	25000	30000	35000

2. View the QoS configuration data of CPEs, as described in [Table 19](#).

Table 19: List of parameters in the CPE QoS page

Parameter	Description
Sys Name	Name of the CPE system.
ULBR (kbps)	The uplink bit rate or sustained uplink rate (in kbps) at which each CPE has registered with the BTS. The BTS is replenished with credits for transmission.
ULBL (kbits)	The uplink bit limit or uplink burst allocation (in kbits). The maximum amount of data that each CPE is allowed to transmit before being recharged at the sustained uplink data rate (in kbps).
DLBR (kbps)	The downlink bit rate or sustained downlink rate (in kbps) at which the BTS is replenished with credits (tokens) for transmission to each of the CPEs in its sector.
DLBL (kbits)	The downlink bit limit or downlink burst allocation (in kbits). The maximum amount of data that the BTS is allowed to transmit to any registered CPE before it is replenished with the transmission credits at the sustained downlink data rate (in kbps).
LPULCIR (kbps)	The minimum rate (in kbps) at which a low priority traffic is sent over the

Parameter	Description
	uplink (unless Committed information rate (CIR) is oversubscribed or the RF link quality is degraded).
MPULCIR (kbps)	The minimum rate (in kbps) at which a medium priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
HPULCIR (kbps)	The minimum rate (in kbps) at which a high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
UHPULCIR (kbps)	The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
LPDLCIR (kbps)	The minimum rate (in kbps) at which a low priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
MPDLCIR (kbps)	The minimum rate (in kbps) at which a medium priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
HPDLCIR (kbps)	The minimum rate (in kbps) at which a high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
UHPDLCIR (kbps)	The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).

CPE wireless port statistics

The **CPE Wireless Port Stats** page provides information about statistics of all the data transmitted on the wireless link when it is up.

To view the wireless port statistics, perform the following steps:

1. From the left navigation column in the B1000 dashboard, navigate to **Subscribers > CPE Wireless Port Stats**.

The **CPE Wireless Port Stats** page appears, as shown in [Figure 30](#).

Figure 30: The CPE Wireless Port Stats page

Sys Name	In Octets	In Ucast Pkts	In Multicast Pkts	In Broadcast Pkts	Out Octets	Out Ucast Pkts	Out Multicast Pkts	Out Broadcast Pkts	In Discards	In Errors	Out Discards	Out Errors
CPE Release 3.1.1b2	18352776	15447	687	84897	19906466	78031	112	1	0	0	53527	0
CPE Release 3.1.1b2	18349040	15514	687	84897	19872017	78128	112	1	0	0	53498	0
CPE Release 3.1.1b2	18359513	15494	685	84897	19890191	78029	170	1	0	0	53436	0
CPE Release 3.1.1b2	18348427	15502	687	84868	19848653	78086	113	2	0	0	53536	0
CPE Release 3.1.1b2	18343479 +241	15529 +1	687	84868	19881111 +1086	78049 +4	115	2	0	0	53492 +2	0
CPE Release 3.1.1b2	18362377 +243	15535 +1	687	84868	19864342 +549	77978 +2	108	2	0	0	52629 +2	0
CPE Release 3.1.1b2	18367957	15671	687	84868	19932046	78116	185	1	0	0	53568	0

- View the wireless port statistics for CPEs, as described in [Table 20](#).

Table 20: List of parameters in the CPE Wireless Port Stats page

Parameter	Description
Sys Name	Name of the CPE system.
In Octets	Number of data bytes received by the BTS from the CPEs.
In Ucast Pkts	Number of data packets received by the BTS from a specific CPE.
In Multicast Pkts	Number of data packets received by the BTS from specific two or more CPEs.
In Broadcast Pkts	Number of data packets received by the BTS from all the connected CPEs.
Out Octets	Number of data bytes sent by the BTS to the CPEs.
Out Ucast Pkts	Number of data packets sent by the BTS to a specific CPE.
Out Multicast Pkts	Number of data packets sent by the BTS to specific two or more CPEs.
Out Broadcast Pkts	Number of data packets sent by the BTS to all the connected CPEs.
In Discards	Number of incoming data packets discarded by the CPE.
In Errors	Number of incoming data packets that contain errors.
Out Discards	Number of outgoing data packets (from CPE) that are marked or labelled as discarded by the CPE.
Out Errors	Number of outgoing data packets (from CPE) that contain errors.

CPE Ethernet port statistics

The **CPE Ethernet Port Stats** page provides statistics of the data that is entering the main Ethernet port.

To view the Ethernet port statistics, perform the following steps:

- From the left navigation column in the B1000 dashboard, navigate to **Subscribers > CPE Ethernet Port Stats**.

The **CPE Ethernet Port Stats** page appears, as shown in [Figure 31](#).


Figure 31: The CPE Ethernet Port Stats page

Sys Name	In Octets	In Ucast Pkts	In Multicast Pkts	In Broadcast Pkts	Out Octets	Out Ucast Pkts	Out Multicast Pkts	Out Broadcast Pkts	In Discards	In Errors	Out Discards	Out Errors
CPE Release 3.1.1b2	3744255 +53	0	51855 +1	1901	1127806	0	53	6084	0	0	79705 +2	0
CPE Release 3.1.1b2	3740517	0	51794	1901	1127276	0	53	6082	0	0	79677	0
CPE Release 3.1.1b2	3743838	0	51838	1901	2255780	0	108	12168	0	0	73564	0
CPE Release 3.1.1b2	3743651	0	51844	1901	1127202	0	52	6082	0	0	79678	0
CPE Release 3.1.1b2	3740775	0	51801	1900	1127350	0	54	6082	0	0	79676	0
CPE Release 3.1.1b2	3337592	1679	51859	970	5396255	3486	106	12204	0	0	73502	0
CPE Release 3.1.1b2	3753045 +492	0	51962 +7	1901	2276106	0	107	12324	0	0	73381	0

- View the Ethernet port statistics for CPEs, as described in [Table 20](#).

Configuring tools

The **Tools** page in the B1000 UI allows you to upload new firmware (software) or reboot the unit. There are set of tools, such as **Link Capacity Test**, which help to troubleshoot the radio links.

You must use the **Tools** icon () to configure, view, and manage the devices.

The **Tools** page contains the following tabs:

- [Firmware](#)
- [Configuration](#)
- [Link Capacity Test](#)
- [Network Test](#)
- [Engineering](#)

Firmware

The **Firmware** page allows you to upgrade or downgrade software firmware. This page also provides the device summary, upload details, and upgrade status of a firmware image.

Before upgrading or downgrading a firmware, consider the requirements and compatibility matrix specific to cnWave™ 5G Fixed products (BTS or CPE).

This topic covers the following sections:

- [Requirements for firmware version upgrade or downgrade](#)
- [Compatibility matrix](#)
- [Upgrade or downgrade a firmware](#)

Requirements for firmware version upgrade or downgrade

Consider the following minimum requirements related to BTS or CPE software version compatibility:

- An official BTS release version must be compatible with the previous official CPE release version.
- A beta BTS release version must be compatible with the previous official CPE release version.
- A BTS or CPE running with an official release software version can be upgraded to the following official release software version.
- A BTS or CPE running with an official release software version can be downgraded to the previous official release software version, except for when that version is lower than the factory version of the BTS or CPE.
- For best results, the CPE software versions on a sector must match the BTS software version. A sector with one or more CPE running with a software version different from the BTS software version may not meet the performance specification claimed for the BTS software version.

Compatibility matrix

The following compatibility matrix is required for upgrading or downgrading official BTS or CPE software versions.

Table 21: Compatibility matrix required for upgrade or downgrade

BT S	CPE												
	1.0	1.1	2.0	2.1	2.1.1	2.1.3	3.0	3.1	3.1.1	3.1.2	3.2	3.3	
1.0	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS	LOST BTS
1.1	Link establis hed but CPE cannot be accesse d on 169.254 .1.1 and shows IP address 0.0.0.0	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
2.0	No DL Tracking	No DL Tracking	OK	No DL Tracking	No DL Tracki ng	No DL Tracki ng	ON/O FF	ON/O FF	ON/O FF	ON/O FF	ON/O FF	ON/O FF	ON/O FF
2.1		X	OK	OK	OK	OK	X	X	X	X	X	X	X
2.1. 1	No DL Tracking	No Registra tion	No DL Tracki ng	No Registra tion	OK		ON/O FF	ON/O FF	ON/O FF	ON/O FF	ON/O FF	ON/O FF	ON/O FF
2.1. 3	ON/OFF	ON/OFF	No DL Tracki ng	OK	OK	OK	NO DL Tracki ng	NO DL Tracki ng	NO DL Tracki ng	NO DL Tracki ng	NO DL Tracki ng	NO DL Tracki ng	NO DL Tracki ng
3.0	X	X	No DL Tracki ng	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
3.1	X	X	No DL Tracki ng	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
3.1. 1	X	X	No DL Tracki ng	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
3.1. 2	X	X	No DL Tracki ng	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
3.2	X	X	No DL Tracki ng	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK

BTS	CPE											
	3.3	X	X	No DL Tracking	OK	OK	OK	OK	OK	OK	OK	OK

Following are the two types of changes identified, which can cause version incompatibility:

- Air interface change so that a CPE of one release version cannot attach to a BTS of another version.
- Hardware or calibration changes so that a CPE or BTS with early software version does not handle correctly.



Note

There is no need for the compatibility matrix to account explicitly for the hardware or calibration version.

Upgrade or downgrade firmware

You can upgrade or downgrade firmware (BTS or CPE) using the **Tools** page of the respective UI (B1000 UI for BTS and C100 UI for CPE).



Note

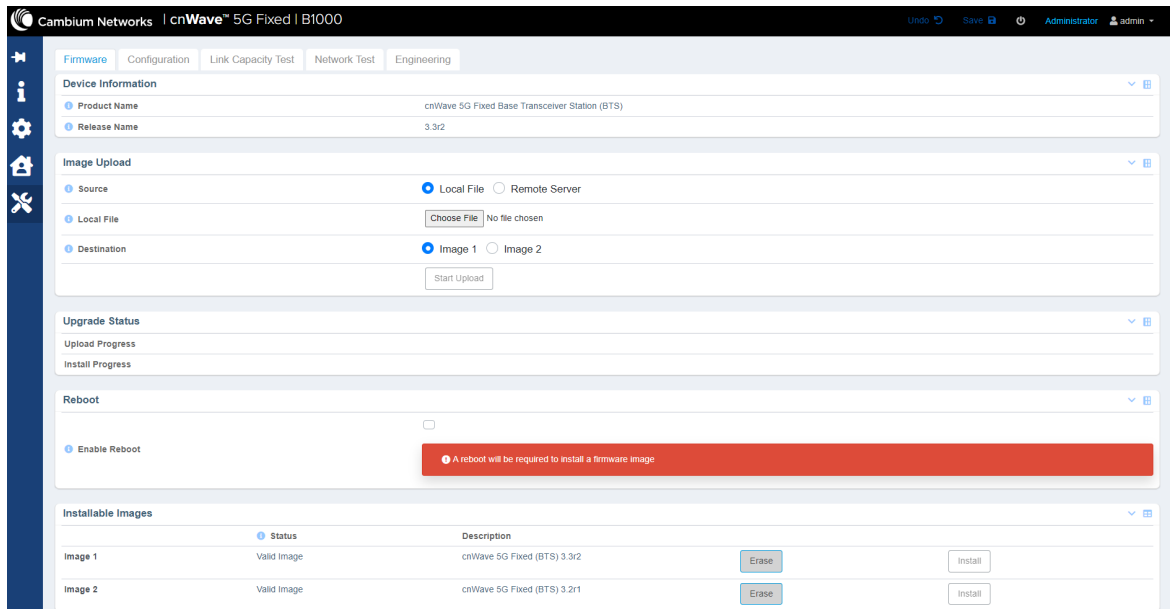
Before upgrading or downgrading firmware, consider the following key points:

- To **upgrade** a sector with the BTS and all CPEs running with an official software release X, perform the following steps using the **Tools** page:
 - Upgrade the BTS first to the next official software release version Y.
 - Upgrade all CPEs to the next official software release version Y.
- To **downgrade** a sector with the BTS and all CPEs running with an official software release X, perform the following steps using the **Tools** page:
 - Downgrade all CPEs first to the previous BTS software version W.
 - Upgrade the BTS to the previous official software release version W.

Using the **Tools** page, perform the following steps to upgrade or downgrade a firmware:

1. Log on to the B1000 UI (as described in the [Accessing the B1000 UI](#) section).
The main B1000 dashboard page appears.
2. On the left navigation column, click the **Tools** icon ().
The **Tools** page appears with multiple tabs, as shown in [Figure 32](#).

Figure 32: The Tool page - B1000 UI



By default, the **Firmware** tab is selected.

3. Set the required parameters, as described in [Table 22](#).

Table 22: List of parameters in the Firmware page

Parameter	Description
Device Information	
Product Name	Name of the device that you have deployed. Example: cnWave 5G Fixed Base Transceiver Station (BTS)
Release Name	Release number of the operational software.
Image Upload	
Source	An option to select the firmware image file from a location (stored). This parameter supports the following options: <ul style="list-style-type: none"> Local File: Indicates the image file that you have stored locally on your machine. Remote Server: Indicates the image file that you have stored on a remote server (for example, SharePoint). Select the required option.
Local File	An option to upload or upgrade the firmware image file. This parameter is applicable only if you have selected Local File as the upload source.

Parameter	Description
	This parameter supports options to upload or upgrade the required firmware image file. For more details on how to upload or upgrade the image file, refer to the Uploading a firmware image file section.
Server URL	This parameter is applicable only if you have selected Remote Server as the upload source. To upload the image file from a remote server, provide the server URL in the text box. Then, click Start Upload on the Firmware page.
Destination	An option to select the destination image in the Installable Images section. Select the required option.
Start Upload	An option to upload the firmware image file. On selecting the required image file (from a local file folder or a remote server), click Start Upload to begin the uploading process.
Upgrade Status	
Upload Progress	Indicates the upgrade status of the firmware.
Install Progress	Indicates the installation status of the firmware (if any).
Reboot	
Enable Reboot	Determines whether to reboot the device on upgrading or installing the firmware. Select the Enable Reboot check box to enable the device to reboot.
Installable Images	List of images that are recently uploaded, with details of the latest uploaded image at the top row. You can upload multiple image files and manage them in this section. This parameter displays the following details for the uploaded images: <ul style="list-style-type: none"> • Status: Displays one of the following supported statuses of the image: <ul style="list-style-type: none"> ◦ Empty: Indicates that the firmware image file is not present. ◦ Invalid Image: Indicates that the firmware image file is not valid. The file might be truncated, damaged, or not an appropriate image of the device (wrong product or old). ◦ Valid Image: Indicates that the firmware image file is valid and may be installed. • Description: A brief description of the firmware image file such as device name, version, build number, and time of uploading. <p>To install an image file that you uploaded, click Install in the corresponding row of the required image file.</p> <p>To delete an image file that you uploaded, click Erase in the corresponding row of the required image file.</p>

4. Click **Save** to save the configuration changes.

Uploading a firmware image file

Using the **Firmware** page, you can upload the required firmware image file locally. You can also install the uploaded image file and reboot the system.



Note

You must first upgrade the BTS software image file. You can follow the same process to upload or upgrade the CPE-specific image file using the **C100 Dashboard > Tools > Firmware** page.

To upload a local image file (internally), perform the following steps:

1. From the main dashboard page, navigate to **Tools > Firmware**.

The **Firmware** page appears. By default, the **Local File** option is selected as the upload source as shown in [Figure 33](#).

Figure 33: *The Local File parameter in the Firmware page*

The screenshot shows the Firmware page interface. The 'Image Upload' section is highlighted with a red box, showing 'Source' set to 'Local File' and 'Remote Server' unselected. Below it, the 'Local File' section has a 'Choose File' button and 'No file chosen' text. The 'Destination' section has 'Image 1' selected. The 'Upgrade Status' section shows 'Upload Progress' and 'Install Progress'. The 'Reboot' section has 'Enable Reboot' unselected and a red notification bar stating 'A reboot will be required to install a firmware image'. The 'Installable Images' section is a table with columns for Status, Description, Erase, and Install.

	Status	Description	Erase	Install
Image 1	Valid Image	cnWave 5G Fixed (BTS) 3.3r2	Erase	Install
Image 2	Valid Image	cnWave 5G Fixed (BTS) 3.2r1	Erase	Install

2. Before uploading the required firmware image file, check the status of the previously uploaded image files (if any) in the **Installable Images** section (located at the bottom of the **Firmware** page).

If there is any image file, which you do not want to use, you can manually remove that file by clicking on **Erase** in the corresponding row in the **Installable Images** section.

You can upload only two image files (in the disc image file format) as **Image 1** and **Image 2**, as shown in [Figure 33](#). For more information about each parameter in the **Firmware** page, refer to [Table 22](#).



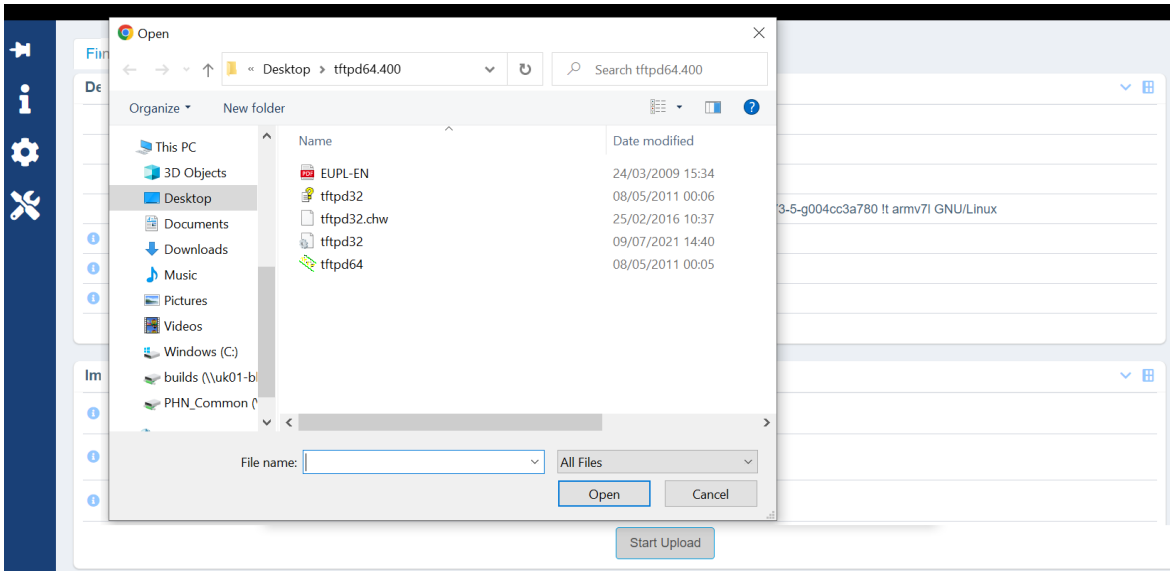
Note

When you select an updated image file from a location to replace an existing image file (for example, Image 1), the selected file overwrites the existing image 1 file in the **Installable Images** section.

3. To upload an image file, click **Choose File** in the Local File field.

A file browser window appears, as shown in [Figure 34](#).

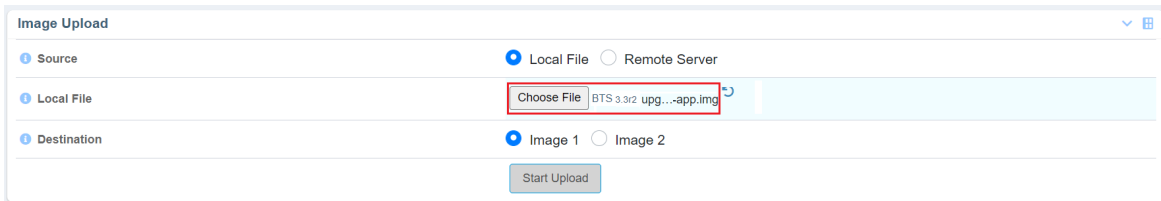
Figure 34: A file browser window



4. Browse the location where you have saved the required firmware image file on your machine, locally.
5. Select the required disc image file (for example, BTS 3.2r1 upgrade-app Disc Image File in case of upgrade) from your machine and click **Open**.

The local image file is selected, as shown in Figure 35.

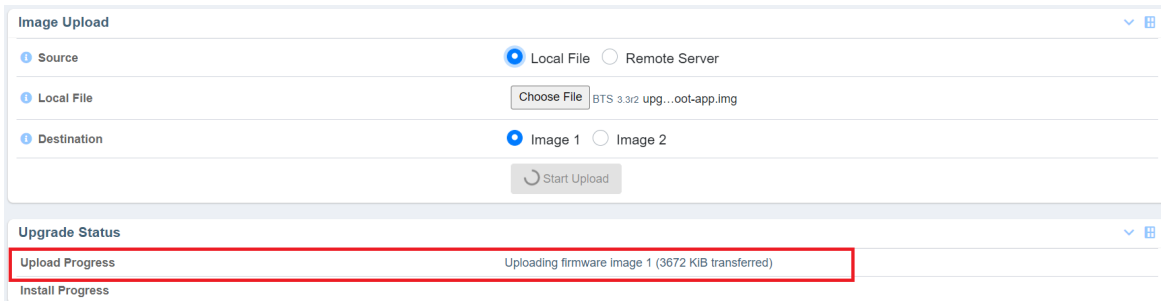
Figure 35: The image file name in the Local File field



6. To upload the selected image file, click **Start Upload**.

A message appears in the **Upload Progress** field, indicating the status of the upload process, as shown in Figure 36.

Figure 36: Upload status details in the Upload Progress field



Depending on the following actions, the **Upload Progress** field displays the status messages:

- When you upload a correct image file, a message appears indicating that the image is uploaded and validated successfully (as shown in [Figure 37](#)).
- When you upload an incorrect image file, a message appears indicating that the uploaded image is invalid.
- When you delete any image file from the **Installable Images** section (located at the bottom of the page), a message appears indicating that the firmware image is erased.

7. To install the uploaded image file, perform the following actions:

- a. Select the **Enable Reboot** check box in the **Reboot** section, as shown in [Figure 37](#).

When you enable the reboot option, the **Install** button is enabled in the **Installable Images** section as shown in [Figure 37](#). By default, the **Install** button is disabled.

Figure 37: *The Enable Reboot and Install options*

Status	Description	Eraser	Install
Valid Image	cnWave 5G Fixed (BTS) 3.3r2	Eraser	Install
Valid Image	cnWave 5G Fixed (BTS) 3.2r1	Eraser	Install

- b. Click **Install** in the corresponding row of the required image file.

This action installs the selected firmware image file and reboots the system.

You have now uploaded and installed the required firmware image file using the UI. Similarly for downgrade, select the required previous software version file, upload the file, and install the image file.

Configuration

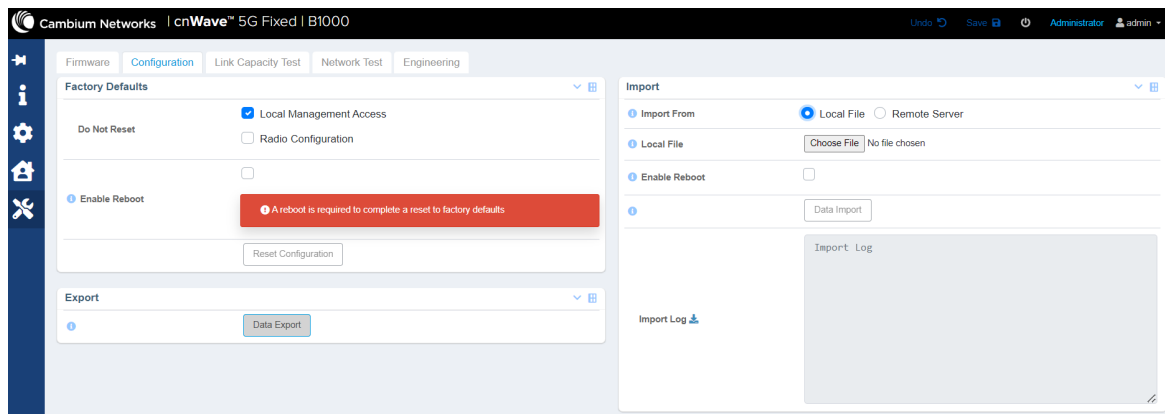
The **Configuration** page allows you to set the BTS to factory defaults. This page also allows you to import a saved configuration or export a BTS configuration for backup (restore). This Import feature exports or imports the date model configuration (and/or status) as a JSON file.

To view and manage the configuration tool-specific settings, perform the following steps:

1. From the main B1000 dashboard page, navigate to **Tools > Configuration**.

The **Configuration** page appears, as shown in [Figure 38](#).


Figure 38: The Configuration page - B1000 UI




2. Set the values for parameters, as described in [Table 23](#).

Table 23: List of parameters in the Configuration page

Parameter	Description
Factory Defaults	
Do not reset	<p>Determines whether you want to reset the device to factory defaults.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Local Management Access • Radio Configuration <p>By default, the Local Management Access check box is selected.</p> <p>If you do not select the Local Management Access check box, then all the configuration data, including IP address, is wiped out and reset to 169.254.1.1.</p> <p>You have a choice of keeping at least local access and IP address, and wiping out all the other data. This means that you can access the CPE on your local network.</p> <p>If you select Radio Configuration, then all the configuration data is wiped out, except for the frequency data and local IP address.</p>
Enable Reboot	<p>Determines whether the device is enabled to reboot to complete the process of reset to factory defaults.</p> <p>Select the check box to enable the reboot for the device.</p>
Reset Configuration	<p>An option to reset the system to factory defaults.</p> <p>Click Reset Configuration if you want to reset the device to factory defaults.</p>

Parameter	Description
Export	
Data Export	<p>An option to export the data model configuration (and/or) status as a JSON file for backup (restore).</p> <p>When you click the Data Export button, the data model configuration is downloaded by the device.</p>
Import	
Import From	<p>An option to select a location (stored) from where you want to import the required data configuration.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Local File: A local import file (which is saved locally) is uploaded by the browser. • Remote Server: An import file that is saved on a remote server is downloaded by the device. <p>Select the required option.</p> <p>Note: When you select Remote Server, the  icon appears indicating to select the Local File option (if required).</p>
Local File	<p>To upload a local import file (internally), perform the following steps:</p> <ol style="list-style-type: none"> Click Choose File in the Local File field. A file browser window appears. Browse the location where you have saved the import file (for example, a JSON file) on your machine locally. Select the file and click Open. The local import file is selected. To upload the import file, click Data Import in the Configuration page.
Server URL	<p>This parameter is applicable only if you have selected Remote Server in the Import From field.</p> <p>To select the import file from a remote server, provide the server URL in the text box. Then, click the Data import button.</p>
Enable Reboot	<p>Determines whether the device is enabled to reboot to complete the import configuration.</p> <p>Select the check box to enable the reboot for the device.</p> <p>When you select the check box, a message appears indicating that the device may reboot immediately after the required configuration is imported.</p> <p>Note: Only some configuration changes require a reboot.</p>
Data Import	<p>An option to import the required data model configuration from a JSON</p>

Parameter	Description
	file.
Import Log	An option to view and download the import logs from the UI. Click the  icon to download the import logs.

3. Click **Save** to apply the changes.

Link Capacity Test

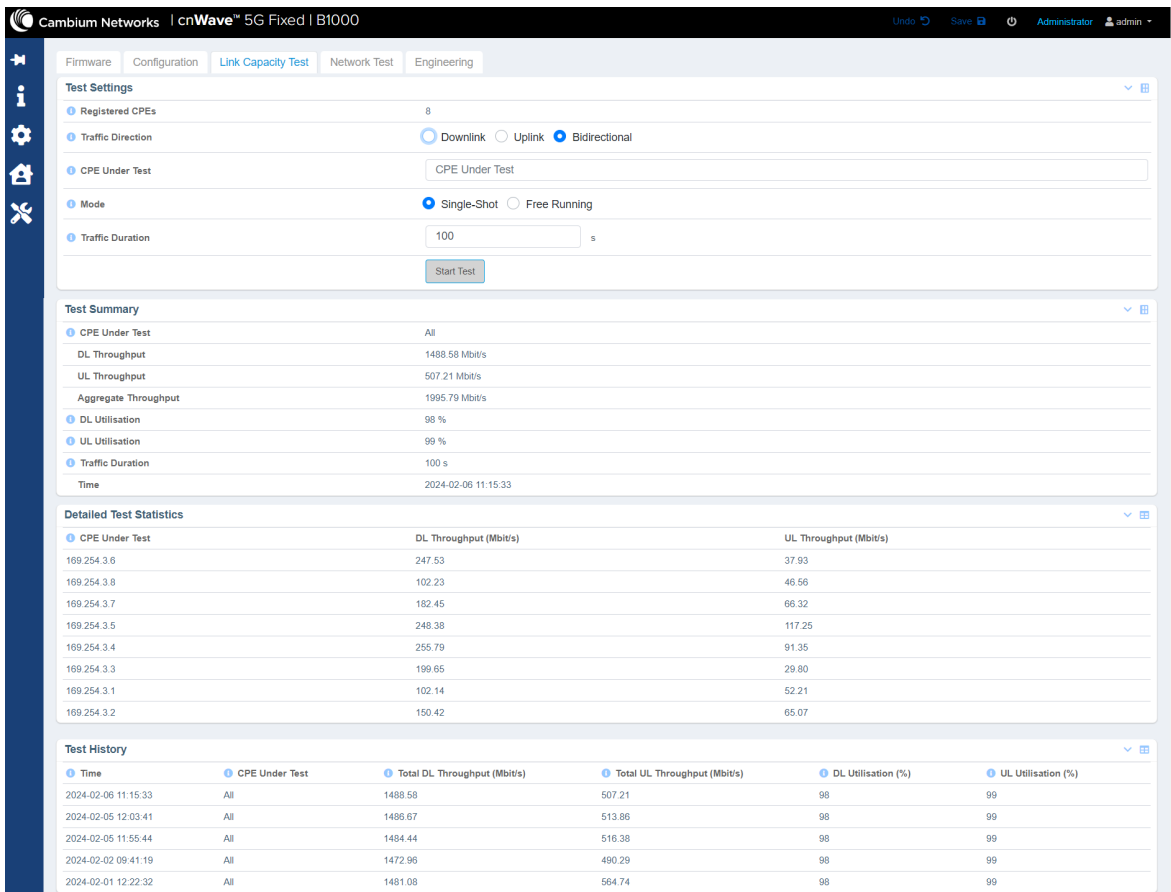
The **Link Capacity Test** page allows you to test the links (uplink, downlink, or both) and analyze the link performance for a subscriber (CPE). The test summary and statistics help in managing the traffic and troubleshooting the links for the subscriber.

To test and view the link capacity, perform the following steps:

1. From the main B1000 dashboard page, navigate to **Tools > Link Capacity Test**.

The **Link Capacity Test** page appears, as shown in [Figure 39](#).

Figure 39: *The Link Capacity Test page*




CPE Under Test	DL Throughput (Mbit/s)	UL Throughput (Mbit/s)
169.254.3.6	247.53	37.93
169.254.3.8	102.23	48.56
169.254.3.7	182.45	86.32
169.254.3.5	248.38	117.25
169.254.3.4	255.79	91.35
169.254.3.3	199.65	29.80
169.254.3.1	102.14	52.21
169.254.3.2	150.42	65.07

Time	CPE Under Test	Total DL Throughput (Mbit/s)	Total UL Throughput (Mbit/s)	DL Utilisation (%)	UL Utilisation (%)
2024-02-06 11:15:33	All	1488.58	507.21	98	99
2024-02-05 12:03:41	All	1486.67	513.86	98	99
2024-02-05 11:55:44	All	1484.44	516.38	98	99
2024-02-02 09:41:19	All	1472.96	490.29	98	99
2024-02-01 12:22:32	All	1481.08	564.74	98	99

The **Link Capacity Test** page displays Test Summary, Detailed Statistics, and Test History sections that contain results for the previous tests.

- To run the link capacity test, set the values of parameters as described in [Table 24](#).

Table 24: List of parameters in the Link Capacity Test page

Parameter	Description
Test Settings	
Registered CPEs	Indicates the current number of CPEs connected and authenticated to the BTS.
Traffic Direction	<p>Direction of the transmission of the traffic that you want to test.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Downlink • Uplink • Bidirectional <p>Select the required traffic direction.</p>
CPE Under Test	<p>IMSI or IP address of a registered CPE, which is used as the remote device, for which you want to test the link.</p> <p>Type an appropriate value in the text box.</p> <p>If you provide an incorrect value in the text box, a message appears, indicating that the provided value is unknown or invalid.</p> <p>Note: You can provide multiple comma-separated IMSIs or IP addresses and/or hyphenated IP addresses. If you test without any IMSI or IP address, the Test Summary and Test History section display results for all the connected CPEs.</p>
Mode	<p>Determines the mode for testing the link traffic.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Single-Shot • Free Running <p>By default, the Single-Shot option is selected.</p> <p>Note: When you select Free Running, the  icon appears indicating to select the Single-Shot option.</p>
Traffic Duration	<p>Duration (in seconds) of the transmission of the traffic that you want to test.</p> <p>Type an appropriate value in the text box.</p>

- Click **Start Test**.

You can click **Stop Test** after running the test for the required period.

The **Test Summary** section displays the test results for the selected subscriber modules (CPEs). The **Detailed Test Statistics** section displays DL throughput and UL throughput (in Mbit/s) for tested CPEs. The **Test History** section displays the results of the current test (as shown in [Figure 40](#)) and the previously tested modules (if any).

Figure 40 is an example of a link capacity test done for IMSIs with the following settings, where:

- **MU MIMO Control** is set to **Disabled** in the System > Radio page of the B1000 UI.
- **Traffic Direction** is set to **Bidirectional** in the Tools > Link Capacity Test page of the B1000 UI.

Figure 40: Link capacity test with MU MIMO disabled

The screenshot displays the 'Link Capacity Test' configuration page. The 'Test Settings' section includes: Registered CPEs (8), Traffic Direction (Bidirectional), CPE Under Test (a list of IMSIs), Mode (Single-Shot), and Traffic Duration (100 s). The 'Test Summary' section shows overall results: DL Throughput (315.58 Mbit/s), UL Throughput (127.21 Mbit/s), Aggregate Throughput (442.79 Mbit/s), DL Utilisation (98%), UL Utilisation (99%), and Traffic Duration (100 s). The 'Detailed Test Statistics' table provides per-CPE data for DL and UL throughput. The 'Test History' table shows a list of test runs with columns for Time, CPE Under Test, Total DL Throughput, Total UL Throughput, DL Utilisation, and UL Utilisation.

Test Settings					
Registered CPEs	8				
Traffic Direction	<input checked="" type="radio"/> Downlink <input type="radio"/> Uplink <input checked="" type="radio"/> Bidirectional				
CPE Under Test	888901007406841,888901007406348,888901007406344,888901007406574,888901007406869,888901007406429,888901007406893,888901007407454				
Mode	<input checked="" type="radio"/> Single-Shot <input type="radio"/> Free Running				
Traffic Duration	100 s				
<button>Start Test</button>					
Test Summary					
CPE Under Test	888901007406841,888901007406348,888901007406344,888901007406574,888901007406869,888901007406429,888901007406893,888901007407454				
DL Throughput	315.58 Mbit/s				
UL Throughput	127.21 Mbit/s				
Aggregate Throughput	442.79 Mbit/s				
DL Utilisation	98 %				
UL Utilisation	99 %				
Traffic Duration	100 s				
Time	2024-02-07 07:11:24				
Detailed Test Statistics					
CPE Under Test	DL Throughput (Mbit/s)	UL Throughput (Mbit/s)			
169.254.3.6	39.44	15.89			
169.254.3.7	39.44	15.91			
169.254.3.2	39.45	15.90			
169.254.3.5	39.44	15.90			
169.254.3.4	39.45	15.91			
169.254.3.8	39.46	15.90			
169.254.3.3	39.45	15.89			
169.254.3.1	39.45	15.91			
Test History					
Time	CPE Under Test	Total DL Throughput (Mbit/s)	Total UL Throughput (Mbit/s)	DL Utilisation (%)	UL Utilisation (%)
2024-02-07 07:11:24	888901007406841,888901007406348,888901007406344,888901007406574,888901007406869,888901007406429,888901007406893,888901007407454	315.58	127.21	98	99
2024-02-07 07:07:44	888901007406841,888901007406348,888901007406344,888901007406574,888901007406869,888901007406429,888901007406893,888901007407454	1495.84	0.11	98	76

Figure 41 is an example of a link capacity test done for the same IMSIs with the following settings, where:

- **MU MIMO Control** is set to **Enabled** in the System > Radio page of the B1000 UI.
- **Traffic Direction** is set to **Downlink** in the Tools > Link Capacity Test page of the B1000 UI.

Figure 41: Link capacity test with MU MIMO enabled

The screenshot displays the 'Link Capacity Test' interface. It features a navigation bar with tabs for 'Firmware', 'Configuration', 'Link Capacity Test', 'Network Test', and 'Engineering'. The 'Link Capacity Test' tab is active, showing the following sections:

- Test Settings:** Registered CPEs: 8; Traffic Direction: Downlink; CPE Under Test: 888901007406841, 888901007406348, 888901007406344, 888901007406574, 888901007406869, 888901007406429, 888901007406893, 888901007406841; Mode: Single-Shot; Traffic Duration: 100 s; Start Test button.
- Test Summary:** CPE Under Test: 888901007406841, 888901007406348, 888901007406344, 888901007406574, 888901007406869, 888901007406429, 888901007406893, 888901007407454; DL Throughput: 1495.84 Mbit/s; UL Throughput: 0.11 Mbit/s; Aggregate Throughput: 1495.95 Mbit/s; DL Utilisation: 98%; UL Utilisation: 76%; Traffic Duration: 100 s; Time: 2024-02-07 07:07:44.
- Detailed Test Statistics:** Table with columns: CPE Under Test, DL Throughput (Mbit/s), UL Throughput (Mbit/s). Rows list individual CPE test results.
- Test History:** Table with columns: Time, CPE Under Test, Total DL Throughput (Mbit/s), Total UL Throughput (Mbit/s), DL Utilisation (%), UL Utilisation (%). A single row is highlighted in yellow.

Table 25 lists and describes each parameter of the **Test Summary** and **Test History** sections in the **Link Capacity Test** page.

Table 25: List of test summary and history-specific parameters

Parameter	Description
Test Summary	
CPE Under Test	IMSI or IP address of the CPE that you used for testing. Note: If you have provided multiple IMSIs or IP addresses, then this parameter displays those values for which the test was conducted.
DL Throughput	The DL throughput (in Mbit/s) of the tested CPE.
UL Throughput	The UL throughput (in Mbit/s) for the tested CPE.
Aggregate Throughput	The aggregate throughput (in Mbit/s) for the tested CPE.
DL Utilisation	The percentage of the available link capacity that has been utilised by the downlink scheduler.
UL Utilisation	The percentage of the available link capacity that has been utilised by the uplink scheduler.
Traffic Duration	Duration (in seconds) of the transmission of the tested traffic.
Time	Date and time (YYYY-MM-DD 24-hour format format) at which the traffic

Parameter	Description
	was tested for a CPE.
Detailed Test Statistics	
CPE Under Test	The IP addresses or IMSIs of the CPE that is used as the remote device for the test.
DL or UL Throughput (Mbit/s)	The DL or UL throughput (in Mbit/s) for the tested CPE based on the value selected in the Traffic Direction parameter.
Test History	
Time	Date and time (in YYYY-MM-DD 24-hour format) at which the link capacity test was conducted.
CPE Under Test	IMSI or IP address of the CPEs (used as remote device) for which the test statistics are available. Note: If you have provided multiple IMSIs or IP addresses then this parameter displays those values for which the test was conducted.
Total DL Throughput (Mbit/s)	Total value (in Mbps) of the downlink throughput.
Total UL Throughput (Mbit/s)	Total value (in Mbps) of the uplink throughput.
DL Utilisation (%)	The percentage of the available link capacity that has been utilised by the downlink scheduler.
UL Utilisation (%)	The percentage of the available link capacity that has been utilised by the uplink scheduler.

Network Test

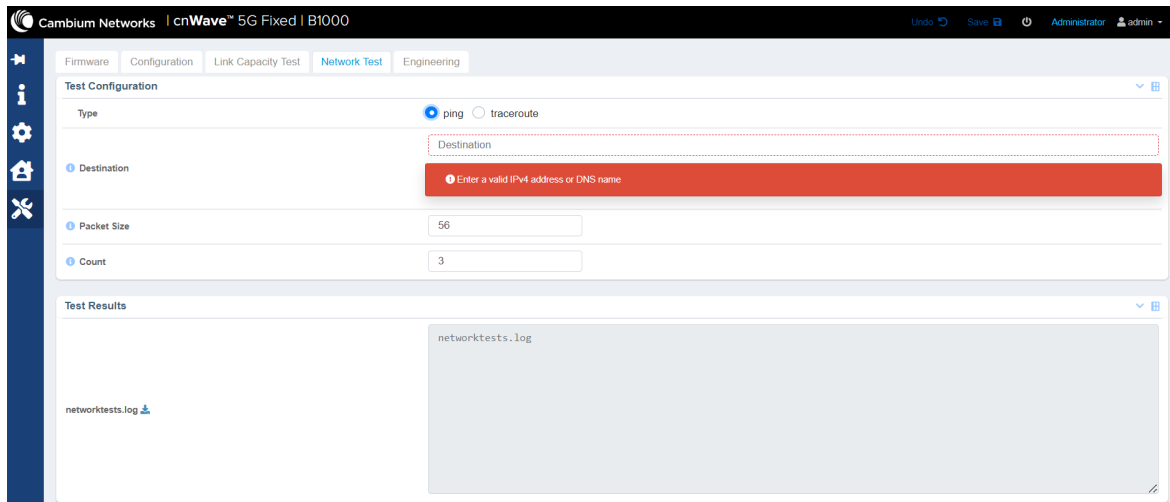
The **Network Test** is a network tool that helps you to test connectivity and accessibility of BTS to a radio network. This page allows you to ensure whether BTS is correctly connected to your network. Example: BTS connectivity with cnMaestro or a RADIUS server. This network test helps in troubleshooting network connection issues.

To test and view the BTS connectivity, perform the following steps:

1. From the main B1000 dashboard page, navigate to **Tools > Network Test**.

The Network Test page appears, as shown in [Figure 42](#).

Figure 42: The Network Test page



2. View and set the values for parameters, as described in Table 26.

Table 26: List of parameters in the Network Test page

Parameter	Description
Test Configuration	
Type	<p>Determines the method used for testing a network.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • ping: BTS pings the required destination (for example, cnMaestro, RADIUS Server, DNS, or a radio network) to ensure its connectivity. <p>If the pig is successful, this implies that BTS can reach the network or the required destination.</p> <ul style="list-style-type: none"> • traceroute: BTS traces the source (IP address) of the required destination (for example, if the BTS is connected to a switch, which is connected to another application such as a host Server) by identifying the number of hops connected to the radio network. <p>If the trace is successful, BTS finds out the IP address of the networks in 30 hops. If the trace fails in 6 to 7 hops, this implies that BTS cannot reach the network.</p> <p>Choose the required testing type.</p> <p>Figure 43 and Figure 44 are examples of ping and traceroute types.</p>
Destination	<p>The valid IPv4 address or a DNS name of the required destination.</p> <p>Provide an appropriate value in the text box.</p>
Packet Size	<p>Number of data bytes that have to be sent to the network.</p>


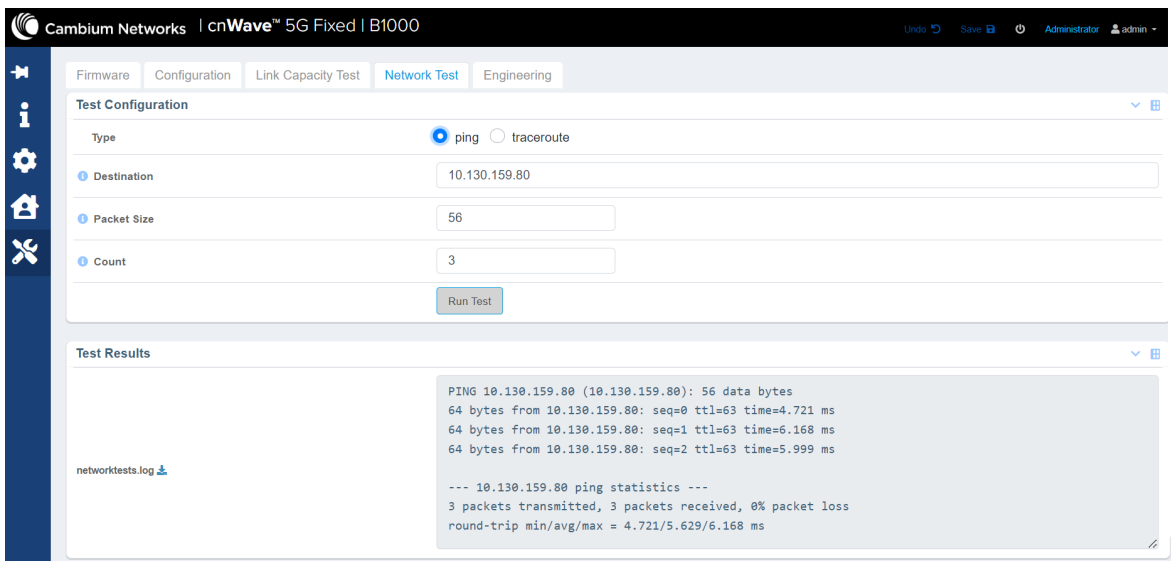
Parameter	Description
	<p>Default value: 56 data bytes, which are translated into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.</p> <p>Provide the required value in the text box.</p> <p>Note: This parameter is not applicable if you select <code>traceroute</code> in the Type field.</p>
Count	<p>Number of ping packets that has to be sent to the network.</p> <p>Default value: 3</p> <p>Provide the required value in the text box.</p> <p>Note: This parameter is not applicable if you select <code>Traceroute</code> in the Type field.</p>
Run Test	<p>An option to run the test.</p> <p>This option appears only when you provide a value in the Destination text box.</p>
Stop Test	<p>An option to stop the test that has begun.</p> <p>This option appears only when you run the test.</p>
Test Results	
networktests.log	<p>Displays the test results for the required destination.</p> <p>By default, this field is disabled. When you run the test, this field displays the test results.</p> <p>You can use the  icon to download the log file.</p>

Figure 43 is an example of a test result for the **ping** type:

Figure 43: Test result - ping



The screenshot shows the 'Network Test' configuration page in the cnWave 5G Fixed B1000 interface. The 'Type' is set to 'ping'. The 'Destination' is '10.130.159.80', 'Packet Size' is '56', and 'Count' is '3'. A 'Run Test' button is visible. Below the configuration, the 'Test Results' section displays the output of the ping command:

```

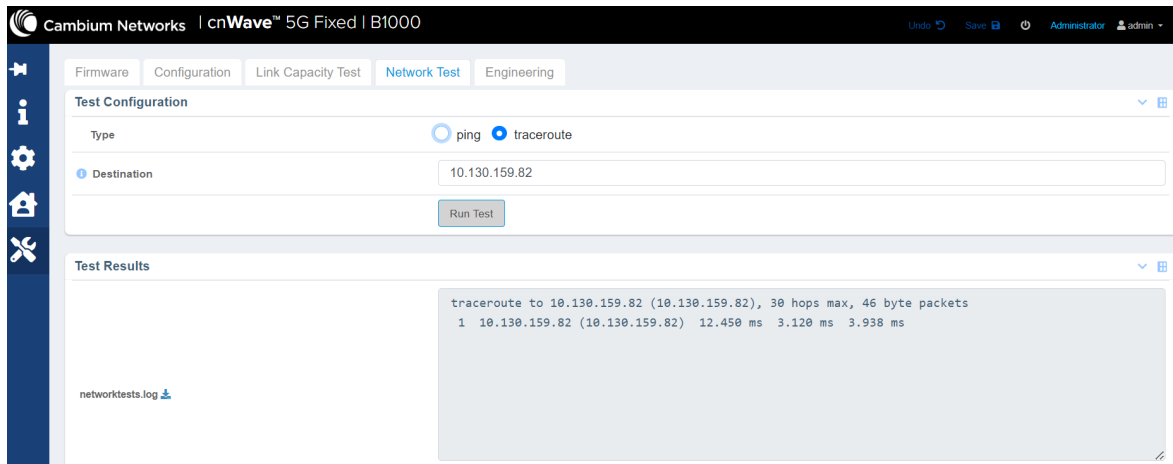
PING 10.130.159.80 (10.130.159.80): 56 data bytes
64 bytes from 10.130.159.80: seq=0 ttl=63 time=4.721 ms
64 bytes from 10.130.159.80: seq=1 ttl=63 time=6.168 ms
64 bytes from 10.130.159.80: seq=2 ttl=63 time=5.999 ms

--- 10.130.159.80 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 4.721/5.629/6.168 ms

```

Figure 44 is an example of a test result for the **traceroute** type:

Figure 44: Test result - traceroute



Engineering

The **Engineering** page allows engineers (of Cambium Networks) to access the BTS radio remotely. Engineers can allow the users to access the radio using Telnet, SSH, and console secured cable (HTTP is not allowed).



Note

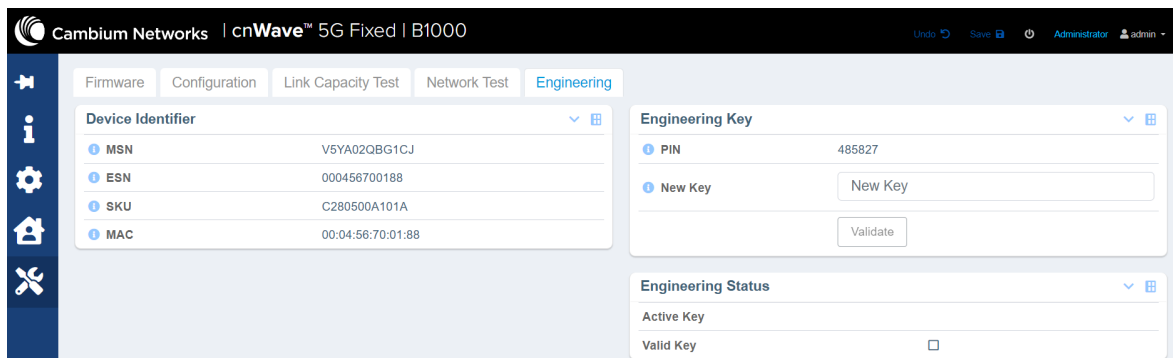
The **Engineering** page is configured and applicable only for troubleshooting and support purposes.

To view and set the **Engineering** page, perform the following steps:

1. From the main B1000 dashboard page, navigate to **Tools > Engineering**.

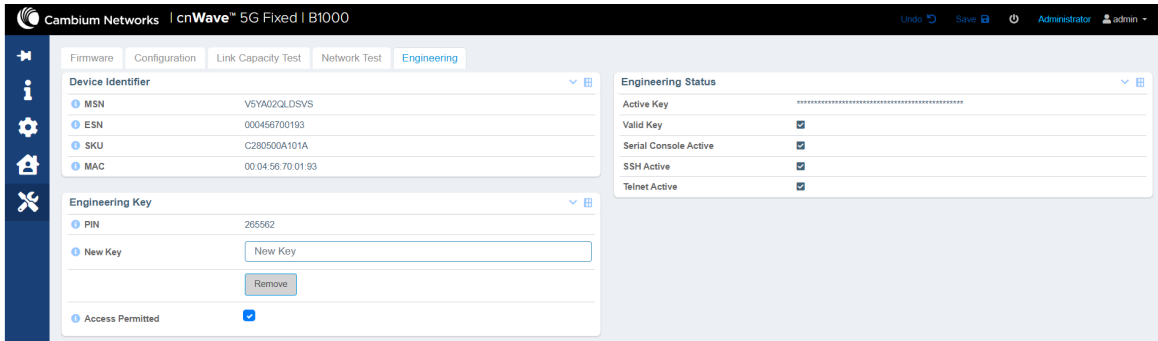
The **Engineering** page appears, as shown in Figure 45.

Figure 45: The Engineering page - B1000 UI



If the engineers (from Cambium Networks) have not removed any engineering keys from the UI, then the **Engineering Status** section in the **Engineering** page displays all the configured engineering keys as shown in Figure 46.

Figure 46: The Engineering page with all the key details



2. View and set the values for parameters, as described in Table 27.

Table 27: List of parameters in the Engineering page

Parameter	Description
Device Identifier	
MSN	MSN of the device that is used for device identification.
ESN	ESN of the device.
SKU	SKU of the device.
MAC	The MAC address that is assigned to the network interface and used for the device management.
Engineering Key	
PIN	Unique six-digit number used by the Engineering team of Cambium Networks to generate an engineering key for the BTS device. This is a read-only field.
New Key	The new engineering key generated and provided by the Engineering team of Cambium Networks using PIN. This new engineering key allows privileged engineering access to the BTS device. Enter the engineering key in the text box.
Remove	An option to remove the installed key and access the BTS device. If you click Remove , then the installed new key and access (using SSH, Serial Console, and Telnet) are removed.
Access Permitted	Determines whether the new key enables engineering access to the BTS device. Select the check box to enable the engineering access for the new key. Note: By default, the engineering access is enabled when a new key is installed.
Engineering Status - Following are the read-only parameters:	

Parameter	Description
Active Key	Indicates whether the new generated key is accessible.
Valid Key	Indicates whether the generated key is valid.
Serial Console Active	Indicates whether the serial console is accessible for the users.
SSH Active	Indicates whether SSH is accessible for the users.
Telnet Active	Indicates whether the Telnet is accessible for the users.

The C100 Dashboard

This section provides information on accessing the C100 dashboard. It also explains how to configure the C100 dashboard for managing CPEs.

This section covers the following topics:

- [Accessing the C100 UI](#)
- [Viewing the C100 dashboard](#)
- [Configuring C100 \(CPE\)](#)

Accessing the C100 UI

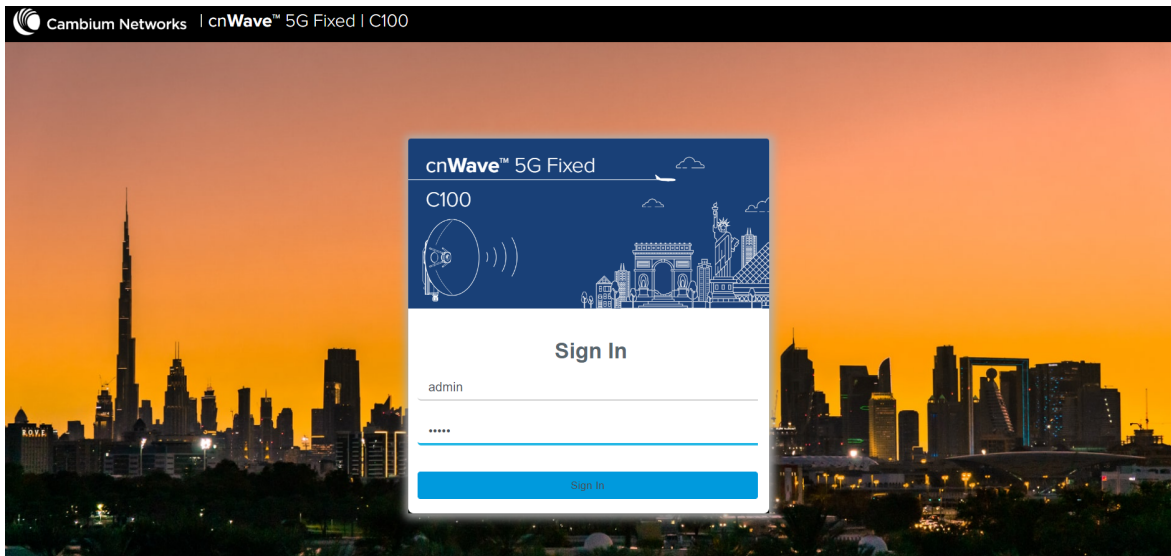
This section explains how to log on to the C100 (CPE) UI and view the C100 dashboard.

To access the C100 UI, perform the following steps:

1. Use the default IP address (169.254.1.1) to connect to the CPE setup.
2. Ensure that your PC is set up to communicate with the required range of IP addresses.
3. Open a web browser and type the URL - <http://169.254.1.1> to access the C100 UI.

The **Sign In** page appears, as shown in [Figure 47](#).

Figure 47: The Sign In page for C100 UI (CPE)



4. Type an appropriate username and password.

Default username: admin

Default password: admin

5. Click **Sign In**.

The **Profile** page appears, as shown in [Figure 48](#). This page allows you to change the password.

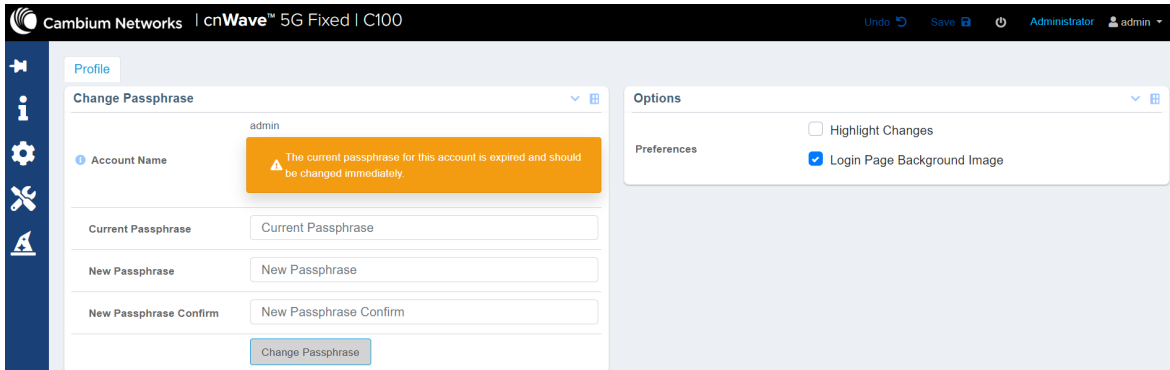


Note

Do not change the password every time when the **Profile** page appears. You must change the password only when it is required.

You can also access the **Profile** page by selecting **Profile** from the **admin** drop-down list on the top right side of the C100 UI.

Figure 48: *The Profile page*



[Table 28](#) lists and describes the parameters on the Profile page of C100 UI.

Table 28: List of parameters in the Profile page

Parameter	Description
Change Passphrase	
Account Name	The default name of the user account required for accessing the C100 UI. This is read-only parameter.
Current Passphrase	The default password used for the first time log in or for the previous access. Default password: admin Enter the current password in the text box.
New Passphrase	Enter a new password in the text box. Note: The maximum character limit for the password is eight.
New Passphrase Confirm	Reenter the new password in the text box to confirm.
Change Passphrase	An option to change the current password. Click on Change Passphrase to change the current password.
Options Used for the engineering purpose.	
Preferences	An option to set your preferences in the UI. Following options are supported:

Parameter	Description
	<ul style="list-style-type: none"> • Highlight Change: Use this option to easily identify the new changes, which are highlighted in light yellow color on UI pages. These highlighted values help you in quickly monitoring the system changes. Example: The System > Interface UI page displays the highlighted values in light yellow color. • Login Page Background Image: Use this option to set the background image on the Sign In page of UI (as shown in Figure 47). <p>Select the check boxes, if required.</p>

6. On changing the password, log on to the C100 UI using admin (username) and the new password (which you set on the **Profile** page).

The **Profile** page appears, as shown in [Figure 48](#).

7. To view the main C100 dashboard, click the **i** icon (Dashboard) on the left navigation pane.

The main **Dashboard** page appears, as shown in [Figure 49](#).

Figure 49: The C100 dashboard page

The screenshot displays the Cambium Networks C100 dashboard. The top navigation bar includes the logo, product name 'cnWave™ 5G Fixed | C100', and user information 'Administrator admin'. The main content area is divided into several sections:

- General:** Tabs for General, Device, Radio, and Session.
- Device Summary:**
 - Product Name: cnWave 5G Fixed Consumer Premises Equipment (CPE)
 - Release Name: 3.3r2
 - System Description: Cambium Networks cnWave 5G Fixed Consumer Premises Equipment (CPE) 3.3r2 arm71 GNU/Linux
 - System Name: CPE Release 3.1.1b2
 - System Location: D1 Lab
 - System Contact: Yassine Poc Rig 1
 - System Time: 2024-03-07 07:04:31
- Radio:**
 - Current Frequency: 27000.000 MHz
 - Rx Power: -45 dBm
 - EVM: -28.8 dB
 - DL MCS: 23
 - DL Backoff: 13 dB
 - UL MCS: 23
 - UL Backoff: 5 dB
 - Calibration Status: Calibrated
 - Tx State: Tx Enabled (with a warning: Transmit control overridden by Engineering key)
- Session:**
 - Registration State: Registered
 - Registration Count: 1
 - Link Uptime: 1d 21h 52m
 - Auth Mode: RADIUS AAA
- Network:**
 - MAC: 00:04:56:71:04:F9
 - IP Address: 169.254.3.1
 - Prefix: 24
 - Default Gateway: 169.254.3.99
- VLAN:**
 - VLAN Configured By RADIUS:
 - Active VLAN Configuration:
 - Management VID: 1 [from RADIUS]
 - Management VID Priority: 0
 - Allow Frame Types: Tagged Frames [from RADIUS]
 - Accept Q-in-Q Frames: True
 - CPE Management VID Pass-through: Disabled [from RADIUS]
 - VLAN Enabled: Enabled [From BTS]
 - Q-in-Q Ether Type: 0x8100 [From BTS]
 - VLAN Port Type: Q
 - Default Port VID: 50 [from RADIUS]
 - Default Port VID Priority: 0
 - Dynamic Learning: Enabled [from RADIUS]
 - VLAN Aging Timeout: 25 [from RADIUS]

For more information about the C100 dashboard page, refer to the [Viewing the C100 \(CPE\) dashboard](#) section.

You can now use the required UI controls (as described in [Table 1](#)) for configuring and managing CPEs.



Note

To log out from the UI, select **Logout** from the **admin** drop-down list on the top right side of the UI.

For information on UI controls available on the C100 dashboard, refer to [Table 2](#).

Viewing the C100 (CPE) dashboard

The C100 dashboard (as shown in [Figure 49](#)) provides comprehensive information about the link status, radio parameters, RADIUS session settings, and other network details. Example: In [Figure 49](#), the dashboard indicates that the CPE is up for more than 15000 seconds and that the Receive Power is -46 dBm.

The main C100 dashboard page contains the following tabs:

- [General](#)
- [Device](#)
- [Radio](#)
- [Session](#)

General

When you access the C100 UI, the main C100 dashboard appears with the **General** tab (by default).

The **General** page provides a summary (read-only) of the connected devices (as shown in [Figure 49](#)) and registered sessions. It also displays details of ESN (MAC), IMSI, Rx Power, and the other system related details. [Table 29](#) lists and describes parameters available on the **General** page.

Table 29: Parameters in the General page

Parameter	Description
Device ESN	The Electronic Serial Number (ESN) of the hardware device (CPE), which is the same as the MAC address.
IMSI	IMSI that is associated with the CPE (of a subscriber). IMSI is a number that uniquely identifies the user of a cellular network.
Session	Time (in seconds) at which the last successful registration is available for the CPE.
Radio	Indicates the Rx Power (data) and the Error Vector Magnitude (EVM) of the radio downlink signal.
Device Summary	
Product Name	Name of the device that you have deployed. Example: cnWave 5G Fixed Consumer Premises Equipment (CPE)
Release Name	Release number of the operational software.
System Description	A brief description of the CPE system (device).
System Name	An administratively assigned name of the device. When using DNS, this name must be the device's fully qualified domain name (FQDN).
System Location	The physical location of the device node.
System Contact	Contact details of the device administrator.
System Time	Date and time (in YYYY-MM-DD 24-hour format) that are configured in the system.

Parameter	Description
Radio	
Current Frequency	The current operating frequency in MHz.
Rx Power	The Receive power of data symbols in dBm.
EVM	The EVM of the radio downlink signal (in dB).
DL MCS	MCS of the downlink.
DL Backoff	<p>Indicates the amount (in dB) of power backoff for the downlink.</p> <p>This is the amount by which the BTS is currently reducing its power from the maximum configured EIRP when transmitting to the CPE. The BTS uses the greatest backoff that it can achieve while still maintaining the downlink throughput required by the CPE.</p> <p>Note: Backing off the BTS transmit power means the power allocation maximized for the CPE, which also requires for minimizing interference.</p>
UL MCS	MCS of the uplink.
UL Backoff	<p>Indicates the amount (in dB) of power backoff for the uplink.</p> <p>The Tx Power is reduced if there is link budget during the top modulation mode to improve the spectral efficiency.</p>
Calibration Status	<p>Indicates the unit calibration status.</p> <p>The calibrated status implies that CPE has been tested and calibrated for all the frequency ranges.</p> <p>Note: A production unit showing an uncalibrated or a persistent uncalibrated state indicates a problem that requires factory repair.</p>
Tx State	<p>Specifies the status of transmit control (Tx).</p> <p>This is a read-only parameter. By default, this parameter is enabled.</p> <p>Note: If the engineering keys (used for troubleshooting and support) are enabled, then this parameter displays a message (highlighted in orange) indicating that transmit control is overridden by the Engineering key. For more information about the engineering keys, refer to the Engineering section.</p> <p>If CPE cannot connect to BTS due to frequency or any other reason, this parameter displays a message (highlighted in red) indicating that the frequency is not locking.</p>
Session	
Registration State	<p>Indicates the progress that a CPE (device) has made to enter the network.</p> <p>For more information about this parameter, refer to Table 32.</p>
Registration Count	<p>Number of times that the CPE has successfully registered with the BTS.</p> <p>For more information about this parameter, refer to Table 32.</p>
Link Uptime	Time (in seconds) at which the last successful registration of the link is available for the CPE.

Parameter	Description
Auth Mode	Indicates the CPE authentication mode. For more information about this parameter, refer to Table 32 .
Network - Based on the RADIUS configuration, this section (in the C100 UI) populates values.	
MAC	The Ethernet MAC address that is assigned to the network interface and used for managing the device.
IP Address	The IP address that is assigned to the network interface and used for managing the device.
Prefix	The IP network prefix that is assigned to the network interface and used for managing the device.
Default Gateway	The IP address of the default gateway (if any) that is used for managing the device.
VLAN	
VLAN Configured by RADIUS	Determines whether the VLAN configuration is set through RADIUS AAA. At the time of boot, the CPE network configuration uses the locally configured VLAN settings, and these settings may be overridden by the RADIUS-specific settings during registration. For more details, refer to the Configuring system settings section.
Active VLAN Configuration	Details of the VLAN configuration that is currently active for the CPEs. For more details on configuring the VLAN, refer to the Configuring system settings section.

Device

When you click on the **Device** tab in the main C100 dashboard page, the **Device** page appears.

The **Device** page provides details (read-only) of the device identifiers, reboot history, reboot reasons, and the hardware version of the device (as shown in [Figure 50](#)).

Figure 50: *The Device page - C100 UI*

The screenshot shows the 'Device' page in the C100 UI. It features a navigation sidebar on the left and a main content area with several sections:

- Device Identifier:** MSN (V5YA01XDV62D), ESN (0004567104F9), SKU (C280500C001A).
- Boot Loader:** Git Tag (develop/4/111), Build Name (BOOTLOADER 111/2023-09-25 (W) 11:19:15 -0500).
- Hardware:** Hardware Version (Digits P7.0 RF 8.0), RFID (X60610000481).
- Boot:** Startup Reason (Non-Power Cycle), Startup Count (947).
- Shutdown:** A table with columns: History, Reason, Date, Detail.

History	Reason	Date	Detail
1	Firmware Upgrade	2024-02-01 11:51:32	develop-5-27-1-g969ccef7e0-nT to 3.2r1
2	Shutdown	1980-01-01 02:28:39	
3	Power Loss	0000-00-00 00:00:00	Boot after long power cycle
4	Power Loss	0000-00-00 00:00:00	Boot after long power cycle
5	Power Loss	0000-00-00 00:00:00	Boot after long power cycle
6	Power Loss	0000-00-00 00:00:00	Boot after long power cycle
7	Power Loss	0000-00-00 00:00:00	Boot after long power cycle
8	Power Loss	0000-00-00 00:00:00	Boot after long power cycle

[Table 30](#) lists and describes parameters available on the **Device** page.

Table 30: Parameters in the Device page

Parameter	Description
Device Identifier	
MSN	Manufacturer Serial Number (MSN) of the device that is used for device identification.
ESN	ESN of the device.
SKU	Stock Keeping Unit (SKU) of the device.
Boot Loader	
Git Tag	ID of the software build version.
Build Name	Build name of the BTS software.
Hardware	
Hardware Version	Hardware version of the CPE.
RFID	The radio frequency (RF) module ID.
Boot	
Startup Reason	<p>Indicates the reason for the previous system reboot.</p> <p>The following reasons are supported:</p> <ul style="list-style-type: none"> • Non-Power Cycle: The device was reset without a power cycle. • Short Power Cycle: Power to the device was briefly interrupted. • Long Power Cycle: Power to the device was interrupted.
Startup Count	Indicates the counter that is incremented each time when the device starts up.
Shutdown - Provides details of the boot history.	
History	<p>Index of the boot history.</p> <p>The history for the most recent system reboot is always available in the first row.</p>
Reason	<p>Reasons specified for each boot history.</p> <p>The following boot reasons are supported:</p> <ul style="list-style-type: none"> • Unspecified: The shutdown was not planned (for example, power loss or Watchdog reset). • Shutdown - Shutdown due to a user action. • Firmware Upgrade: A firmware upgrade requiring a reboot to complete. • Configuration Change: A configuration change requiring a reboot to complete. • User Action: A user action requiring a reboot. • Watchdog: A managed shutdown due to a fatal system fault.

Parameter	Description
	<ul style="list-style-type: none"> • Application Fatal: A managed shutdown due to an application managed error. • Application Panic: A managed shutdown due to an application fatal error.
Date	Date and time at which the system was rebooted.
Detail	A brief description of the reboot.

Radio

When you click on the **Radio** tab in the main C100 dashboard page, the **Radio** page appears.

The **Radio** page provides information (read-only) about the status of operating frequency, receive power levels, EIRP, and the range (distance) to BTS (as shown in [Figure 51](#)). You can monitor the C100 (CPE) dashboard to ensure that a connection has been authenticated and established with the desired BTS.

Figure 51: *The Radio page - C100 UI*

[Table 31](#) lists and describes parameters available on the **Radio** page.

Table 31: Parameters in the Radio page

Parameter	Description
Summary	
Current Frequency	The current operating frequency (in MHz).
Scan State	<p>The current status of the BTS signal specific acquisition state machine.</p> <p>The following states are supported:</p> <ul style="list-style-type: none"> • Scanning • Scanning - Fine • Acquiring • Tracking

Parameter	Description
	Note: The acquisition state machine must reach the Tracking state to establish a wireless connection.
Current EIRP	The current Effective Isotropic Radiated Power (EIRP) in dBm.
Current Polarisation	The current antenna polarisation.
Bandwidth	The bandwidth of an active radio channel. The bandwidth is automatically determined from the signal received from the BTS.
Extended Range	The extended range status for operating the BTS. You can set the Extended Range parameter using the System > Radio page of the B1000 UI. For more information, refer to the Radio section.
Range	The distance measured between BTS and CPE (in Km).
Downlink Details	
Rx Power	The receive power of data symbols (in dBm).
DL MCS	MCS of the downlink.
DL Backoff	Indicates the amount (in dB) of power backoff for the downlink. For more details about this parameter, refer to Table 29 .
Spatial Frequency	Indicates the spatial frequency for the downlink multi-user multi-input-multi-output (MU-MIMO).
DL Channel Distortion	Indicates the channel distortion (in dB) for the downlink MU-MIMO.
DL Multipath Distortion	Indicates the downlink MIMO multipath distortion (in dB). The value of this parameter indicates how suitable the downlink MIMO channel is for the MU-MIMO operation.
Uplink Details	
Max EIRP	The maximum EIRP configured for the uplink.
Current EIRP	The current EIRP in dBm.
UL MCS	MCS of the uplink.
UL Backoff	Indicates the amount (in dB) of power backoff for the uplink. The Tx Power is reduced if there is link budget during the top modulation mode to improve the spectral efficiency.

Session

When you click on the **Session** tab on the C100 dashboard page, the **Session** page appears (as shown in [Figure 52](#)).

The **Session** page provides information (read-only) about the registration state of CPEs, registration count of CPEs, and the RADIUS session details.

Figure 52: The Session page

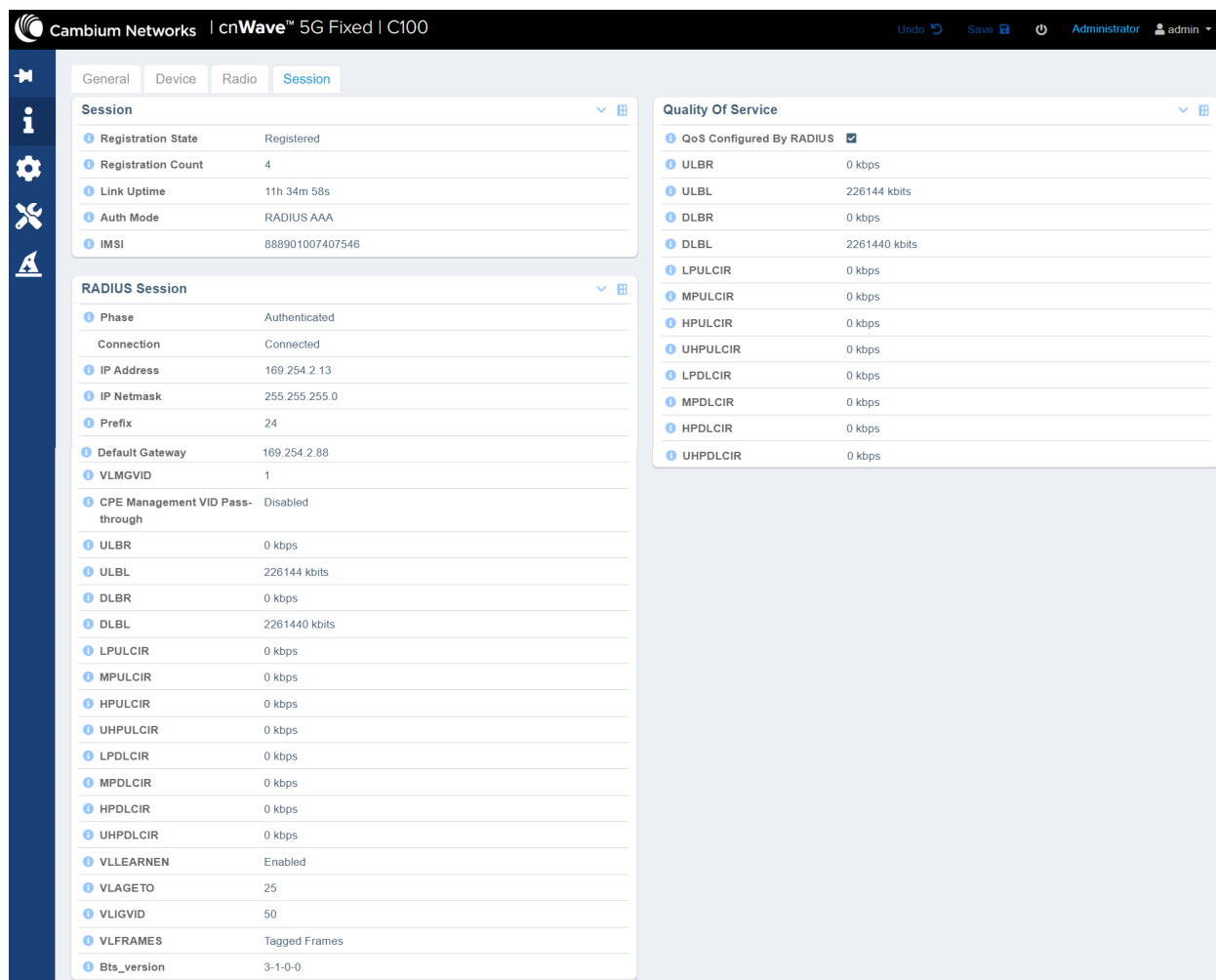


Table 32 lists and describes parameters available on the **Session** page.

Table 32: Parameters in the Session page

Parameter	Description
Session	
Registration State	<p>Indicates the progress that a CPE (device) has made to enter the network.</p> <p>This parameter supports the following device transition states:</p> <ul style="list-style-type: none"> • Down - Indicates that the device is yet to attach to a BTS. • Attaching - Indicates the device has attached to the BTS radio. • Authenticating - Indicates the device is authenticating (using Radius) with the BTS. • Configuring - Indicates that the CPE is being configured. • Registered - Indicates that the CPE is ready to pass user traffic.

Parameter	Description
Registration Count	Number of times that the CPE has successfully registered to the BTS. Note: The value of this parameter is reset to zero at the time of restarting the system.
Link Uptime	Time (in seconds) at which the last successful registration of the link is available for the CPE.
Auth Mode	Indicates the CPE authentication mode. This parameter supports the following values: <ul style="list-style-type: none"> None: CPEs are allowed to connect to the BTS without authentication. In this mode, user traffic is bridged when the CPE gets connected. RADIUS AAA: CPEs are authenticated to a RADIUS AAA back-end server. A CPE might not bridge the user traffic until it is authenticated.
IMSI	Unique number used for identifying a subscriber in a cellular network. Each subscriber is associated with a unique IMSI. The IMSI is usually obtained from a CPE's SIM card. If there is no SIM for a CPE, then it is derived from the CPE's serial number.
RADIUS Session	
Phase	Indicates the authentication phase.
Connection	Determines the connection state.
IP Address	The Radius-supported IP address that is assigned to the network interface and used for managing the device.
IP Netmask	The Radius-supported netmask for the IP address, which is assigned to the network interface and used for managing the device.
Prefix	The IP network prefix, which is derived from the Radius-supported IP netmask (assigned to the network interface and used for the device management).
Default Gateway	The Radius-supported IP address of a system (computer) in the current network, which acts as a gateway.
VLMGVID	The VLAN ID that is used to communicate with BTS and CPE for the management purpose.
CPE Management VID Pass-through	Determines whether the Management VID traffic (VLMGVID) is allowed to or from the CPE wired interface. Default value: Enabled Note: You can configure this parameter using the System > General page of C100 UI.
ULBR	The uplink bit rate or sustained uplink rate (in kbps) at which each CPE has registered with the BTS. This BTS is replenished with credits for transmission.
ULBL	Indicates the uplink bit limit or uplink burst allocation (in kbits). The maximum amount of data that each CPE is allowed to transmit before being recharged at the sustained uplink data rate (in kbps).
DLBR	The downlink bit rate or sustained downlink rate (in kbps) at which the BTS is

Parameter	Description
	replenished with credits (tokens) for transmission to each of the CPEs in its sector.
DLBL	Indicates the downlink bit limit or downlink burst allocation (in kbits). The maximum amount of data that the BTS is allowed to transmit to any registered CPE before it is replenished with the transmission credits at the sustained downlink data rate (in kbps).
LPULCIR	The minimum rate (in kbps) at which a low priority traffic is sent over the uplink (unless Committed information rate (CIR) is oversubscribed or the RF link quality is degraded).
MPULCIR	The minimum rate (in kbps) at which a medium priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
HPULCIR	The minimum rate (in kbps) at which a high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
UHPULCIR	The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
LPDLCIR	The minimum rate (in kbps) at which a low priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
MPDLCIR	The minimum rate (in kbps) at which a medium priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
HPDLCIR	The minimum rate (in kbps) at which a high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
UHPDLCIR	The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
VLEARNEN	Determines whether the CPE must add the VLAN IDs (VIDs) of upstream frames to the VID table (VLAN learning). This parameter supports the following values: <ul style="list-style-type: none"> • Enabled: Indicates that the CPE must add the VIDs to the VID table. • Disabled: Indicates that the CPE must not add the VIDs to the VID table. Default value: Enabled Note: The CPE might drop any frames with VIDs that are not stored in the VID table.
VLGETO	The period (in minutes) during which the CPE must dynamically keep learning about VIDs. This parameter supports values ranging from 5 to 1440 (in minutes). Default value: 25 (in minutes) You can configure this parameter using the System > General page of C100 UI. Note: VIDs that you set for the Untagged Ingress VID and Management VID parameters do not time out.

Parameter	Description
VLIQVID	The VLAN ingress VID that is used for incoming untagged frames. This VID corresponds to the Qtag for 802.1Q frames (if the VLAN port type is Q) or the C-tag for 802.1ad frames (if the VLAN port type is Q-in-Q).
VLFRAMES	Indicates the allowed frame types (all, untagged, or tagged). The type of arriving frames that the CPE must tag by using the VID, which is stored in the Untagged Ingress VID parameter. Default value: All Fames
Bts_Version	Specifies the build version number of BTS. Example: 3-1-0-0 This parameter supports numerical values. The value of this parameter is determined based on the following points specific to release types: <ul style="list-style-type: none"> • Major: This release type is not frequent and implies a significant feature addition or an architectural change. • Minor: This release type is often and implies incremental improvements and corrections. • Point: This release type implies a collection of bug fixes from the previous minor release. • Dot: This release type implies an emergency bug fix or a customer-specific change. Note: A dot release is not posted publicly, and a bug fix gets rolled into the next point release.
Quality of Service	
QoS Configured by RADIUS	Determines whether the QoS configuration is set through RADIUS AAA. At boot, locally configured settings are used for the QoS network configuration. These settings are overridden by RADIUS-supplied settings during registration.
For the following parameter descriptions, refer to the RADIUS Session section of this table:	
ULBR	
ULBL	
DLBR	
DLBL	
LPULCIR	
MPULCIR	
HPULCIR	
UHPULCIR	
LPDLCIR	

Parameter	Description
MPDLCIR	
HPDLCIR	
UHPDLCIR	


Configuring C100 (CPE)

Using the C100 UI, you can configure, view, and manage the CPE configurations. This section covers the following CPE-specific configurations:

- [Configuring System settings](#)
- [Configuring tools](#)
- [Setting up a wizard](#)

Configuring system settings

The **System** page in the C100 UI allows you to view and configure the required settings for the device such as radio, interface, and session related parameters.

You must use the **System** icon () in the C100 dashboard to configure, view, and manage the system settings for CPEs.

The **System** page in the C100 dashboard contains the following tabs:

- [General](#)
- [VLAN](#)
- [Management](#)
- [Radio](#)
- [Interface](#)
- [Session](#)
- [RADIUS Authentication](#)

General

The **General** page allows you to configure generic system settings such as system name, its location, and contact person details. You can also configure the network settings such as IP address, prefix, and default gateway.

To access and configure the system settings, perform the following steps:


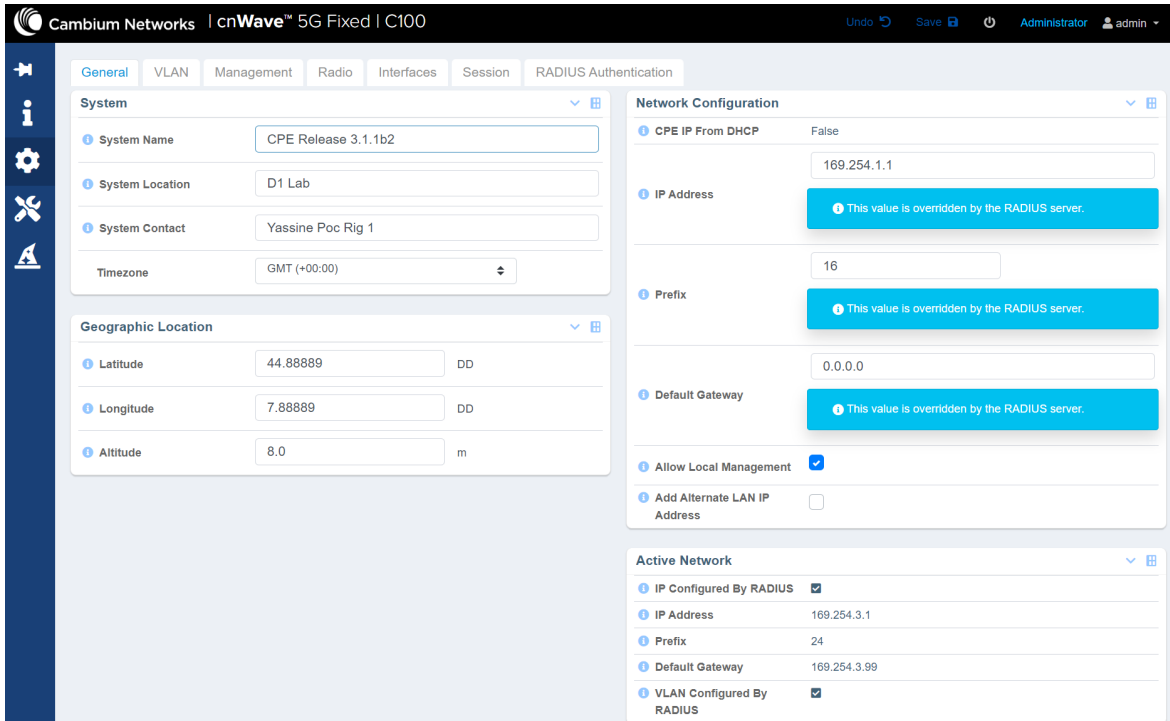
1. Log on to the C100 UI (as described in the [Accessing the C100 UI](#) section).
The main C100 dashboard page appears (as shown in [Figure 49](#)).
2. On the left navigation column, click the **System** icon ().
A system setting-specific page appears, as shown in [Figure 53](#). By default, the **General** tab is selected.

Figure 53: The System page - General settings



3. Set the values for each parameter, as described in Table 33.

Table 33: Parameters on the General page

Parameter	Description
System	
System Name	An administratively assigned name of the device. When using DNS, this name must be the device's fully qualified domain name (FQDN). Provide an appropriate name in the text box for the system.
System Location	The physical location of the device node. Provide appropriate location details in the text box.
System Contact	Contact details of the device administrator. Enter appropriate details in the text box.
Timezone	Time zone that you want to set for the system. Select the required time zone from the drop-down list. Example: GMT (+00:00)
Geographic Location	
Latitude	Latitude (in DD) of the geographical location where the CPE is located. Enter an appropriate value in the text box.

Parameter	Description
	<p>Note: Decimal degrees (DD) indicates latitude and longitude geographic coordinates in decimal fractions of a degree. Example: A positive latitude is north of the equator and a negative latitude is south of the equator. A DD to five decimal places is precise to approximately one metre.</p>
Longitude	<p>Longitude (in DD) of the geographical location where the CPE is located.</p> <p>Enter an appropriate value in the text box.</p> <p>Example: A positive longitude is east of the Prime Meridian and a negative longitude is west of the Prime Meridian.</p>
Altitude	<p>Altitude (in m) of the geographical location relative to mean sea level (MSL).</p> <p>Enter an appropriate value in the text box.</p>
Network Configuration	
CPE IP From DHCP	<p>Determines whether the CPE's IP network configuration is supplied by a DHCP server.</p> <p>The following values are supported:</p> <ul style="list-style-type: none"> • True: If enabled, the DHCP server supplies the CPE's IP network configuration. • False: If disabled and the Authentication Mode is RADIUS AAA, the configured RADIUS server supplies the CPE's IP network configuration. <p>If disabled and the Authentication Mode is None, the CPE's IP network configuration is set locally at each CPE.</p> <p>You can configure this parameter using the CPE Provisioning page of the B1000 UI.</p>
IP Address	<p>The IP address that is assigned to the network interface and used for the device management.</p> <p>Provide appropriate value in the text box.</p> <p>Note: The values of this parameter is overridden by the RADIUS server (if connected).</p>
Prefix	<p>The IP network prefix that is assigned to the network interface and used for the device management.</p> <p>Provide appropriate value in the text box.</p> <p>Note: The values of this parameter is overridden by the RADIUS server (if connected).</p>
Default Gateway	<p>The IP address of the default gateway (if any) that is used for the device management.</p> <p>Provide appropriate value in the text box.</p>

Parameter	Description
	<p>Note: The values of this parameter is overridden by the RADIUS server (if connected).</p>
Allow Local Management	<p>Determines whether you want to manage this device through the local management interface or the radio link.</p> <p>By default, the check box is selected (enabled), indicating that the local management interface is used for this device management.</p> <p>If you disable or uncheck the Allow Local Management check box, all local management traffic is dropped and the device management is possible only through the radio link.</p> <p>Note: If you disable this check box, this setting can only be re-enabled by remote management or by resetting to factory defaults.</p>
Add Alternate LAN IP Address	<p>Determines whether you want to configure or add a second IP address (alternate LAN IP address) for the device management. This alternate LAN IP address is accessible only when connected to the Ethernet port.</p> <p>If you select the check box, the following parameters appear:</p> <ul style="list-style-type: none"> • Alternate LAN IP Address • Alternate LAN Prefix
Alternate LAN IP Address	<p>The alternate management IP address that is accessible only when connected to the Ethernet port. The management performed using this interface may be untagged traffic only. The system does not implement any configured management VID.</p> <p>Note: The alternate LAN IP configuration is not installed if it intersects with the primary management IP address configuration (which is assigned by DHCP or RADIUS).</p> <p>Type the alternate LAN IP address in the text box (if required). By default, this text box displays the primary IP address that is currently used by the management agent for the operation.</p> <p>A warning message is visible, indicating that the alternate LAN IP address is installed When the CPE next registers on reboot or the Activate Saved Alternate LAN IP Configuration button is clicked. Otherwise, it overlaps with the primary IP address (which is assigned by DHCP or RADIUS) and the alternate LAN IP address is not installed.</p>
Alternate LAN Prefix	<p>The IP network prefix of the alternate LAN IP address.</p> <p>Default value: 16</p> <p>A warning message is visible, indicating that the alternate LAN prefix is installed When the CPE next registers on reboot or the Activate Saved Alternate LAN IP Configuration button is clicked.</p> <p>Type an appropriate value in the text box (if required).</p>
Activate Saved Alternate LAN IP Configuration	<p>An option to update the alternate LAN IP configuration and use the currently saved settings.</p>

Parameter	Description
	Note: If you are currently managing the device using the previous alternate LAN IP address, then the contact with the device is lost until you use the new alternate IP address.
Active Network - Specifies the parameters that are configured using the RADIUS Server. Following are the read-only parameters:	
IP Configured by RADIUS	<p>Indicates whether the network configuration is set through RADIUS AAA.</p> <p>The check box is selected if the network configuration is set through RADIUS AAA.</p> <p>Note: On a CPE that is configured for RADIUS authentication, the network configuration uses the locally configured settings and swaps to the Radius-supported settings when the RADIUS authentication takes place.</p> <p>The locally configured settings may be overridden by the Radius-supported settings during registration.</p>
IP Address	The IP address that is assigned to the network interface and used for the device management.
Prefix	The IP network prefix that is assigned to the network interface and used for the device management.
Default Gateway	The IP address of the default gateway (if any) that is used for the device management.
VLAN Configured by RADIUS	<p>Indicates whether the VLAN configuration is set through RADIUS AAA.</p> <p>At boot, locally configured settings are used for the VLAN network configuration. These settings are overridden by RADIUS-supplied settings during registration.</p> <p>The check box is selected if the network configuration is set through RADIUS AAA.</p>

4. Click **Save** (located at the top right side of the page) to save the configuration changes.

VLAN

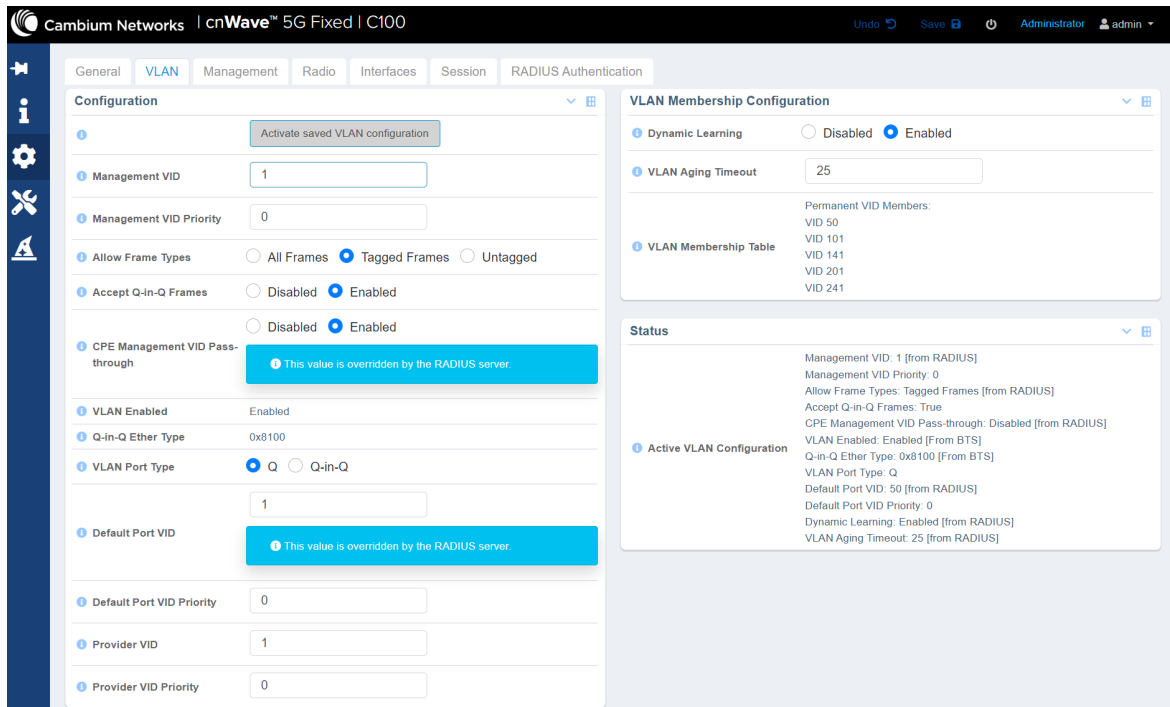
The **VLAN** page allows you to configure VLANs and related settings for the CPE device. This page also displays the active VLAN configuration.

To access and configure the VLAN settings, perform the following steps:

1. From the main C100 dashboard page, navigate to **System > VLAN**.

The VLAN page appears, as shown in [Figure 54](#).

Figure 54: The VLAN page



2. Set the values for each parameter, as described in Table 33.

Table 34: Parameters on the VLAN page

Parameter	Description
Configuration	
Activate Saved VLAN Configuration	<p>An action that updates the live VLAN configuration to use the currently saved settings unless they are overridden by RADIUS.</p> <p>Note: If you have changed Management VID, then you will lose contact with the device until you make the corresponding changes.</p> <p>If you change any parameter in this VLAN Configuration section, you must save the changes and then click the Activate Saved VLAN Configuration button. When the CPE reboots, it uses the saved VLAN configuration.</p>
Management VID	<p>The VLAN ID used to communicate with BTS and CPE for the management purpose.</p> <p>Type an appropriate value in the text box.</p> <p>Default value: 1 - which implies that there is no VLAN in the system.</p> <p>You can set up an ID value between 2 and 4094.</p>
Management VID Priority	The priority value that is set for the management VLAN ID.
Allow Frame Types	Type of incoming or arriving frames that the CPE must tag using the VID, which is stored in the Untagged Ingress VID parameter.

Parameter	Description
	<p>Following options are supported:</p> <ul style="list-style-type: none"> • All Frames • Tagged Frames • Untagged <p>Select the required incoming frame type.</p> <p>Default value: All Frames</p> <p>Note: The values of this parameter is overridden by the RADIUS server (if connected).</p>
Accept Q-in-Q Frames	<p>Determines whether a Q-in-Q frames are accepted or blocked.</p> <p>This option is valid for the Q-in-Q port as you might force the blocking of existing 802.1ad Q-in-Q frames. Then, only untagged or single tagged packets come in and go out of the Ethernet interface.</p> <p>if a Q-in-Q frame is about to ingress or egress the Ethernet interface and if this parameter is disabled, then the Q-in-Q frames are dropped.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Disabled • Enabled <p>Default value: Disabled</p> <p>Select the required option.</p>
CPE Management VID Pass-through	<p>Determines whether the Management VID traffic (VLMGVID) is allowed to or from the CPE wired interface.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Disabled • Enabled <p>Default value: Enabled</p> <p>Select the required option.</p> <p>Note: The values of this parameter is overridden by the RADIUS server (if connected).</p>
VLAN Enabled	<p>Determines whether the VLAN functionality for the BTS and all linked CPEs is enabled.</p> <p>If this parameter is disabled, then you cannot modify VLAN-related parameters on this C100 UI. You must enable the VLAN using the System > General page of the B1000 UI. For more details, refer to Table 7.</p>
Q-in-Q Ether Type	<p>The Ether types for Q-in-Q (802.1ad) and outer tag (S-Tag).</p> <p>Default value: 0x88a8</p>

Parameter	Description
	You can configure this option using the System > General page of the B1000 UI. For more details, refer to Table 7 . To understand how Q-in-Q works, refer to the Q-in-Q section.
VLAN Port Type	<p>Indicates the VLAN tunnel technique or port type used by the Ethernet service provider for segregating the traffic.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Q: Indicates that it operates on 802.1q C-tags only. • Q-in-Q: Indicates that it must add and remove the S-tag, and add a C-tag (if necessary) for untagged packets. <p>Note: The VLAN port type configures the behaviour of the local Ethernet only and the internal management interfaces always operate as Q ports.</p> <p>Default value: Q</p> <p>Select the required port type.</p>
Default Port VID	<p>VID that is used for untagged frames and corresponds to the Q-tag for 802.1Q frames (if the VLAN Port Type is Q) or the C-tag for the 802.1ad frames (if the VLAN Port Type is Q-in-Q).</p> <p>Default value: 1</p> <p>Note: The values of this parameter is overridden by the RADIUS server (if connected).</p>
Default Port VID Priority	<p>The priority value that is set for the default VID VLAN.</p> <p>Default value: 0</p>
Provider VID	<p>The provider VID that is used for the S-tag. This VID is used only if the Port Type is q-in-Q and for the S-tag.</p> <p>If an existing 802.1Q frame arrives, the provider VID is what is used for adding and removing the outer S-tag. If an untagged frame arrives to a Q-in-Q port, the provider VID is the S-tag and the Default Port VID (or the port VID MAC address mapping, if valid) is used for the C-tag.</p> <p>Default value: 1</p>
Provider VID Priority	<p>The priority value that is set for the default VID VLAN.</p> <p>Default value: 0</p>
VLAN Membership Configuration	
Dynamic Learning	<p>Determines whether the CPE must add the VLAN IDs (VIDs) of upstream frames to the VID table.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Disabled: The CPE does not add the VIDs. • Enabled: The CPE adds the VIDs. <p>The CPE drops frames with VIDs, which are not stored in the VID table.</p>

Parameter	Description
	<p>Default value: Enabled</p> <p>Select the required option.</p> <p>Note: If you modify the values of this parameter, the value is overridden during RADIUS AAA registration.</p>
VLAN Aging Timeout	<p>Specifies the period (in minutes) during which the CPE must dynamically keep learning about VLANs.</p> <p>This parameter supports values ranging from 5 to 1440 (in minutes).</p> <p>Default value: 25 (in minutes)</p> <p>Provide an appropriate value in the text box.</p> <p>Note: VLANs that you set for the Untagged Ingress VLAN and Management VLAN parameters do not time out.</p>
VLAN Membership Table	<p>Lists the permanent VLAN members.</p> <p>This is a read-only parameter.</p>
Status	
Active VLAN Configuration	Details a summary of the active VLAN configuration.

3. Click **Save** to apply the changes.

Management

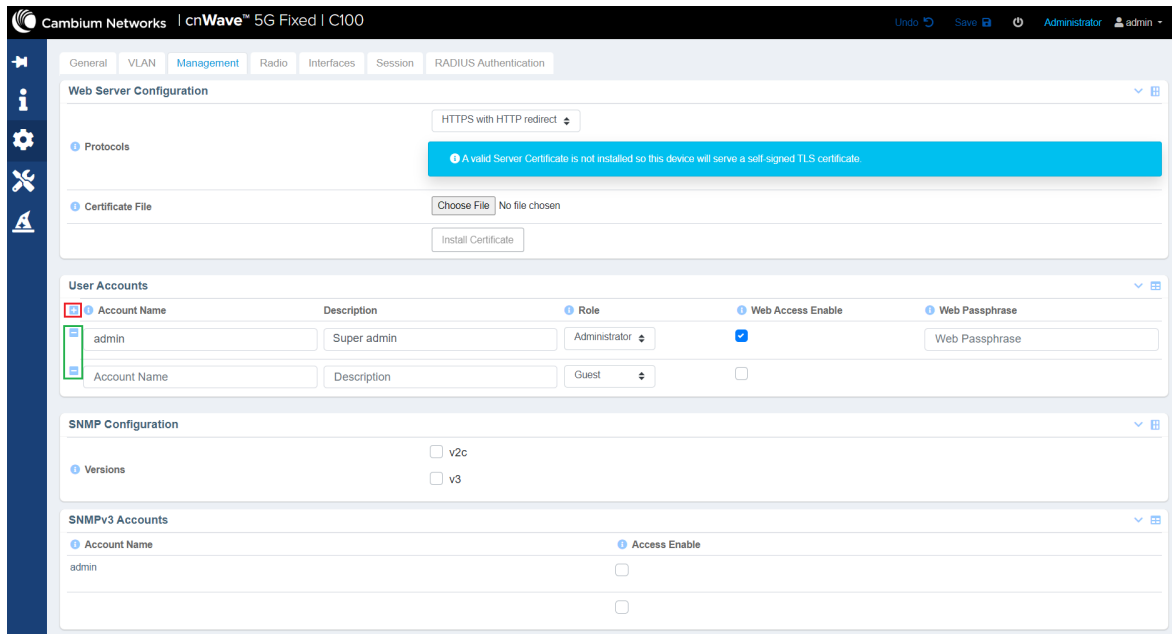
The **Management** page allows you to set user account and SNMP configuration related information. This configuration allows the users to manage the C100 dashboard and the CPEs using SNMP.

To view and configure the management settings, perform the following steps:

1. From the main C100 dashboard page, navigate to **System > Management**.

The **Management** page appears, as shown in [Figure 55](#).



Figure 55: The Management page



2. Set the values for each parameter, as described in Table 35.

Table 35: Parameters in the Management page

Parameter	Description
Web Server Configuration	
Protocols	<p>Type of protocol that must be configured for accessing and managing the web UI of CPE.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • HTTP Only: Indicates that only HTTP is available. • HTTPS Only - Indicates that only HTTPS is available. • HTTP and HTTPS: Indicates that both HTTP and HTTPS are available. • HTTPS with HTTP redirect: Indicates that both HTTP and HTTPS are available, but an incoming HTTP connection is automatically redirected to HTTPS. <p>Default value: HTTPS with HTTP redirect</p> <p>Select the required protocol from the drop-down list.</p> <p>Note: Except for the HTTP option, a message is visible for the rest of the options. This message indicates that a valid server certificate is not installed, and the device serves a self-assigned TLS certificate.</p>

Parameter	Description
Certificate File	<p>An option to browse and upload a certificate file (.PEM) from a location locally. This certificate file must contain a device private key and matching certificate that is signed by the trusted CA.</p> <p>To upload a certificate file (.PEM) from the desired location locally, perform the following steps:</p> <ol style="list-style-type: none"> Click Choose File. A file folder appears. Browse the location where you have saved the required certificate file (.PEM) on your machine. Click Open. The certificate file is selected, and the file name appears next to the Choose File button. Click Install Certificate. The selected certificate file is installed, which is authenticated and encrypted.
User Accounts	
Account Name	<p>Name of the account used for administering the CPE device. This name must be unique and start with a letter. An account name can contain lower case letters, numbers, and hyphens.</p> <p>Provide an appropriate name in the text box. Example: admin</p> <p>The account name can belong to a guest, an administrator, an engineer, a support team member, or a user. You can add multiple names to the user account using the text boxes.</p> <p>Note: To add a new user account row, use the  icon located beside the Account name parameter (as shown in Figure 55). To delete a user account, use the  icon located beside the corresponding account name.</p>
Description	<p>A brief description of the account.</p> <p>Provide a brief description for the user account that you want to add. Example: Super admin</p>
Role	<p>Specifies the role of the user who wants to access the CPE device.</p> <p>This parameter supports the following roles, which have different capabilities and server different functions:</p> <ul style="list-style-type: none"> Guest: This role has limited, read-only access to the device configuration and status. All fields in the web UI are read-only and some of them are also not available for guest roles. The guest roles have limited SNMP access with a read-only view of MIB-II.

Parameter	Description
	<ul style="list-style-type: none"> • User: This role has limited access to the device configuration and status. Some UI fields are read-only and some fields are not available on the web UI. The user roles cannot change any parameters on the UI. • Administrator: This role has visibility of the device configuration and status. These role can view, configure, and change everything in the UI, but cannot access the sensitive security information. • Security: This role (for example, a security officer) has visibility of the device configuration and status, including sensitive security information. • Support: This role (for example, a support agent) can access diagnostics information for the product support purpose. • Engineer: This role (for example, an engineer) has privileged write access to specific engineering settings and read access to engineering status information. • Factory: This role (for example, a factory operator) has privileged write access to the device customisation settings such as ESN and SKU. <p>Select an appropriate option from the drop-down list.</p>
Web Access Enables	<p>Determines whether the access for web UI of the CPE device is enabled for the selected role.</p> <p>Select the check box if you want to enable the web access for the required user role.</p> <p>Note: Multiple users are allowed to access the UI simultaneously.</p>
Web Passphrase	<p>The passphrase (password) that is assigned to the user role of this account for accessing the web UI.</p> <p>Type an appropriate password in the text box.</p>
SNMP Configuration	
Versions	<p>The version of the SNMP protocol that is supported by the agent running on this CPE device.</p> <p>The following SNMP protocol versions are supported:</p> <ul style="list-style-type: none"> • V2c: This is an obsolete version with weak security. • V3 <p>Choose the required check box.</p> <p>Note: A message is visible in this field, providing an option to download the SNMP MIB files directly from the device (as shown in Figure 56). Using the SNMP MIB files, you can access VLAN and QoS attributes of CPEs.</p>

Parameter	Description
Port	<p>This parameter appears only when you select an SNMP version (V2c or V3).</p> <p>Indicates the network port number assigned to the SNMP agent, which is running on the device.</p> <p>Default value: 161</p> <p>Provide an appropriate value in the text box.</p>
The following parameters appear only when you set V2c in the Versions field:	
Read/Only Community	<p>Name of the SNMP V2c community for read-only access to the device.</p> <p>Provide an appropriate value in this text box.</p>
Read/Write Community	<p>Name of the SNMP V2c community for read-write access to the device.</p> <p>Provide an appropriate value in this text box.</p>
SNMP Account - This section is applicable only when you set V3 in the Versions field (as shown in Figure 56).	
Account Name	<p>The account name that is used for authentication to the CPE device.</p> <p>This is read-only parameter that contains account names, which you added in the User Accounts section.</p>
Access Enable	<p>Determines whether the permission is set for this account name to access the CPE device using SNMPv3 credentials (which are configured in this SNMPv3 Accounts section).</p> <p>Select the check box for the required account names. This setting permits the user role to access the CPE device using SNMP.</p> <p>Note: To modify this parameter, you must enable V3 using the Versions parameter in the SNMP Configuration section.</p>
When you enable the access for the account names using the Access Enable parameter, the following parameters specific to authentication appear (as shown in Figure 56):	
Authentication Type	<p>Indicates the authentication type to use.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • None • MD5 • SHA1 <p>Select the required option from the drop-down list.</p>
Authentication Passphrase	<p>The authentication passphrase that is assigned to the user. This passphrase must be the same one that is set at the SNMP site for the user.</p>

Parameter	Description
	<p>The value of this parameter can contain any combination of ASCII characters. The value must consist of eight characters in length.</p> <p>Type a valid value in the text box.</p>
Privacy Protocol	<p>Specifies the protocol that must be used for account privacy.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • None • DES • AES <p>Select the required option from the drop-down list.</p>
Privacy Passphrase	<p>The privacy passphrase that is assigned to the user. This passphrase must be the same one that is set at the SNMP site for the user.</p> <p>The value of this parameter can contain any combination of ASCII characters. Also, the value must consist of eight characters in length.</p> <p>Type a valid value in the text box.</p> <p>If you do not provide any privacy passphrase in this text box, then the value is assumed to be the same as the authentication passphrase.</p>

Figure 56 is an example of configuring the **Management** page for the CPE.

Figure 56: The Management page - C100 UI

The screenshot displays the Management page of the C100 UI, organized into several sections:

- Web Server Configuration:** Includes a dropdown for "HTTPS with HTTP redirect" and a message: "A valid Server Certificate is not installed so this device will serve a self-signed TLS certificate." There is also a "Certificate File" section with a "Choose File" button and an "Install Certificate" button.
- User Accounts:** A table with columns: Account Name, Description, Role, Web Access Enable, and Web Passphrase.

Account Name	Description	Role	Web Access Enable	Web Passphrase
admin	Super admin	Administrator	<input checked="" type="checkbox"/>
user	user1	User	<input checked="" type="checkbox"/>	Web Passphrase
- SNMP Configuration:** Includes "Versions" with checkboxes for v2c and v3 (v3 is selected). A message states: "An archive of all MIB modules for this device may be downloaded directly from this device here: mbs.lar.gz". The "Port" is set to 161.
- SNMPv3 Accounts:** A table with columns: Account Name, Access Enable, Authentication Type, Authentication Passphrase, Privacy Protocol, and Privacy Passphrase.

Account Name	Access Enable	Authentication Type	Authentication Passphrase	Privacy Protocol	Privacy Passphrase
admin	<input checked="" type="checkbox"/>	SHA1	Authentication Passphrase	AES	Privacy Passphrase
user1	<input checked="" type="checkbox"/>	SHA1	AES

3. Click **Save** to apply the settings.

Radio

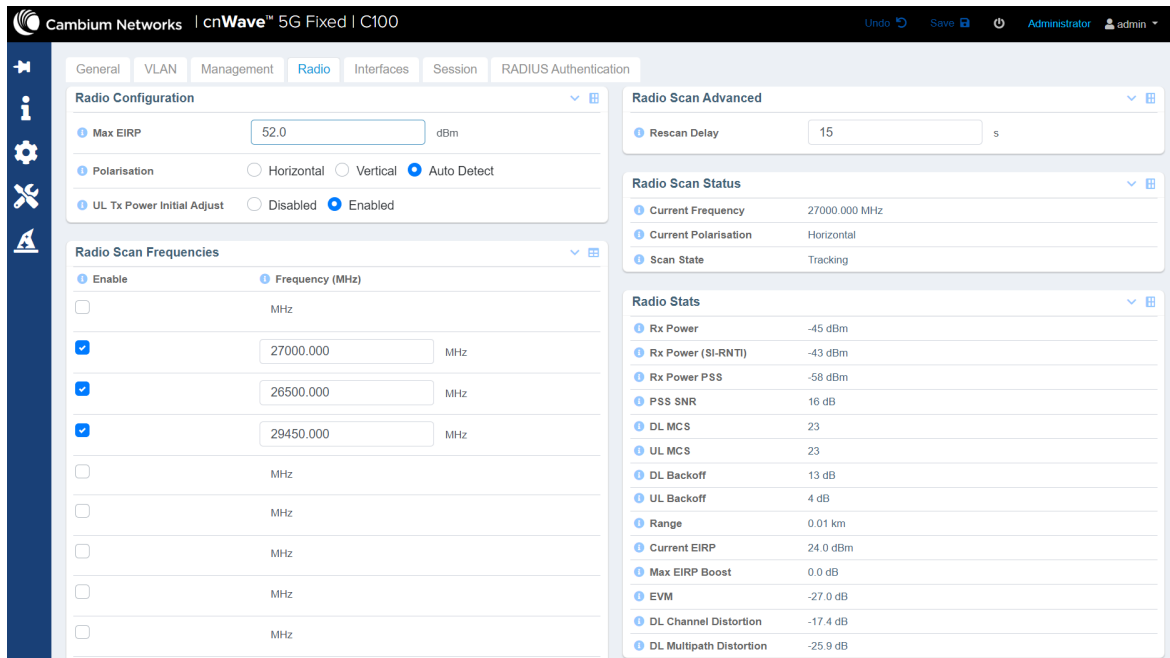
This **Radio** page allows you to configure the radio configuration parameters and radio scan frequencies. It also provides information about the radio scan status and statistics.

To view and configure the radio settings, perform the following steps:

1. From the main C100 dashboard page, navigate to **System > Radio**.

The **Radio** page appears, as shown in [Figure 57](#).

Figure 57: The Radio page - C100 UI



2. Set the values for each parameter, as described in Table 36.

Table 36: Parameters on the Radio page

Parameter	Description
Radio Configuration	
Max EIRP	<p>The maximum EIRP configured value (in dBm). Type an appropriate value in the text box.</p> <p>Note: Ensure that the value is greater than or equal to 20.0 dBm.</p>
Polarisation	<p>Determines the antenna polarisation settings. This parameter supports the following polarisation settings:</p> <ul style="list-style-type: none"> Horizontal Vertical Auto Detect (the recommended value for the CPE) <p>Select the required polarisation for the antenna.</p>
UL Tx Power Initial Adjust	<p>Indicates the uplink initial transmit power control mode for CPEs. This parameter supports the following options:</p> <ul style="list-style-type: none"> Disabled - If this parameter is disabled, CPEs use their configured maximum transmit power.

Parameter	Description
	<ul style="list-style-type: none"> Enabled - If this parameter is enabled, CPEs adjust their transmit power to reach the BTS target receive power before starting transmission. <p>By default, this parameter is Enabled.</p> <p>Select the required option.</p>
Radio Scan Frequencies	<p>List of required frequencies (in MHz) that the CPE can use.</p> <p>You can also enable the configured frequency, for effective use, by selecting the corresponding frequency check box.</p> <p>Type appropriate frequency values (in MHz) and select the check box in the corresponding row.</p> <p>Note: A CPE can have a number of frequencies that can be enabled or disabled per sector. However, the BTS can have only one frequency.</p>
Radio Scan Advanced	
Rescan Delay	<p>The delay period (in seconds) before rescanning radio frequencies when the signal is lost.</p> <p>Type an appropriate value in the text box.</p>
Following parameters are read-only:	
Radio Scan Status	
Current Frequency	Value (in MHz) of the current operating frequency.
Current Polarisation	The current antenna polarization.
Scan State	<p>Indicates the radio scan state.</p> <p>Example: Tracking</p>
Radio Stats	
Rx Power	The Receive power of data symbols (in dBm).
Rx Power (SI-RNTI)	<p>Indicates the Receive power (in dBm) for the SI-RNTI on the strongest beam.</p> <p>This Receive power might be lower than received data. This is due to CPE being within the 6 dB bandwidth of the selected SIRNTI beam and not necessarily on its peak.</p> <p>Note: The CPE reports the SI-RNTI statistics such as bandwidth (in MHz) and DL Rx Power (SI-RNTI) in dBm.</p>
Rx Power PSS	The Receive power for the PSS symbols (in dBm) at the CPE.
PSS SNR	The SNR of the PSS symbols (in dB) at the CPE.
DL MCS	The Modulation and Coding Scheme (MCS) index of the downlink.
UL MCS	The MCS index of the uplink.
DL Backoff	Indicates the amount (in dB) of power backoff for the downlink.

Parameter	Description
	<p>This is the amount by which the BTS is currently reducing its power from the maximum configured EIRP when transmitting to the CPE. The BTS uses the greatest backoff that it can achieve while still maintaining the downlink throughput required by the CPE.</p> <p>Note: Backing off the BTS transmit power means the power allocation maximized for the CPE, which also requires for minimizing interference.</p>
UL Backoff	<p>Indicates the amount (in dB) of power backoff for the uplink.</p> <p>The Tx Power is reduced if there is link budget during the top modulation mode to improve the spectral efficiency.</p>
Range	The distance measured between BTS and CPE (in Km).
Current EIRP	The current EIRP value in dBm.
Max EIRP Boost	The maximum EIRP boost that the device is currently allowed to use (in dB).
EVM	EVM (in dB) of the downlink signal.
DL Channel Distortion	<p>Value (in dB) that indicates the distortion (or degraded) length of the downlink MU-MIMO.</p> <p>Note: Values that are less than -10 are considered good values.</p>
DL Multipath Distortion	<p>Indicates the downlink MIMO multipath distortion (in dB).</p> <p>The value of this parameter indicates how suitable the downlink MIMO channel is for the MU-MIMO operation.</p>

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

Interface

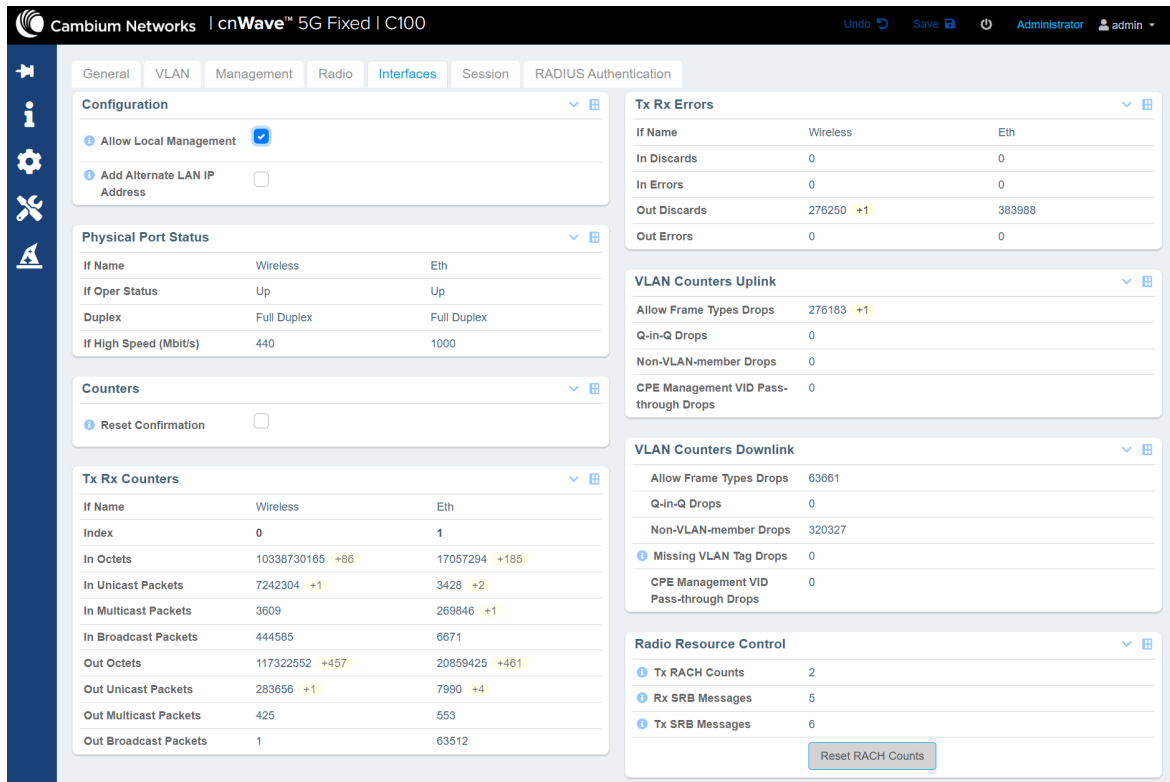
The **Interface** page allows you to configure the local management of interfaces. It also provides statistical information about all the CPE interfaces (such as Copper).

To configure and view the interface settings, perform the following steps:

1. From the main C100 dashboard page, navigate to **System > Interface**.

The **Interface** page appears, as shown in [Figure 58](#).

Figure 58: The Interface page



2. View or monitor the interface related parameters, as described in Table 37.

Table 37: Parameters in the Interface page

Parameter	Description
Configuration	
Allow Local Management	<p>Determines whether you want to manage this device through the local management interface or the radio link.</p> <p>By default, the check box is selected (enabled), indicating that the local management interface is used for this device management.</p> <p>If you disable or uncheck the Allow Local Management check box, all local management traffic is dropped and the device management is possible only through the radio link.</p> <p>Note: If you disable this check box, this setting can only be re-enabled by remote management or by resetting to factory defaults.</p>
Add Alternate LAN IP Address	<p>Determines whether you want to configure or add a second IP address (alternate LAN IP address) for the device management. This alternate LAN IP address is accessible only when connected to the Ethernet port.</p> <p>If you select the check box, the following parameters appear:</p>

Parameter	Description
	<ul style="list-style-type: none"> Alternate LAN IP Address Alternate LAN Prefix
Alternate LAN IP Address	<p>The alternate management IP address that is accessible only when connected to the Ethernet port. The management performed using this interface may be untagged traffic only. The system does not implement any configured management VID.</p> <p>Note: The alternate LAN IP configuration is not installed if it intersects with the primary management IP address configuration (which is assigned by DHCP or RADIUS).</p> <p>Type the alternate LAN IP address in the text box (if required). By default, this text box displays the primary IP address that is currently used by the management agent for the operation.</p> <p>A warning message is visible, indicating that the alternate LAN IP address is installed When the CPE next registers on reboot or the Activate Saved Alternate LAN IP Configuration button is clicked. Otherwise, it overlaps with the primary IP address (which is assigned by DHCP or RADIUS) and the alternate LAN IP address is not installed.</p>
Alternate LAN Prefix	<p>The IP network prefix of the alternate LAN IP address.</p> <p>Default value: 16</p> <p>A warning message is visible, indicating that the alternate LAN prefix is installed When the CPE next registers on reboot or the Activate Saved Alternate LAN IP Configuration button is clicked.</p> <p>Type an appropriate value in the text box (if required).</p>
Activate Saved Alternate LAN IP Configuration	<p>An option to update the alternate LAN IP configuration and use the currently saved settings.</p> <p>Note: If you are currently managing the device using the previous alternate LAN IP address, then the contact with the device is lost until you use the new alternate IP address.</p>
Physical Port Status	
If Oper Status	Indicates the working status (up or down) of wireless and Ethernet ports for CPE.
Duplex	Indicates the capability mode of wireless and Ethernet ports to send and receive data.
If High Speed (Mbit/s)	Indicates the data transmission speed of wireless and Ethernet ports (in Mbits per second).
Counters	
Reset Confirmation	An option to reset the SNMP MIB-II interface counters.

Parameter	Description
	When you select the check box, the Reset Counters button appears. You can use this button to reset the SNMP MIB-II interface counters.
<p>Tx Rx Counters - Applicable to data ports and wireless.</p> <p>The data report is listed in the following columns:</p> <ul style="list-style-type: none"> • Wireless - Indicates all the data transmitted on the wireless link when it is up. • Eth -Indicates the data that is entering the main Ethernet port. 	
Index	Index number assigned to each counter column.
In Octets	Number of data bytes received by the CPE from a particular connected BTS.
In Unicast Packets	Number of data packets received by the CPE from the BTS.
In Multicast Packets	Number of data packets received by specific two or more CPEs from the BTS.
In Broadcast Packets	Number of data packets received by all the connected CPEs from the BTS.
Out Octets	Number of data bytes sent by the CPEs to the BTS.
Out Unicast Packets	Number of data packets sent by a specific CPE to the BTS.
Out Multicast Packets	Number of data packets sent by specific two or more CPEs to the BTS.
Out Broadcast Packets	Number of data packets sent by all the connected CPEs to the BTS.
<p>Tx Rx Errors - Applicable to data ports and wireless.</p>	
In Discards	Number of incoming data packets discarded by the CPEs.
In Errors	Number of incoming data packets that contain errors.
Out Discards	Number of outgoing data packets (from CPEs) that are marked or labelled as discarded by the CPEs.
Out Errors	Number of outgoing data packets (from CPEs) that contain errors.
<p>VLAN Counters Uplink</p>	
Allow Frame Types Drops	Count of allowed frames type events that are dropped by the CPE in the uplink direction.
Q-in-Q Drops	Count of Q-in-Q events that are dropped by the CPE in the uplink direction.
Non-VLAN-member Drops	Count of non-VLAN member events that are dropped by the CPE in the uplink direction.
CPE Management VID Pass-through Drops	Count of CPE management VID pass-through events that are dropped by the CPE in the uplink direction.

Parameter	Description
VLAN Counters Downlink	
Allow Frame Types Drops	Count of allowed frames type events that are dropped by the CPE in the downlink direction.
Q-in-Q Drops	Count of Q-in-Q events that are dropped by the CPE in the downlink direction.
Non-VLAN-member Drops	Count of non-VLAN member events that are dropped by the CPE in the downlink direction.
Missing VLAN Tag Drops	Count of downlink frames with no tags that are dropped by the CPE. When CPE runs with an VLAN enabled mode, the DL traffic must be tagged as default port VID (in Q and Q-in-Q modes) and provider VID (in the Q-in-Q mode only) are added to any untagged ingress frames before transmitting them to the BTS. Therefore, reciprocal tags are expected to be present on any downlink frames received from the BTS.
CPE Management VID Pass-through Drops	Count of CPE management VID pass-through events that are dropped by the CPE in the downlink direction.
Radio Resource Control	
Tx RACH Counts	Number of registration requests sent by the device using the Random Access Channel (RACH). A registration request is the first message that is transmitted when a suitable BTS signal is locked on.
Rx SRB Messages	Number of Signalling Radio Bearer (SRB) response messages that are received by the device. An increase in the number of messages indicates that the device is receiving data bearer establishment messages from a BTS.
Tx SRB Messages	Number of SRB request messages that are sent by the device. An increase in the number of messages indicates that the device is transmitting data bearer establishment messages to a BTS.
Reset RACH Counts	An option to reset the Tx RACH count from the System > Interfaces page of the C100 UI.

3. Click **Save** to apply the settings.

Session

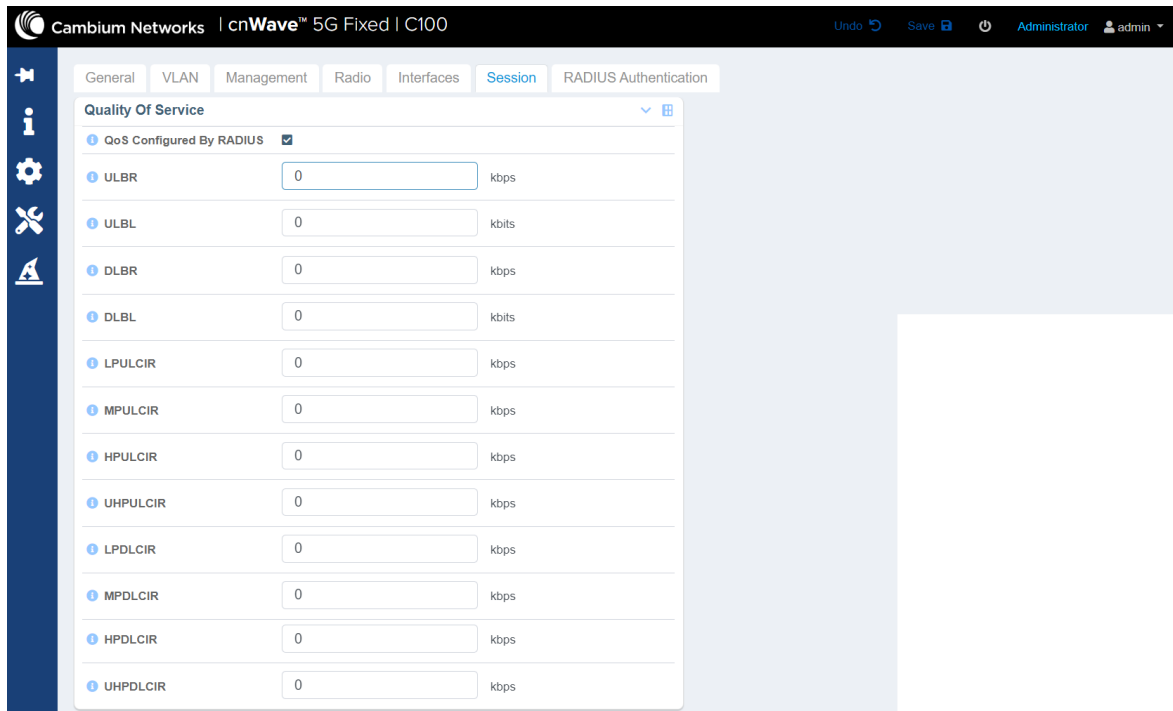
The **Session** page allows you to enable the Watchdog to monitor the registration sessions of the CPE.

To view the session settings, perform the following steps:

1. From the main C100 dashboard page, navigate to **System > Session**.

The **Session** page appears, as shown in [Figure 59](#).

Figure 59: The Session page - C100 UI



2. View the session related settings, as described in Table 38.

Table 38: List of parameters in the Session page

Parameter	Description
Quality of Service	
QoS Configured by RADIUS	<p>Determines whether the QoS configuration is set through RADIUS AAA.</p> <p>The check box is selected if the QoS configuration is set through RADIUS AAA.</p> <p>Note: At the time of boot, the QoS configuration uses the locally configured settings, which may be overridden by the RADIUS-specific settings during registration.</p>
Note: A change to following settings is applicable only when this device next registers with the BTS. These settings are overridden during the RADIUSAAA registration.	
ULBR	<p>The uplink bit rate or sustained uplink rate (in kbps) at which each CPE has registered with the BTS. This BTS is replenished with credits for transmission.</p> <p>Enter an appropriate value in the text box.</p>
ULBL	The uplink bit limit or uplink burst allocation (in kbits).

Parameter	Description
	<p>The maximum amount of data that each CPE is allowed to transmit before being recharged at the sustained uplink data rate (in kbps).</p> <p>Enter an appropriate value in the text box.</p>
DLBR	<p>The downlink bit rate or sustained downlink rate (in kbps) at which the BTS is replenished with credits (tokens) for transmission to each of the CPEs in its sector.</p>
DLBL	<p>Indicates the downlink bit limit or downlink burst allocation (in kbits).</p> <p>The maximum amount of data that the BTS is allowed to transmit to any registered CPE before it is replenished with the transmission credits at the sustained downlink data rate (in kbps).</p> <p>Enter an appropriate value in the text box.</p>
LPULCIR	<p>The minimum rate (in kbps) at which a low priority traffic is sent over the uplink (unless Committed information rate (CIR) is oversubscribed or the RF link quality is degraded).</p> <p>Enter an appropriate value in the text box.</p>
MPULCIR	<p>The minimum rate (in kbps) at which a medium priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).</p> <p>Enter an appropriate value in the text box.</p>
HPULCIR	<p>The minimum rate (in kbps) at which a high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).</p> <p>Enter an appropriate value in the text box.</p>
UHPULCIR	<p>The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).</p> <p>Enter an appropriate value in the text box.</p>
LPDLCIR	<p>The minimum rate (in kbps) at which a low priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).</p>
MPDLCIR	<p>The minimum rate (in kbps) at which a medium priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).</p>
HPDLCIR	<p>The minimum rate (in kbps) at which a high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).</p>
UHPDLCIR	<p>The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).</p>

- Click **Save** to apply the settings.

RADIUS Authentication

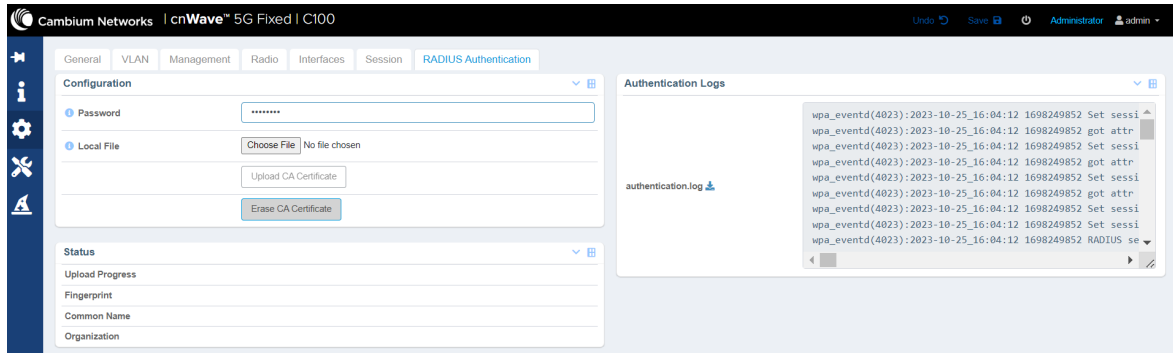
The **RADIUS Authentication** page allows you to configure the RADIUS server specific certificate authority (CA) certificate (for security purpose) required for the RADIUS authentication.

To configure the RADIUS server certificates, perform the following steps:

1. From the main C100 dashboard page, navigate to **System > RADIUS Authentication**.

The **RADIUS Authentication** page appears, as shown in [Figure 60](#).


Figure 60: The RADIUS Authentication page - C100 UI



2. Set the parameters, as described in [Table 39](#).

Table 39: List of RADIUS Authentication-related parameters

Parameter	Description
Configuration	
Password	The RADIUS password used for the authentication.
Local File	An option to select an appropriate CA certificate file that you want to use for RADIUS authentication. To select the local CA certificate, perform the following steps: <ol style="list-style-type: none"> Click Choose File in the Local File field. A file browser window appears. Browse the location where you have saved the CA certificate on your system locally. Select the certificate file and click Open. The local file is selected. To upload the selected local file, click Upload CA Certificate in the RADIUS Authentication page.
Upload CA Certificate	An option to upload the selected CA certificate from your system.
Erase CA Certificate	An option to delete the selected CA certificate from the RADIUS Authentication page.

Parameter	Description
Status	
Upload Progress	Indicates the upload status of the CA certificate.
Fingerprint	Indicates the unique identifier of the certificate.
Common Name	Indicates the domain name of the RADIUS server that you want to secure with the certificate.
Organization	Name of the trusted CA organization. The CA organization validates identities and bind them to cryptographic key pairs with digital certificates.
Authentication Logs	
authentication.log	An option to view and download the authentication logs from the C100 UI. Click the  icon to download the authentication logs.

3. Click **Save** to apply the settings.

Configuring tools

The **Tools** page in the C100 UI allows you to upload new firmware and reboot the unit. The **Tools** page helps to troubleshoot the radio links.

You must use the **Tools** icon () to configure, view, and manage the device for CPEs.

The **Tools** page contains the following tabs:

- [Firmware](#)
- [Configuration](#)
- [Network Test](#)
- [Engineering](#)

Firmware

The **Firmware** page allows you to upgrade or downgrade software firmware. This page also provides the device summary, upload details, and upgrade status of a firmware image.



Note

Before upgrading or downgrading firmware, consider the requirements and compatibility matrix specific to cnWave™ 5G Fixed products (BTS or CPE), as described in:

- [Requirements for firmware version upgrade or downgrade](#)
- [Compatibility matrix](#)

Upgrade or downgrade firmware

You can upgrade or downgrade firmware (CPE) using the **Tools** page of C100 UI.



Note

Before upgrading or downgrading firmware, consider the following key points:

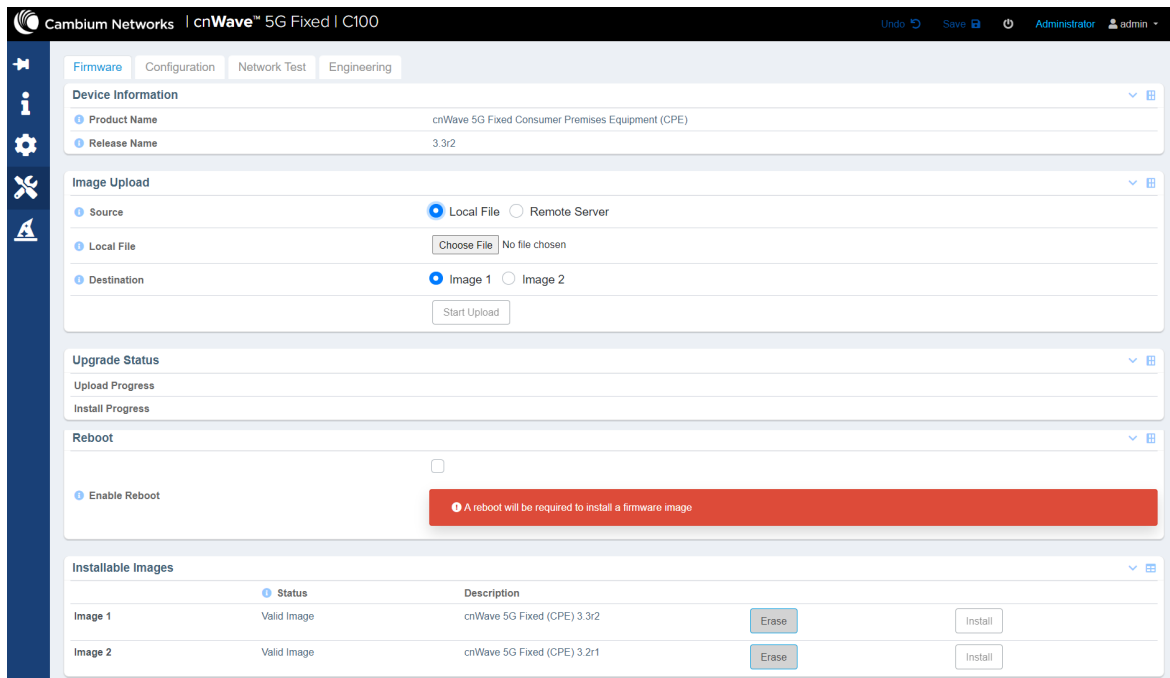
- To **upgrade** a sector with the BTS and all CPEs running with an official software release X, perform the following steps using the **Tools** page:
 - a. Upgrade the BTS first to the next official software release version Y.
 - b. Upgrade all CPEs to the next official software release version Y.
- To **downgrade** a sector with the BTS and all CPEs running with an official software release X, perform the following steps using the **Tools** page:
 - a. Downgrade all CPEs first to the previous BTS software version W.
 - b. Upgrade the BTS to the previous official software release version W.

Using the **Tools** page, perform the following steps to upgrade or downgrade a firmware:

1. From the main C100 dashboard page, navigate to **Tools > Firmware**.

The **Tools** page appears with multiple tabs, as shown in [Figure 61](#). By default, the **Firmware** tab is selected.

Figure 61: *The Tools page - C100 UI*



2. Set the required parameters, as described in [Table 40](#).

Table 40: List of parameters in the Firmware page

Parameter	Description
Device Information	
Product Name	Name of the device that you have deployed.

Parameter	Description
	Example: cnWave 5G Fixed Customer Premise Equipment (CPE)
Release Name	Release number of the operational software.
Image Upload	
Source	<p>An option to select the firmware image file from a location (stored).</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> Local File: Indicates the image file that you have stored locally on your machine. Remote Server: Indicates the image file that you have stored on a remote server (for example, SharePoint). <p>Select the required option.</p>
Local File	<p>This parameter is applicable only if you have selected Local File as the upload source.</p> <p>This parameter supports options to upload or upgrade the required firmware image file. For more details on how to upload the image file, refer to the Uploading or upgrading a firmware image file section.</p>
Server URL	<p>This parameter is applicable only if you have selected Remote Server as the upload source.</p> <p>To upload the image file from a remote server, provide the server URL in the text box. Then, click Start Upload on the Firmware page.</p>
Destination	<p>An option to select the destination image in the firmware images table.</p> <p>Select the required option.</p>
Start Upload	<p>An option to upload the firmware image file.</p> <p>On selecting the required image file (from a local file folder or a remote server), click Start Upload to begin the uploading process.</p>
Upgrade Status	
Upload Progress	Indicates the upgrade status of the firmware.
Install Progress	Indicates the installation status of the firmware, if any.
Reboot	
Enable Reboot	<p>Determines whether to reboot the device on upgrading or installing the firmware.</p> <p>Select the check box to enable the device to reboot.</p> <p>When you select the check box, a message appears indicating that the device will reboot to install a firmware image.</p>
Installable Images	<p>List of images that are recently uploaded, with details of the latest uploaded image at the top row.</p> <p>You can upload multiple image files and manage them in this section.</p>

Parameter	Description
	<p>This parameter displays the following details for the uploaded images:</p> <ul style="list-style-type: none"> • Status: Displays one of the following supported statuses of the image: <ul style="list-style-type: none"> ◦ Empty: Indicates that the firmware image file is not present. ◦ Invalid Image: Indicates that the firmware image file is not valid. The file might be truncated, damaged, or not an appropriate image of the device (wrong product or old). ◦ Valid Image: Indicates that the firmware image file is valid and may be installed. • Description: A brief description of the firmware image file such as device name, version, build number, and time of uploading. <p>To install an image file that you uploaded, click Install in the corresponding row of the required image file.</p> <p>To delete an image file that you uploaded, click Erase in the corresponding row of the required image file.</p>

3. Click **Save** to apply the changes.

Configuration

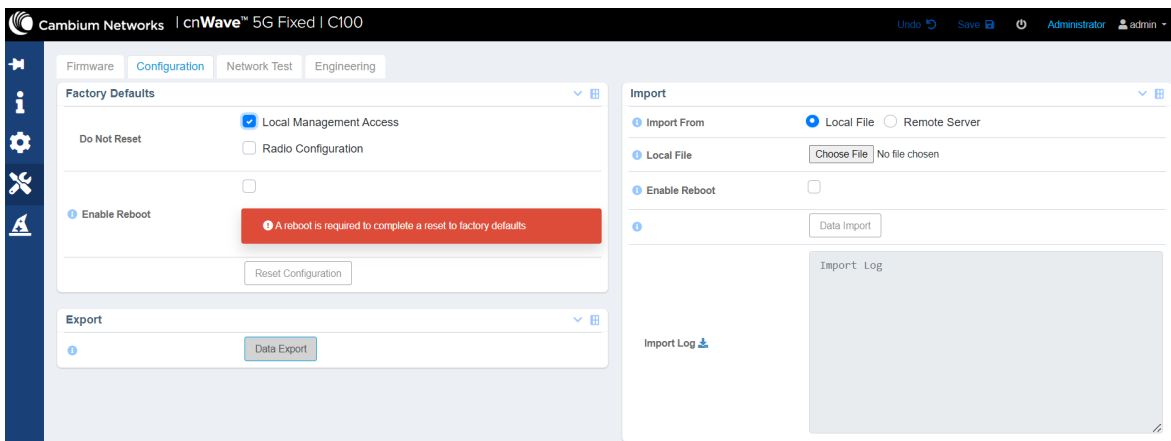
The **Configuration** page allows you to set the CPE to factory defaults. This page also allows you to import a saved configuration or export a CPE configuration for backup (restore). This Import feature exports or imports the data model configuration (and/or status) as a JSON file.

To view and manage the configuration tool-specific settings, perform the following steps:

1. From the main C100 dashboard page, navigate to **Tools > Configuration**.


The **Configuration** page appears, as shown in [Figure 62](#).


Figure 62: *The Configuration page - C100 UI*



2. Set the values for parameters, as described in [Table 41](#).

Table 41: List of parameters in the Configuration page

Parameter	Description
Factory Defaults	
Do not reset	<p>Determines whether you want to reset the CPE to factory defaults.</p> <p>The following options are supported:</p> <ul style="list-style-type: none"> • Local Management Access • Radio Configuration <p>By default, the Local Management Access check box is selected.</p> <p>If you do not select the Local Management Access check box, then all the configuration data, including IP address, is wiped out and reset to 169.254.1.1.</p> <p>You have a choice of keeping at least local access IP address and wiping out all other data. This means that you can access the CPE on your local network.</p> <p>If you select Radio Configuration, then all the configuration data is wiped out, except for the frequency data and local IP address.</p>
Enable Reboot	<p>Determines whether the device is enabled to reboot to complete the process of reset to factory defaults.</p> <p>Select the check box to enable the reboot for the device.</p>
Reset Configuration	<p>An option to reset the system to factory defaults.</p> <p>Click Reset Configuration if you want to reset the CPE to factory defaults.</p>
Export	
Data Export	<p>An option to export the data model configuration (and/or status) as a JSON file for backup (restore).</p> <p>When you click the Data Export button, the data model configuration is downloaded by the device.</p>
Import	
Import From	<p>An option to select a location (stored) from where you want to import the required data configuration.</p> <p>This parameter supports the following options:</p> <ul style="list-style-type: none"> • Local File: A local import file (which is saved locally on your system) is uploaded by the browser. • Remote Server: An import file that is saved on a remote server is downloaded by the device. <p>Select the required option.</p> <p>Note: When you select Remote Server, the  icon appears indicating to select the Local File option (if required).</p>

Parameter	Description
Local File	<p>To upload a local import file (internally), perform the following steps:</p> <ol style="list-style-type: none"> Click Choose File in the Local File field. A file browser window appears. Browse the location where you have saved the import file (for example, a JSON file) on your machine locally. Select the file and click Open. The local import file is selected. To upload the import file, click Data Import in the Configuration page.
Server URL	<p>This parameter is applicable only if you have selected Remote Server in the Import From field.</p> <p>To select the import file from a remote server, provide the server URL in the text box. Then, click the Data import button.</p>
Enable Reboot	<p>Determines whether the device is enabled to reboot to complete the import configuration process.</p> <p>Select the check box to enable the reboot for the device.</p> <p>Note: Reboot is applicable only to some configuration changes.</p>
Data Import	<p>An option to import the required data model configuration from a JSON file.</p>
Import Log	<p>An option to view and download the import logs from the C100 UI.</p> <p>Click the  icon to download the import logs.</p>

- Click **Save** to apply the changes.

Network Test

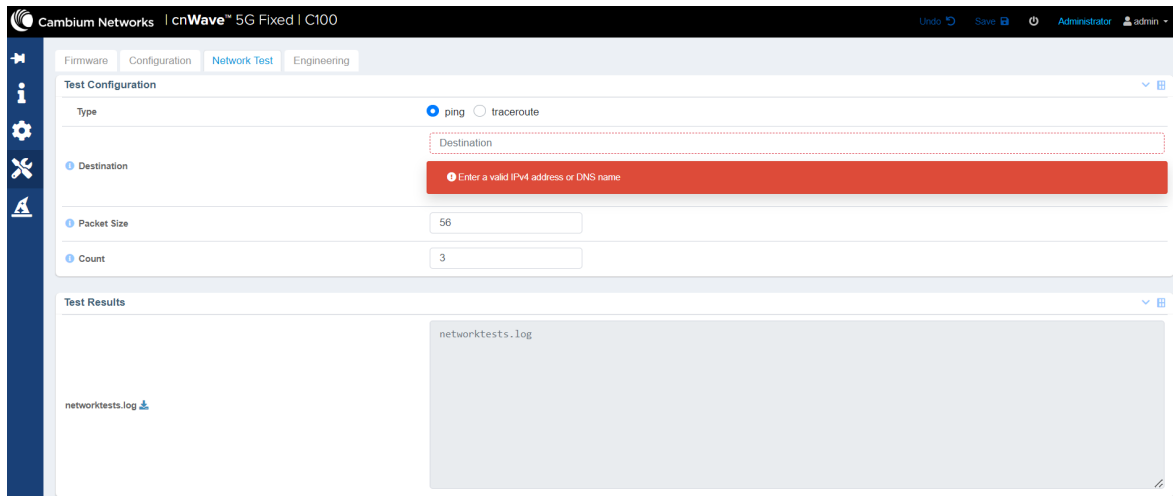
The **Network Test** is a network tool that helps you to test connectivity and accessibility of CPE to a radio network. This page allows you to ensure whether the CPE is correctly connected to your network. Example: CPE's connectivity to BTS or RADIUS Server. This network test helps in troubleshooting network connection issues.

To test and view the network connectivity, perform the following steps:

- From the main C100 dashboard page, navigate to **Tools > Network Test**.

The Network Test page appears, as shown in [Figure 63](#).


Figure 63: The Network Test page - C100 UI



2. View and set the values for parameters, as described in Table 42.

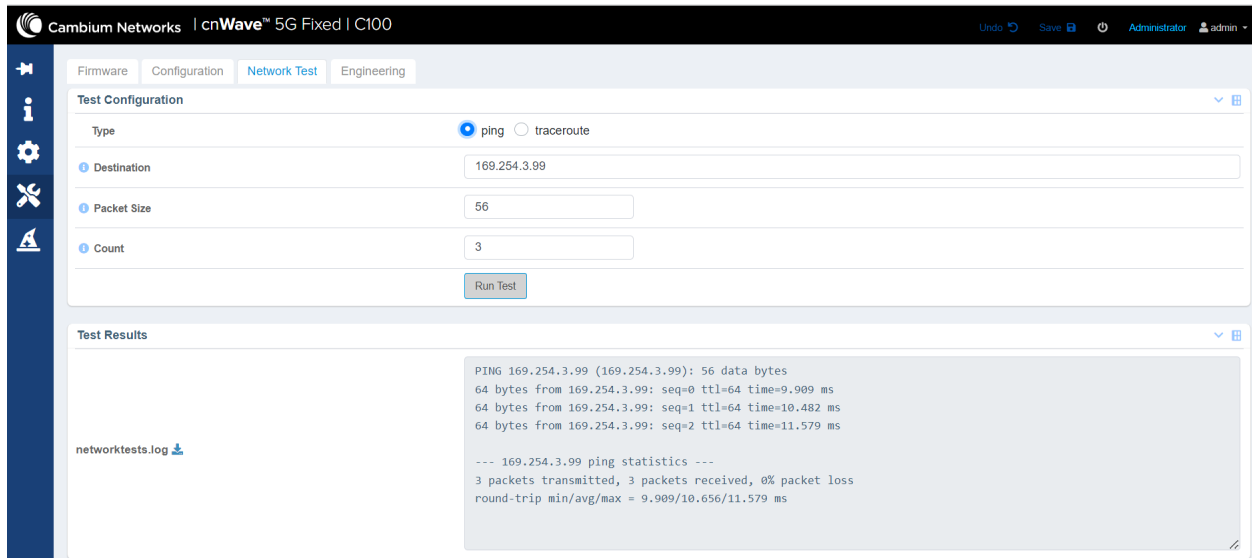
Table 42: Parameters in the Network Test page - C100 UI

Parameter	Description
Test Configuration	
Type	<p>Determines the method used for testing a network.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • ping: The CPE pings the required destination (for example, BTS, cnMaestro, RADIUS Server, DNS, or a radio network) to ensure its connectivity. <p>If the ping is successful, this implies that CPE can access the BTS or the required network.</p> <ul style="list-style-type: none"> • traceroute: CPE traces the source of the required destination (for example, if the BTS is connected to a switch, which is connected to another application such as a host Server) for identifying the number of hops connected to a radio network. <p>If the trace is successful, CPE finds out the IP address of the BTS or the network in 30 hops. If the trace fails in 6 to 7 hops, this implies that the CPE cannot access the BTS or the network.</p> <p>Choose the required test type.</p> <p>and are examples of ping and traceroute types.</p>
Destination	<p>The valid IPv4 address or a DNS name of the required destination.</p> <p>Provide an appropriate value in the text box.</p>
Packet Size	<p>Number of data bytes that has to be sent to the network.</p>

Parameter	Description
	<p>Default value: 56 data bytes, which are translated into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.</p> <p>Provide the required value in the text box.</p> <p>Note: This parameter is not applicable if you select <code>traceroute</code> in the Type field.</p>
Count	<p>Number of ping packets that have to be sent to the network.</p> <p>Default value: 3</p> <p>Provide the required value in the text box.</p> <p>Note: This parameter is not applicable if you select <code>Traceroute</code> in the Type field.</p>
Run Test	<p>An option to run the test.</p> <p>This option appears only when you provide a value in the Destination text box.</p>
Stop Test	<p>An option to stop the test that has begun.</p> <p>This option appears only when you run the test.</p>
Test Results	
networktests.log	<p>Displays the test results for the required destination.</p> <p>By default, this field is disabled. When you run the test, this field displays the test results.</p> <p>You can use the  icon to download the log file.</p>

is an example of a test result for the **ping** type:

Figure 64: Test result - ping



The screenshot shows the 'Network Test' configuration page in the cnWave 5G Fixed | C100 interface. The 'Test Configuration' section is active, showing the following settings:

- Type: ping traceroute
- Destination: 169.254.3.99
- Packet Size: 56
- Count: 3

A 'Run Test' button is visible below the configuration fields. The 'Test Results' section displays the output of the ping test:

```

PING 169.254.3.99 (169.254.3.99): 56 data bytes
64 bytes from 169.254.3.99: seq=0 ttl=64 time=9.909 ms
64 bytes from 169.254.3.99: seq=1 ttl=64 time=10.482 ms
64 bytes from 169.254.3.99: seq=2 ttl=64 time=11.579 ms

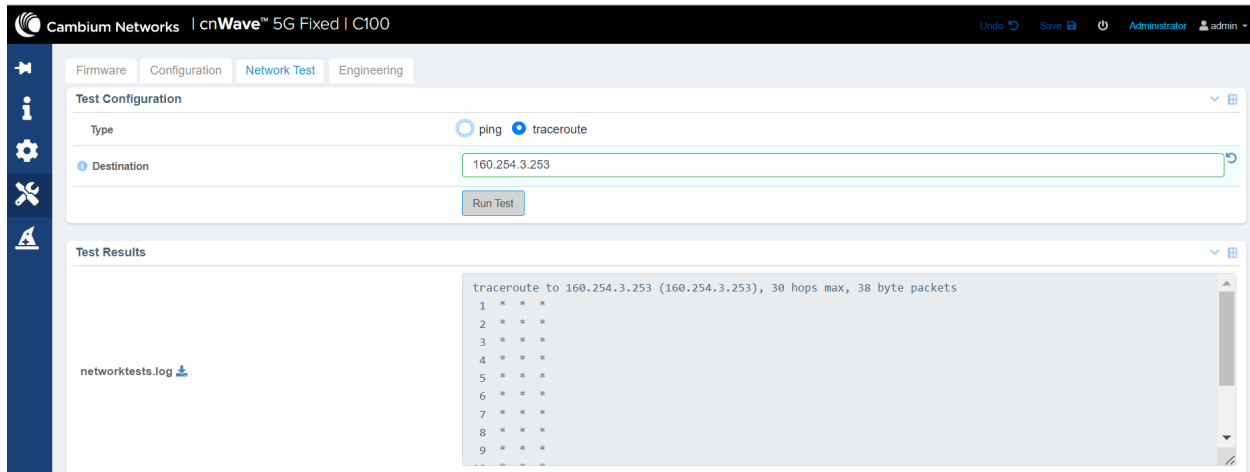
--- 169.254.3.99 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 9.909/10.656/11.579 ms

```

Below the test results, there is a 'networktests.log' label with a download icon.

is an example of a test result for the **traceroute** type:

Figure 65: Test result - traceroute



Engineering

The **Engineering** page allows engineers (of Cambium Networks) to access the CPE radio remotely. Engineers can allow the users to access the radio using Telnet, SSH, and console secured cable (HTTP is not allowed).



Note
The **Engineering** page is configured and applicable only for troubleshooting and support purposes.

To view the **Engineering** page, perform the following steps:

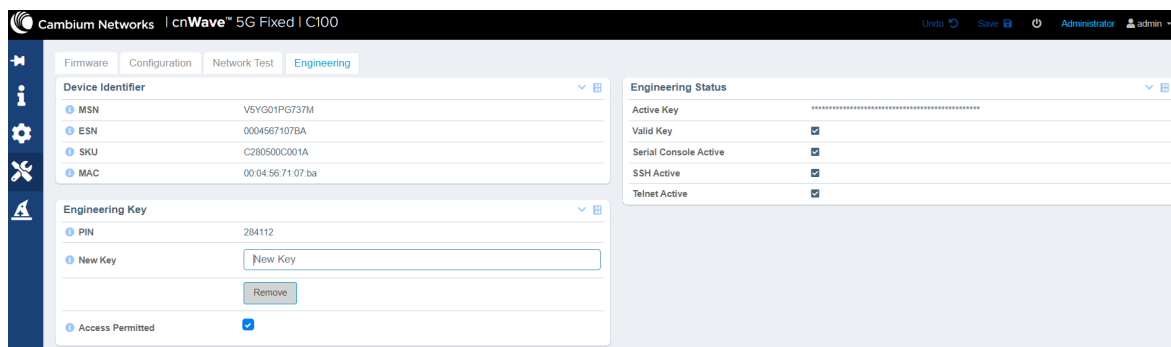
1. From the main C100 dashboard page, navigate to **Tools > Engineering**.

The **Engineering** page appears, as shown in Figure 66..



Note
If the engineers (from Cambium Networks) have not removed any engineering keys from the UI, then the **Engineering Status** section in the **Engineering** page displays all the configured engineering keys as shown in Figure 66.

Figure 66: The Engineering page - C100 UI



- View and set the values for parameters, as described in [Table 43](#).

Table 43: List of parameters in the Engineering page

Parameter	Description
Device Identifier	
MSN	MSN of the device that is used for device identification.
ESN	ESN of the device.
SKU	SKU of the device.
MAC	The MAC address that is assigned to the network interface and used for the device management.
Engineering Key	
PIN	Unique six-digit number used by the Engineering team of Cambium Networks to generate an engineering key for the CPE device. Note: This is a read-only field.
New Key	The new engineering key generated and provided by the Engineering team of Cambium Networks using PIN. This new engineering key allows privileged engineering access to the CPE device. Enter the engineering key in the text box.
Remove	An option to remove the installed key and access the CPE device. If you click Remove , then the installed new key and access (using SSH, Serial Console, and Telnet) are removed.
Access Permitted	Determines whether the new key enables engineering access to the CPE device. Select the check box to enable the engineering access for the new key. Note: By default, the engineering access is enabled when a new key is installed.
Engineering Status - Following are the read-only parameters:	
Active Key	Indicates whether the new generated key is accessible.
Valid Key	Indicates whether the generated key is valid.
Serial Console Active	Indicates whether the serial console is accessible for the users.
SSH Active	Indicates whether SSH is accessible for the users.
Telnet Active	Indicates whether the Telnet is accessible for the users.

Setting up a wizard

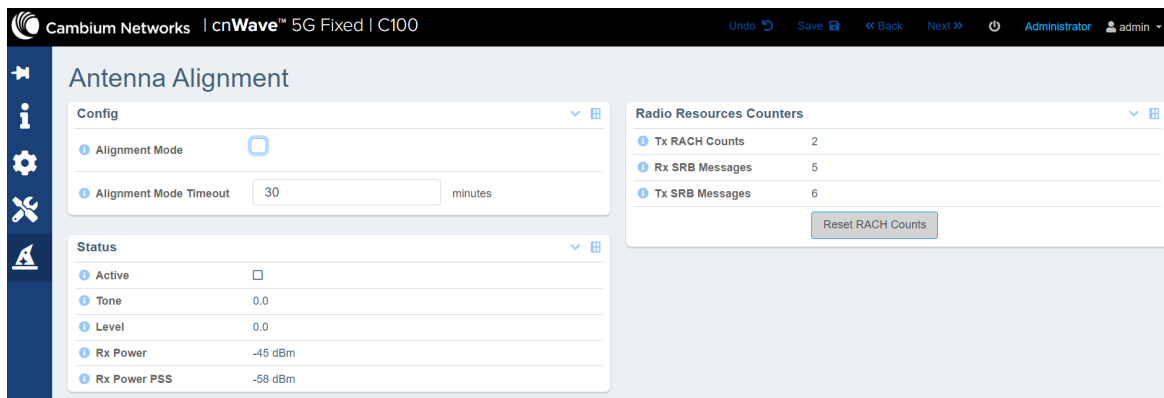
The **Set-up Wizard** page allows you to set the antenna alignment mode and CPE configurations such as frequencies and power.

You can also use the **Set-up Wizard** icon () to configure, view, and manage the setup wizard for CPEs.

To view and configure the **Set-up Wizard** page, perform the following steps:

1. From the left navigation column in the main C100 dashboard page, select the **Set-up Wizard** icon (🔧).
The **Set-up Wizard** page appears, as shown in [Figure 67](#).

[Figure 67](#): The Set-up Wizard page - C100 UI



2. Set and view the details of parameters, as described in [Table 44](#).

Table 44: List of parameters on the Set-up Wizard page

Parameter	Description
Config	
Alignment Mode	Determines whether the alignment mode is enabled to provide audio tones to assist with the CPE installation. After using this parameter in enabled mode, you must explicitly disable this parameter.
Alignment Mode Timeout	Disable the install tone (without the operator intervention) after the link has been up for more than the specified timeout period (in minutes). Type an appropriate value in the text box. You can disable this timeout parameter by setting the timeout period to 0.
Status	
Active	Indicates whether the receive level audio tone indicator is enabled or activated for the antenna alignment.
Tone	Frequency of the audio tone used for the antenna alignment.
Level	Power of the received signal during antenna alignment.
Rx Power	The Receive power (in dBm) of data symbols.
Rx Power PSS	The Receive power (in dBm) of the PSS symbols.
Radio Resource Counters	
Tx RACH Counts	Number of registration requests sent by the device using the Random Access Channel (RACH).

Parameter	Description
	A registration request is the first message that is transmitted when a suitable BTS signal is locked on.
Rx SRB Messages	Number of Signalling Radio Bearer (SRB) response messages that are received by the device. An increase in the number of messages indicates that the device is receiving data bearer establishment messages from a BTS.
Tx SRB Messages	Number of SRB request messages that are transmitted by the device. An increase in the number of messages indicates that the device is transmitting data bearer establishment response messages to the BTS.
Reset RACH Counts	An option to reset the Tx RACH count from the Antenna Alignment page of the C100 UI.

3. Click **Save** to apply the changes.

Appendix 1: cnMaestro X Configuration

cnMaestro X is a network management platform available on cloud and on-premises deployments. If you have installed and configured cnMaestro X for the cnWave™ 5G Fixed platform, you can use the cnMaestro X UI to monitor a cnWave 28 GHz network.



Note

You must use **cnMaestro™ 3.2.0 version or later versions**. Contact your Cambium Networks Sales representative for the details on how to join the cnMaestro™ program.

This topic covers the following sections:

- [Prerequisite tasks](#)
- [Configuring cnMaestro X](#)
- [Managing BTS and CPEs](#)
- [Generating data reports](#)

Prerequisite tasks

Before configuring cnMaestro X (after installation) for the cnWave™ 5G Fixed platform, you must complete the following prerequisite tasks:

1. Create a **Cambium Support Center account**, which sets your username and password, required for accessing the cnMaestro X UI. This action also allows you to register on the Cambium Networks Support site.
2. Use the Cambium Support Center account to log on to cnMaestro X and create a **cnMaestro account**. This action creates a cloud account required for managing devices using the cnMaestro X UI.

During this cnMaestro-specific account creation process, you can set the **Cambium ID** that is required for onboarding the BTS device (using the cnMaestro UI).



Note

A Cambium ID is a string that uniquely identifies an account (which you create). It consists of letters, numbers, and underscores. Example: 28GHz_CNWAVE_PLATFORM_SIT

It is used to onboard devices and is assigned to the devices managed by cnMaestro X. You can locate it on the home page of cnMaestro X UI (on right side of the title bar). When a Cambium ID is set, you cannot modify it. You must contact the Cambium Networks Support team for any changes.

For detailed information about creating the accounts-specific to cnMaestro and logging in to the UI, refer to the latest *cnMaestro User Guide*.

On completing the prerequisite tasks, you must configure cnMaestro and the BTS device using their respective UIs.

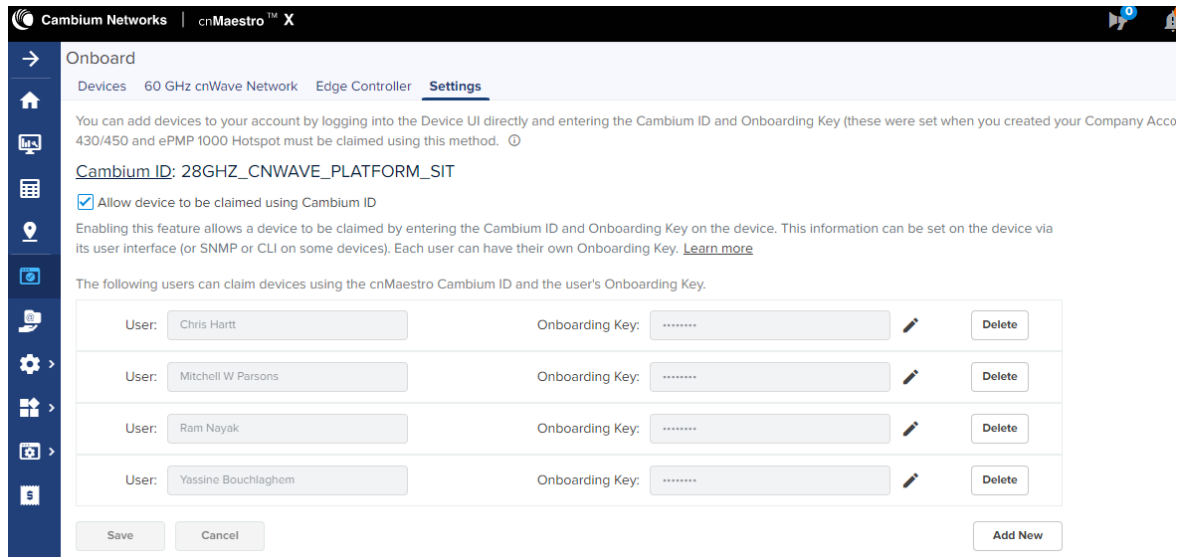
Configuring cnMaestro X

You must configure the cnMaestro X UI to use Cambium ID and onboarding key on the BTS device. To configure cnMaestro X for the BTS device, perform the following steps:

1. Log on to the cnMaestro X UI (cloud or on-premises) using appropriate username and password.
The **cnMaestro X** home page appears.
2. From the home page, navigate to **Onboard > Settings**.

The **Onboard > Settings** page appears, as shown in [Figure 68](#).

Figure 68: The **Settings** page



3. Select the **Allow device to be claimed using Cambium ID** check box.

The **Settings** page allows you to add new users and set onboarding keys (password). In addition, you can edit or delete the required usernames and onboarding keys from the **Settings** page.

To add a new user, perform the following steps:

- a. Click **Add New** on the Settings page.
A new row appears with **User** and **Onboarding Key** text boxes.
- b. Enter the user's name in the **User** text box.
- c. Enter an appropriate value (password) in the **Onboarding Key** text box.
- d. Click **Save**.

The new user credentials are saved in cnMaestro.

4. Log on to the B1000 UI (as described in the [Accessing the B1000 UI](#) section) and perform the following steps:

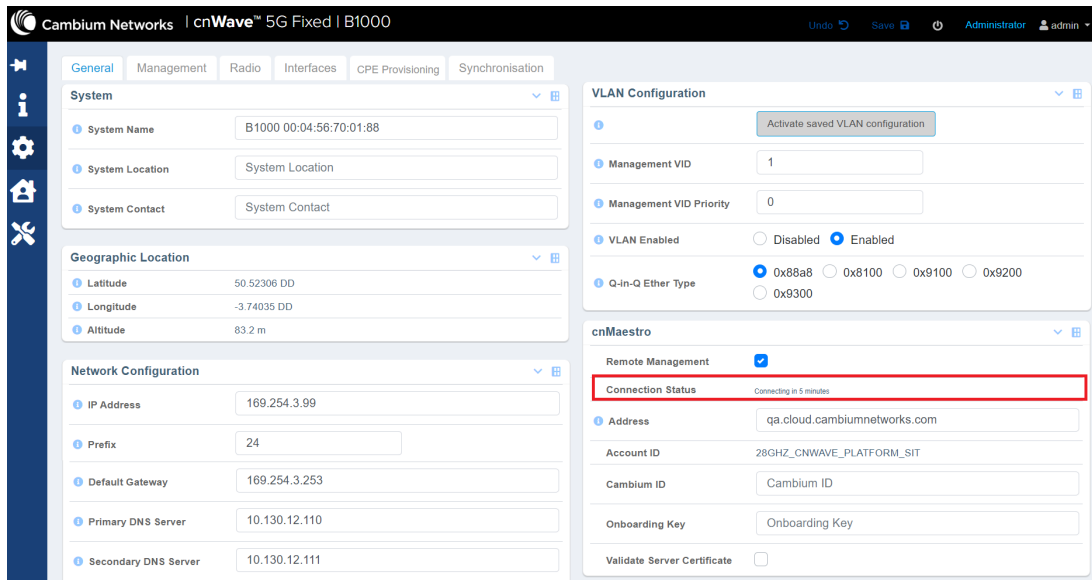
- a. From the main B1000 dashboard page, navigate to **System > General**.

The **General** page appears, as shown in [Figure 10](#).

- b. In the **cnMaestro** section, Select the **Remote Management** check box.

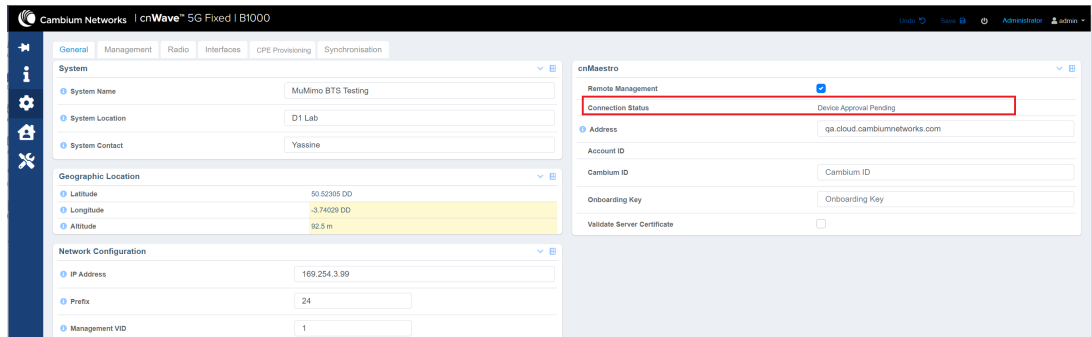
If everything works correctly at the background, the **cnMaestro** section displays the connection status (Connecting in 5 minutes) of the BTS system and cnMaestro-specific parameters (as shown in [Figure 69](#)).

Figure 69: The Connecting status of the BTS device



You must wait for some time until the **Connection Status** parameter displays the **Device Approval Pending** status for the BTS device (as shown in Figure 70).

Figure 70: The Device Approval Pending status

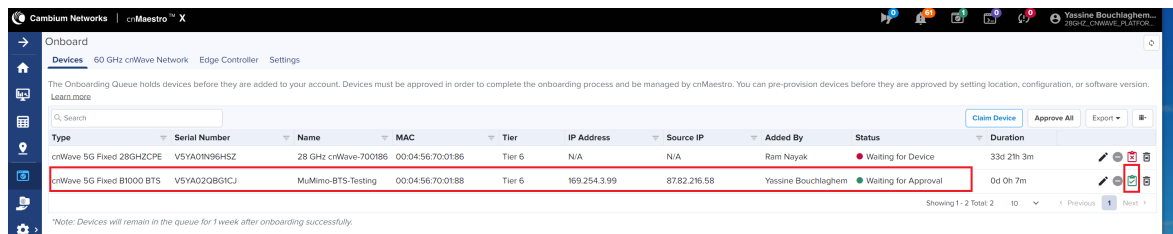



The BTS device needs approval for onboarding.

5. Go to the cnMaestro X UI and navigate to **Onboard > Devices**.

The **Devices** page appears, indicating the waiting for approval status for the BTS device (for example, as shown in Figure 71).

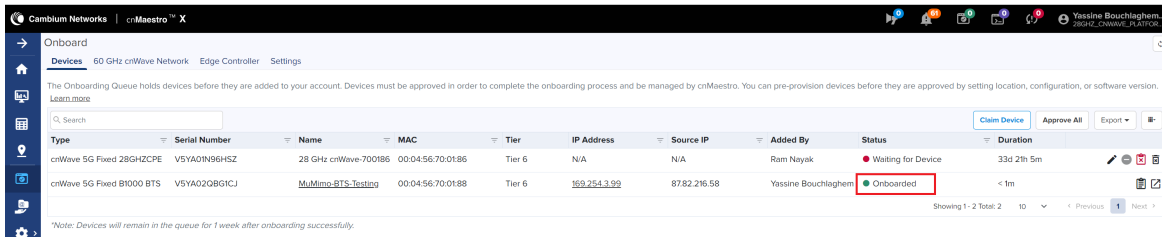
Figure 71: The Waiting for approval status of the BTS device



- Select the tick box () on the required corresponding row, as shown in [Figure 71](#).

When you select this corresponding tick box to approve, the BTS device is onboarded. The **Devices** page indicates the **Onboarded** status, as shown in [Figure 72](#).

Figure 72: *The Onboarded status of the BTS device*



- Go back to the **System > General** page of the B1000 UI and perform the following steps:

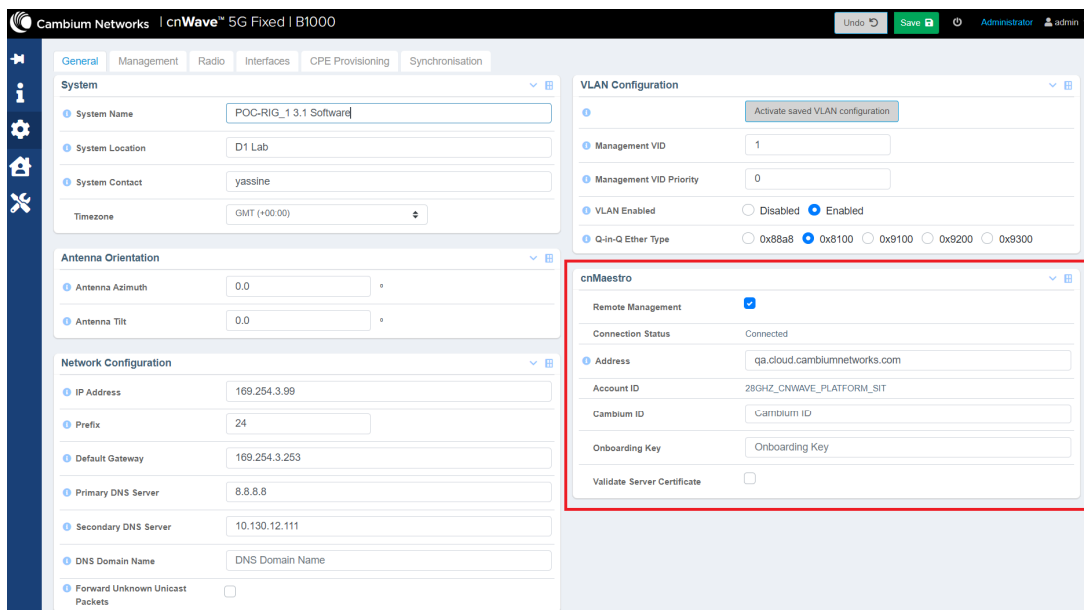
- In the **cnMaestro** section, enter the Cambium ID and the onboarding key that you set on the **Settings** page of cnMaestro UI.

For more information about cnMaestro-specific parameters in the B1000 UI, refer to [Table 8](#).


- Click **Save**.

The **Connection Status** parameter in the **cnMaestro** section displays **Connected**, as shown in [Figure 73](#).

Figure 73: *The connected status of the BTS device*

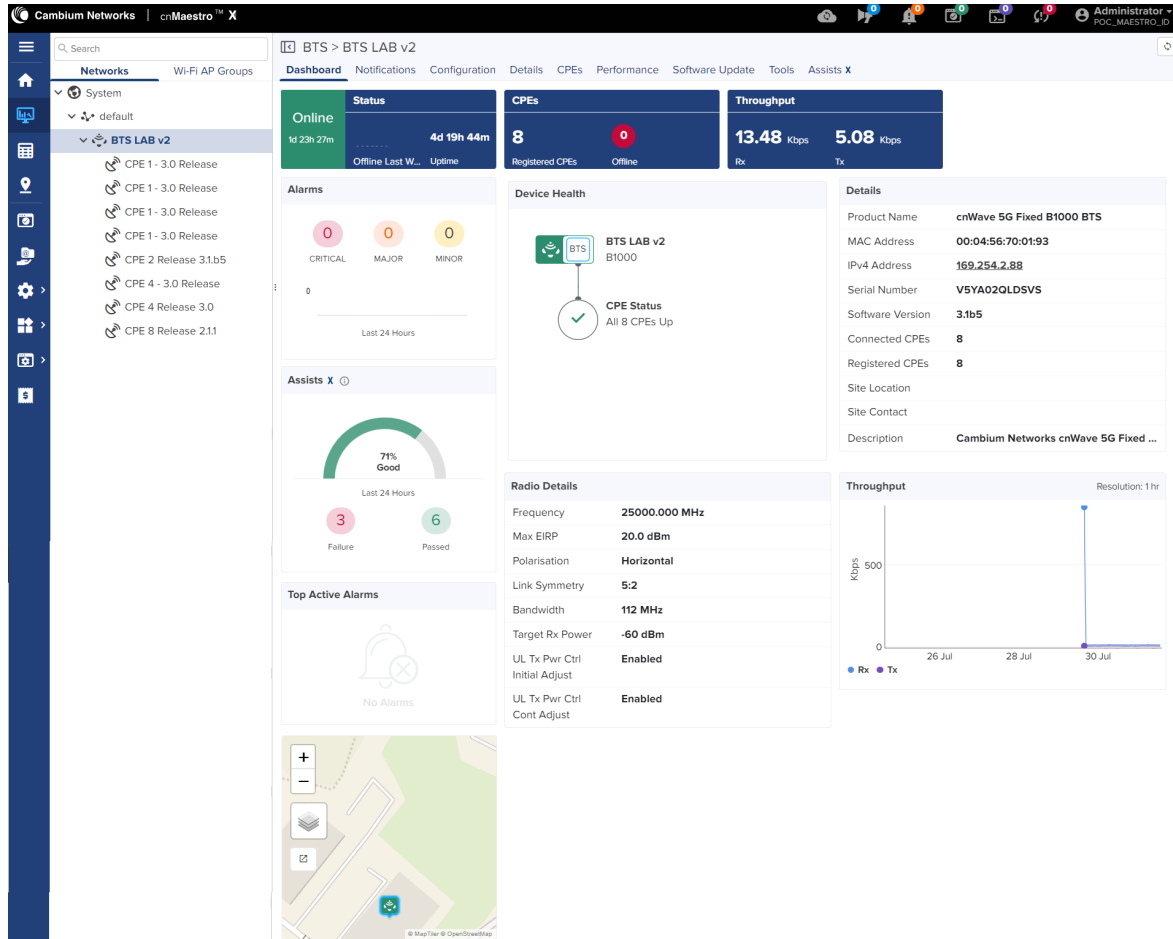


The BTS device has connected to cnMaestro, successfully.

- On the left navigation pane of cnMaestro home page, select the **Monitor and Manage** () icon and expand the options under the **Networks** section.

The BTS dashboard appears on the cnMaestro X UI (as shown in [Figure 74](#)), which you can use to monitor the performance of the BTS and the required CPEs. In addition, you can view information about each CPE on this dashboard.

Figure 74: The BTS monitoring dashboard on the cnMaestro X UI



For detailed information about UI controls in the cnMaestro X UI, refer to the latest *cnMaestro User Guide*.

Managing BTS and CPEs

When you select the required network for BTS using the **Monitor and Manage** () icon on the cnMaestro X UI, the following UI modules are available:

- [Dashboard](#)
- [Notifications](#)
- [Configuration](#)
- [Details](#)
- [CPEs](#)
- [Performance](#)

- [Software Upgrade](#)
- [Tools](#)
- [Assists X](#)

Using these UI modules, you can monitor and manage BTS and CPE devices.

Dashboard

The **Dashboard** page displays summary of the BTS or CPE status (online or offline, uptime), count of registered CPEs and their status, throughput, and the radio details. The **Dashboard** page contains multiple widgets, as shown in [Figure 74](#).

[Table 45](#) 1 lists and describes the widgets available on the **Dashboard** page for the BTS and a CPE.

Table 45: List of widgets on the Dashboard page

Widget	Description
Alarms	Indicates the count of critical, major, and minor alarms observed in the last 24 hours for the BTS or a CPE.
Device Health	Specifies the status of BTS and connected CPEs.
Details	Displays the device details such as product name, MAC and IPv4 address, software version, count of connected and registered CPEs, site location and contact, and a brief description of the device.
Assists X	Indicates the percentage of excellent, good, and poor CPE connections observed in the last 24 hours. This widget also provides the count of failed and passed CPE connections with the BTS.
Radio Details	Provides details of the BTS such as frequency, Max EIRP, polarisation, link symmetry, bandwidth, Target Rx Power, UL Tx Pwr Ctrl Initial Adjust, and UL Tx Pwr Ctrl Cont Adjust. For a CPE, this widget displays radio details such as DL and UL EVM, current EIRP, range, DL Rx power, DL an UL MCS, and alignment active status.
Throughput	Indicates the Rx and Tx throughput of the BTS or a CPE for a period in a graph format.
Top Active Alarms	Displays name of the device (BTS or CPE), device status, and the last up time.
Map	Displays the location of the BTS or a CPE device. Use the zoom in and zoom out options to view the heatmap.
Session	Applicable only to the CPE dashboard. Indicates the registration state, registration time, and link uptime for a CPE.

Notifications

The **Notifications** page provides detailed information of alarms raised for the BTS or the CPE device. This page contains the following tabs:

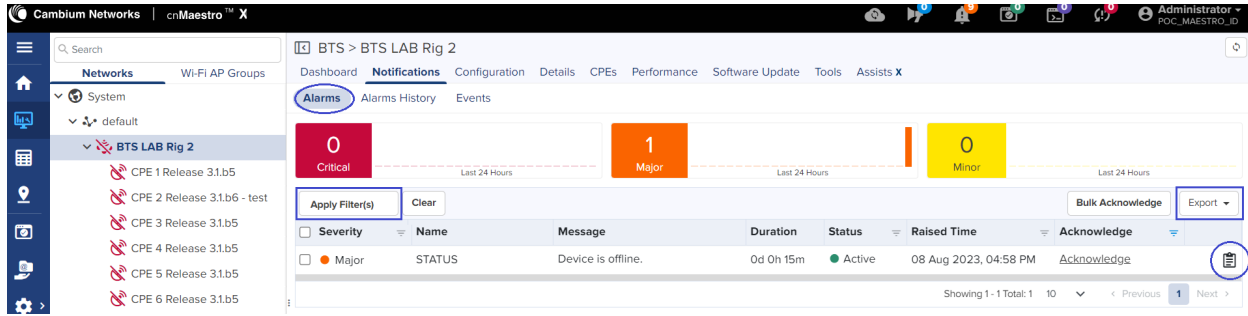
- [Alarms](#)
- [Alarm History](#)

- [Events](#)

Alarms

The **Alarms** page displays the count of critical, major, and minor alarms in different colors (as shown in [Figure 75](#)). This page also provides information of alarms in a table format, indicating severity level, alarm name, message (a brief description), duration, alarm status, raised time, and the acknowledged status of alarm.

Figure 75: *The Notifications > Alarms page*



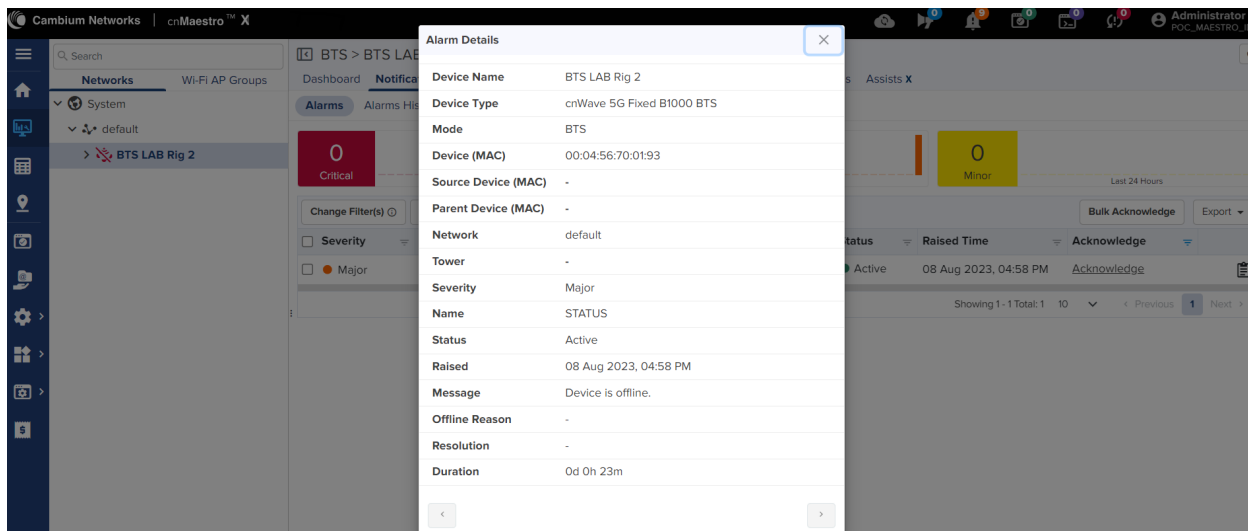
Using the **Apply Filter(s)** button, you can set and apply the following filters for viewing the alarm data in a table:

- Severity (Minor, Major, Critical)
- Status (Active, Inactive)
- Raised Time (Between, Before, After)
- Acknowledge (Acknowledged, Unacknowledged)

Use the **Bulk Acknowledge** button only when you want to acknowledge the alarms in bulk. To export the alarm data (in CSV or PDF format), use the **Export** button (as shown in [Figure 75](#)).

When you click on the **View Details** icon (📄), the **Alarm Details** page appears (as shown in [Figure 76](#)). You can use this page to view the detailed information of an alarm.

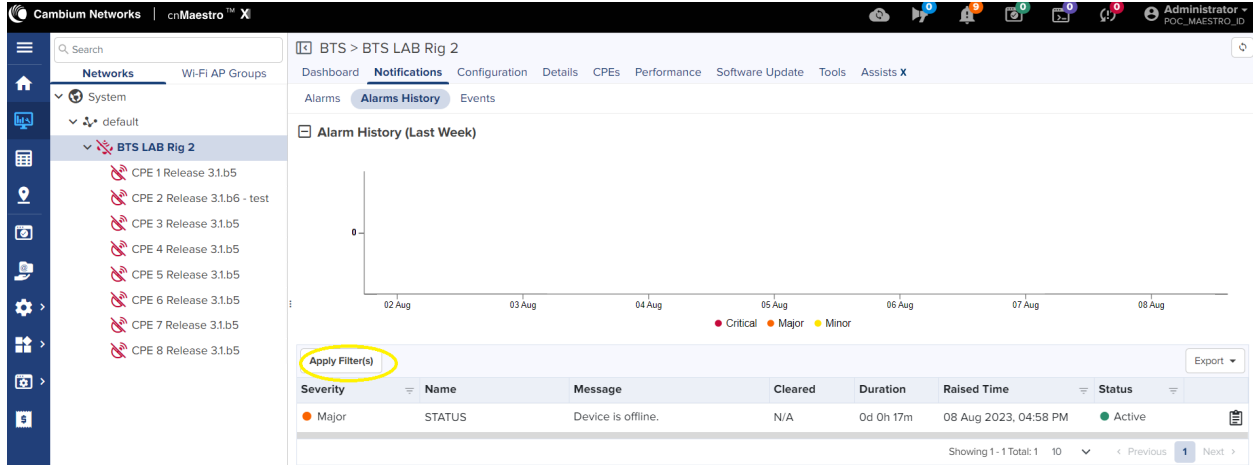
Figure 76: *The Alarm Details page*



Alarm History

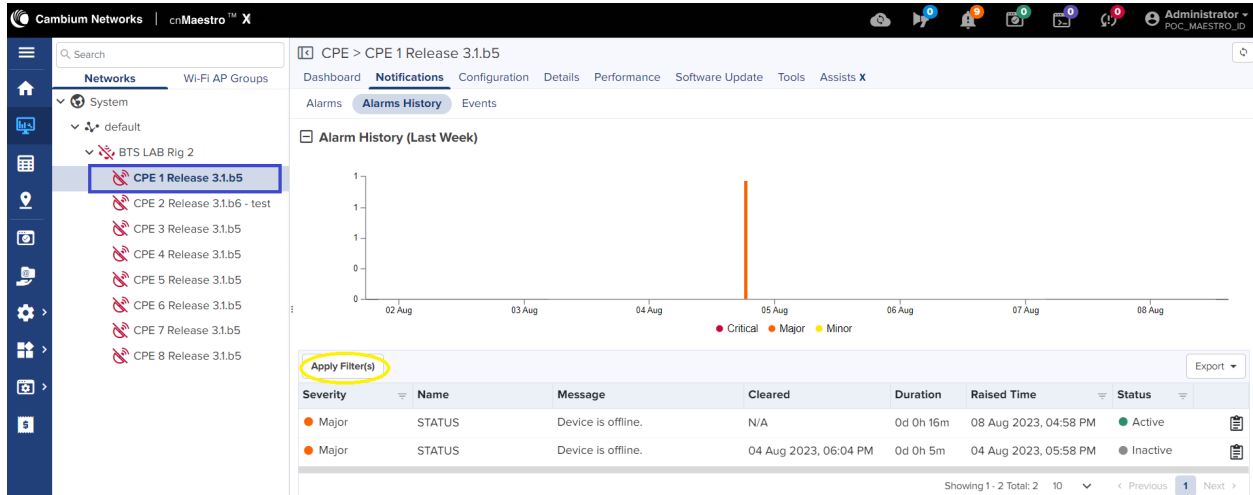
The Alarm History page displays the alarm data for the previous week in graph and table format (as shown in Figure 77).

Figure 77: The Notifications > Alarms History page



When you select a CPE, the Alarms History page displays data as shown in Figure 78.

Figure 78: The alarm history for a CPE (offline)

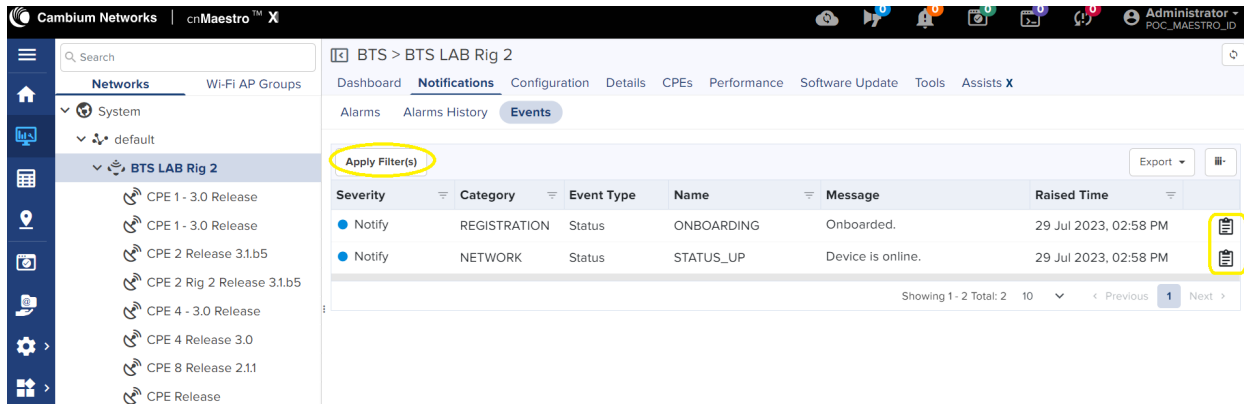


Using the **Apply Filter(s)** button, you can set and apply filters for viewing the alarm data in a table.

Events

The **Events** page displays detailed information of alarms in a table format, as shown in Figure 79.

Figure 79: The Notifications > Events page



Using the **Apply Filter(s)** button, you can set and apply the following filters for viewing the event data in a table:

- Severity (Notify, Minor, Major, Critical)
- Category (Infrastructure, Network, Operations, Others)
- Name (for example, Onboarding, Status_Up)
- Raised Time (Between, Before, After)

When you click on the **View Details** icon () , the **Event Details** page appears. You can use this page to view the detailed information of an event.

Configuration

The **Configuration** page allows you to configure the device settings, as shown in [Figure 80](#).

Figure 80: The Configuration page

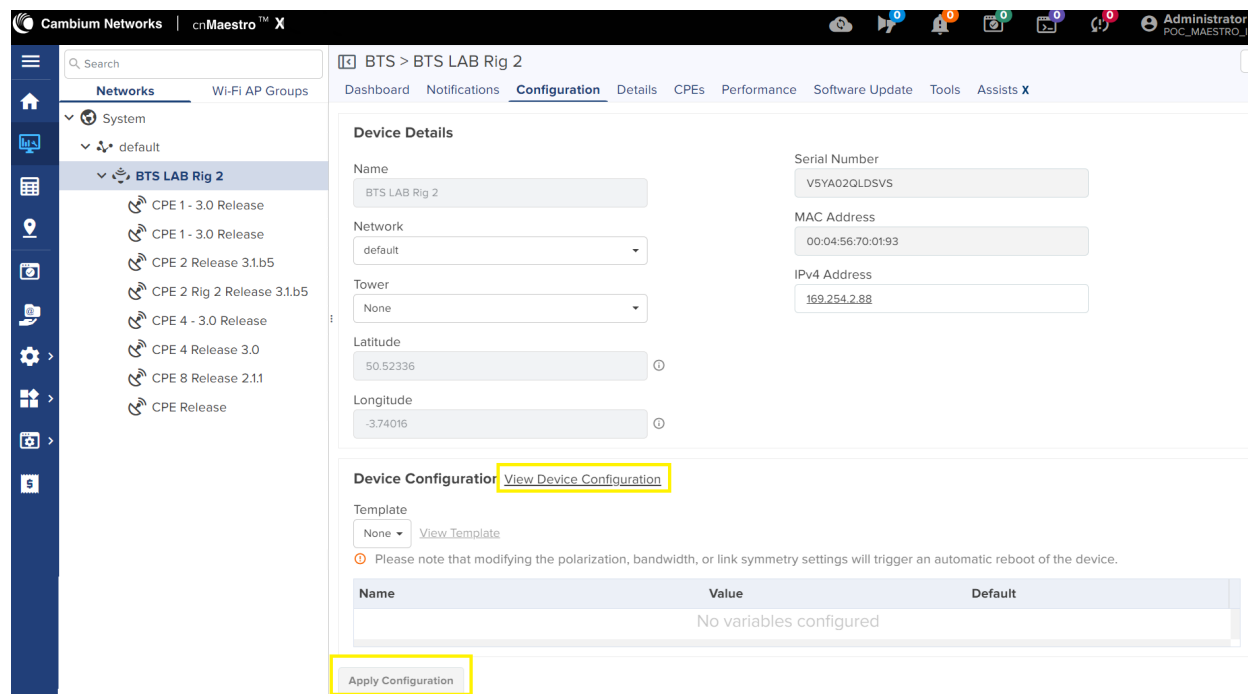


Table 46 lists and describes the parameters available on the Configuration page.

Table 46: Parameters on the Configuration page

Parameter	Description
Device Details	
Name	Name of the BTS device. This is a read-only parameter.
Network	Name of the network where the BTS device is available. Select the appropriate network name from the drop-down list. Note: This parameter is disabled for the CPE specific settings.
Tower	Name of the antenna tower where the BTS device is located. Select the appropriate tower name from the drop-down list. Note: This parameter is disabled for the CPE specific settings.
Latitude	The geographic latitude of the BTS device in decimal degrees (DD). This is a read-only parameter.
Longitude	The geographic longitude of the BTS device in DD. This is a read-only parameter.
Serial Number	The serial number of the BTS device. This is a read-only parameter.

Parameter	Description
MAC Address	The Ethernet Media Access Control (MAC) address that is assigned to the network interface and used for the device management. This is a read-only parameter.
IPv4 Address	The IPv4 address that is set for the BTS or the CPE device. Enter an appropriate value in the text box.
Device Configuration - Allows you to view the existing device configuration and the template. If you modify any parameters in the template (such as polarisation, bandwidth, or link symmetry), the device automatically reboots.	
Apply Configuration	An option to submit or apply the new configuration changes.

Details

The **Details** page provides an overview, interface, and the radio details of the BTS or CPE device. This page contains the following tabs:

- [Overview](#)
- [Interface](#)
- [Radio](#)

Overview

The **Overview** page provides details of the device, boot loader, boot reason and count, and shutdown time. (as shown in Figure 81).

Figure 81: The Details > Overview page for the BTS

The screenshot shows the 'Overview' page for a device named 'BTS LAB v2'. The interface includes a navigation sidebar on the left and a main content area with several sections:

- Details:**
 - Product Name: cnWave 5G Fixed B1000 BTS
 - MAC Address: 00:04:56:70:01:93
 - IPv4 Address: 169.254.2.88
 - Serial Number: V5YA02QLDSVS
 - Software Version: 3.1b5
 - Connected CPEs: 8
 - Registered CPEs: 8
 - Site Location: (empty)
 - Site Contact: (empty)
 - Description: Cambium Networks cnWave 5G Fixed Base ...
- Boot Loader:**
 - Git Tag: develop/4/38
 - Build Name: BOOTLOADER 38/2023-06-22 (W) 07:02:34...
 - Hardware Version: Digits P9.0 RF 6.0
- Boot:**
 - Startup Reason: Non-Power Cycle
 - Startup Count: 261
- Shutdown:**

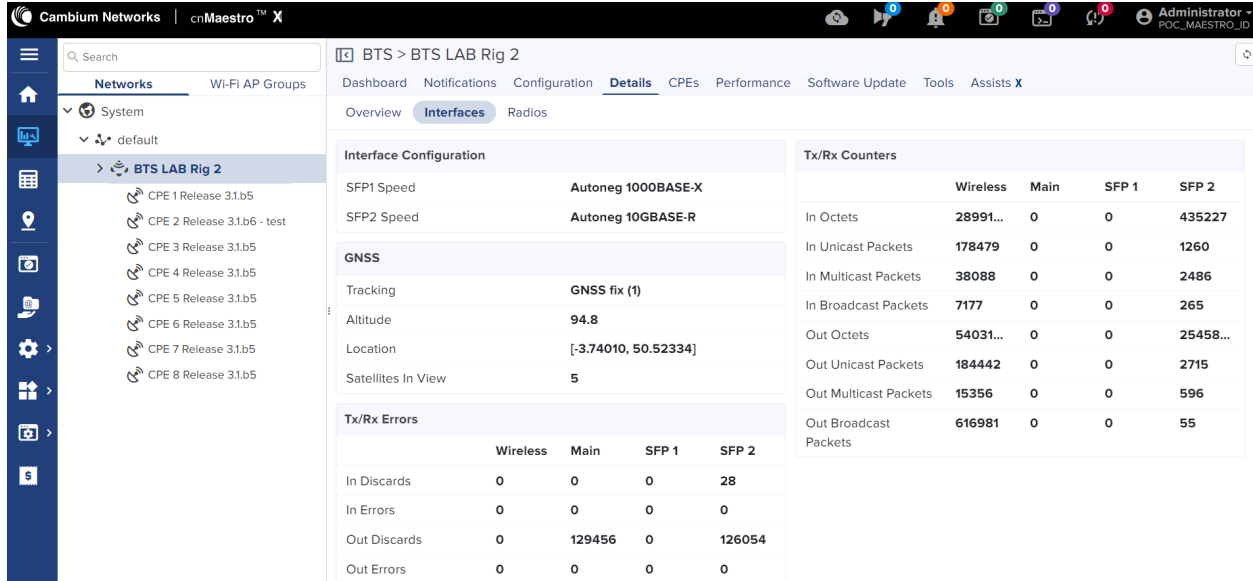
Date & Time	Reason	Detail
2023-07-26 12:09:42.00	Firmware Upgrade	cnmaestro-bts-upgrade
0000-00-00 00:00:00.00	Power Loss	Boot after long power cy...
0000-00-00 00:00:00.00	Power Loss	Boot after long power cy...
0000-00-00 00:00:00.00	Power Loss	Boot after long power cy...
0000-00-00 00:00:00.00	Power Loss	Boot after long power cy...
0000-00-00 00:00:00.00	Power Loss	Boot after long power cy...
2023-07-12 08:31:50.00	Firmware Upgrade	cnmaestro-bts-upgrade
2023-07-03 15:07:19.00	Firmware Upgrade	3.0 to 3.1b4

For each CPE, the **Overview** page displays device, radio, and session details. For information on parameters available of the **Overview** page, refer to [Table 5](#) in the [Device](#) section.

Interface

The Interface page displays the radio interface configuration details of the BTS or the CPE device (as shown in Figure 82).

Figure 82: The Details > Interface page for the BTS



The screenshot shows the 'Interface' page for 'BTS LAB Rig 2'. The page is divided into several sections:

- Interface Configuration:**
 - SFP1 Speed: Autoneg 1000BASE-X
 - SFP2 Speed: Autoneg 10GBASE-R
- GNSS:**
 - Tracking: GNSS fix (1)
 - Altitude: 94.8
 - Location: [-3.74010, 50.52334]
 - Satellites In View: 5
- Tx/Rx Counters:**

	Wireless	Main	SFP 1	SFP 2
In Octets	28991...	0	0	435227
In Unicast Packets	178479	0	0	1260
In Multicast Packets	38088	0	0	2486
In Broadcast Packets	7177	0	0	265
Out Octets	54031...	0	0	25458...
Out Unicast Packets	184442	0	0	2715
Out Multicast Packets	15356	0	0	596
Out Broadcast Packets	616981	0	0	55
- Tx/Rx Errors:**

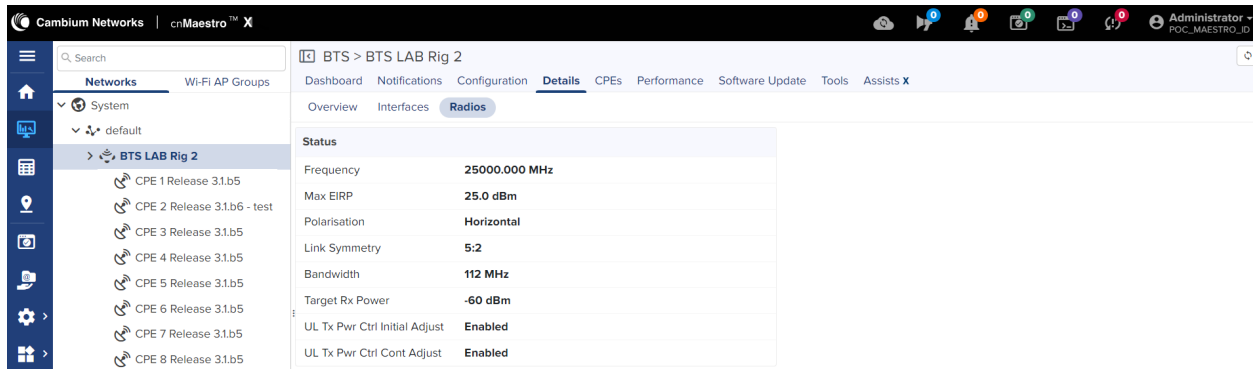
	Wireless	Main	SFP 1	SFP 2
In Discards	0	0	0	28
In Errors	0	0	0	0
Out Discards	0	129456	0	126054
Out Errors	0	0	0	0

For each CPE, the **Interface** page displays Ethernet and wireless interface related details.

Radio

The **Radio** page displays the radio status of the BTS or the CPE device (as shown in Figure 83). Example: Frequency, Polarisation, link symmetry, and bandwidth details of the BTS.

Figure 83: The Details > Radio page for the BTS



The screenshot shows the 'Radio' page for 'BTS LAB Rig 2'. The page displays the following radio status details:

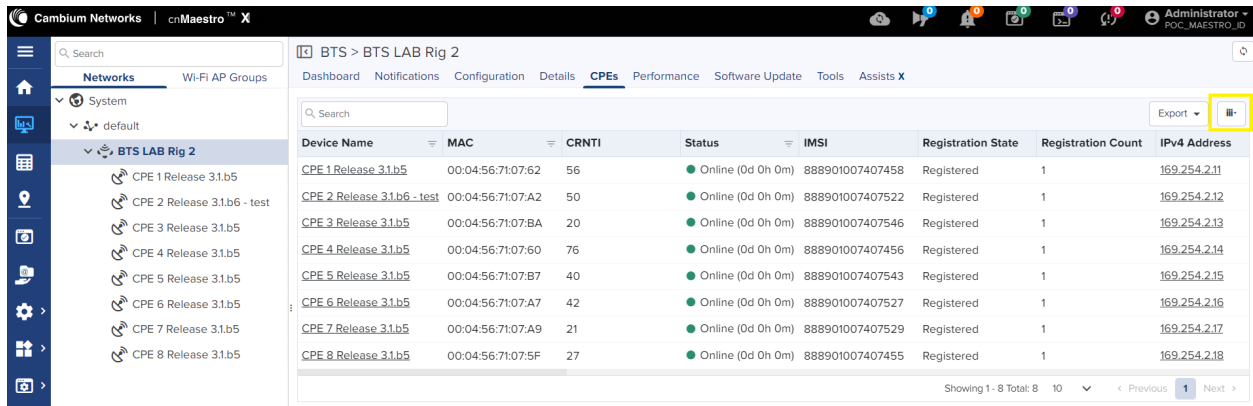
- Frequency: 25000.000 MHz
- Max EIRP: 25.0 dBm
- Polarisation: Horizontal
- Link Symmetry: 5:2
- Bandwidth: 112 MHz
- Target Rx Power: -60 dBm
- UL Tx Pwr Ctrl Initial Adjust: Enabled
- UL Tx Pwr Ctrl Cont Adjust: Enabled

For each CPE, the **Radio** page displays radio interface related details such as alignment active, range, current EIRP, UL sounding state and DL sounding state.

CPEs

The **CPEs** page provides information of all the connected and registered CPEs with the BTS (as shown in Figure 84). The **CPEs** page is applicable only to the BTS.

Figure 84: The CPEs page

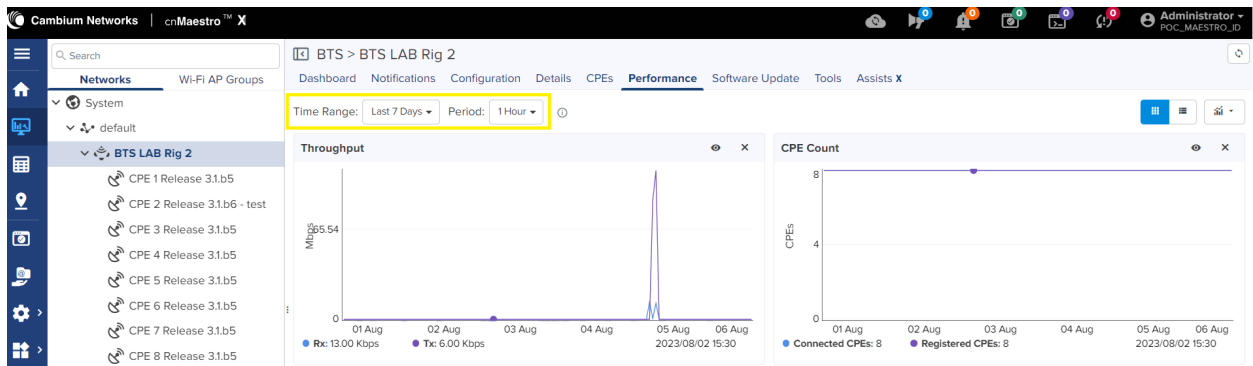


Use the **column Selector** icon (≡) to choose the required parameters and view the CPE data. For information on parameters available on the **CPEs** page, refer to the [Viewing Subscriber \(CPE\) Data](#) section.

Performance

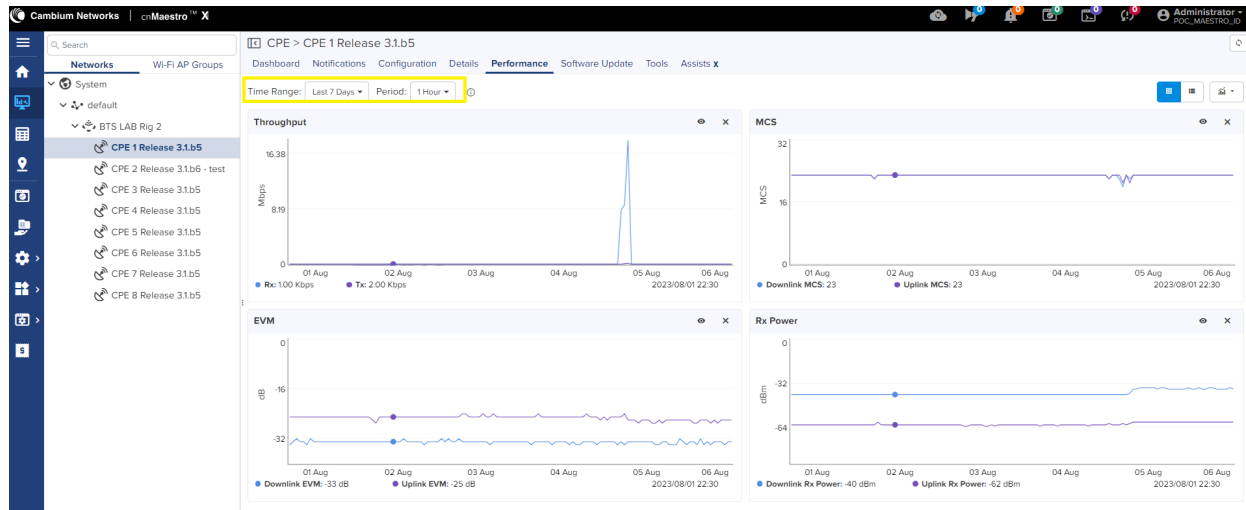
The **Performance** page displays the BTS throughput and count of CPEs for the selected time range and period in a graph format (as shown in [Figure 85](#)). Use **Time Range** and **Period** filters to view the performance data for the required period (for example, last 7 days and 1 hour).

Figure 85: The Performance page statistics for the BTS



For each CPE, the **Performance** page displays throughput, EVM, MCS, and Rx Power for the selected time range and period (as shown in [Figure 86](#)).

Figure 86: The Performance page for each CPE



Software Upgrade

You can upgrade or downgrade BTS and CPE software using the **Software Upgrade** page.



Note

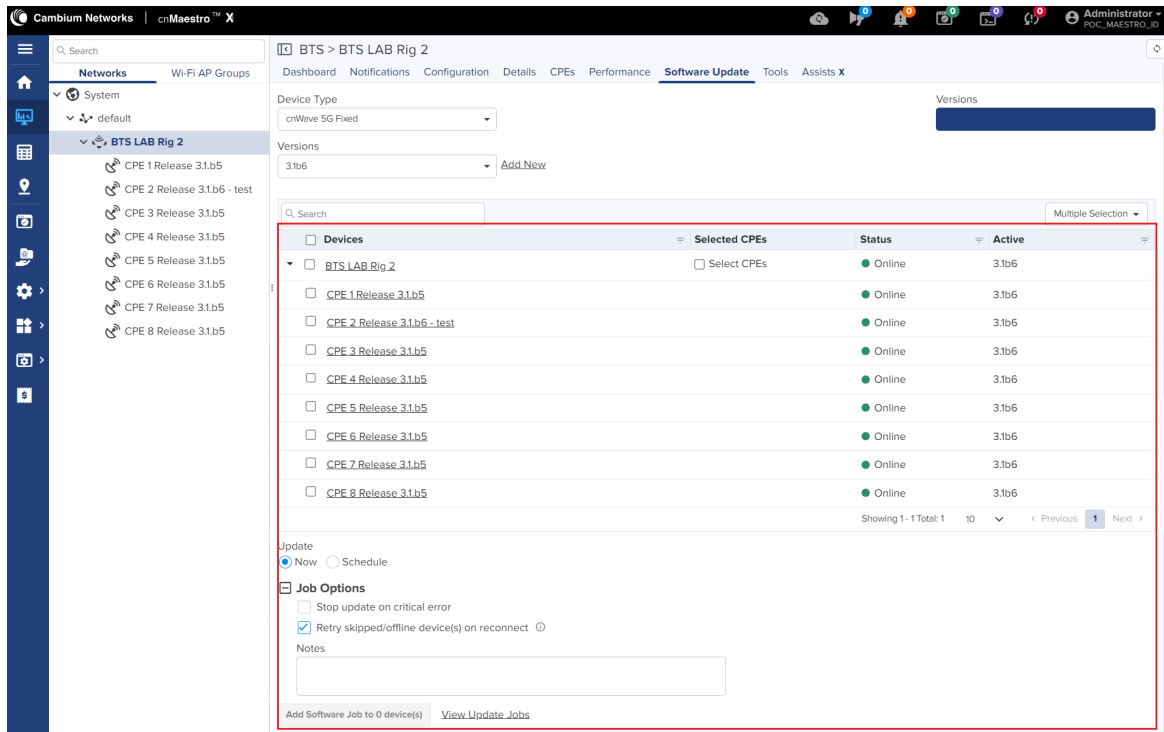
Software upgrade or downgrade using cnMaestro X is applicable only to cnWave™ 5G Fixed release 2.1 version and later versions.

To upgrade or downgrade the BTS and CPE software using the **Software Upgrade** page, perform the following steps:

1. From the BTS **Dashboard** page, navigate to the **Software Update** tab.

The **Software Update** page appears, as shown in [Figure 87](#).

Figure 87: The Software Update page



Note

When you select an individual CPE from the **Networks** group on the left column, the **Software Update** page allows to upgrade or downgrade only that specific CPE software.

2. Perform the following steps to upgrade or downgrade the software:
 - a. From the **Device Type** drop-down list, select `cnWave 5G Fixed`.
 - b. From the **Versions** drop-down list, select the required software version depending on the activity (upgrade or downgrade).
 - c. Select the check box against the required device names, for which you want to schedule this activity, in the **Devices** section (as shown in [Figure 87](#)).
 - d. In the **Update** section, select an option (**Now** or **Schedule**).
If you select **Schedule**, ensure to specify the start date and start time.
 - e. In the **Jobs Options** section, select the **Retry skipped/offline device (s) on reconnect** check box.
 - f. In the **Notes** text box, add a brief description about the activity (upgrade or downgrade).
 - g. Click **Add Software Jobs to <x> device (s)**.
The activity (upgrade or downgrade) is added to the job queue.

3. To run the scheduled job activity (upgrade or downgrade), perform the following steps:

- From the home page of cnMaestro UI, navigate to **Administration > Jobs > Software Update** page.
- On the **Software Update** page, select either **Manual** or **Auto** option.
- Select the check box against the required device name and details.
- Click **Start**.

The software upgrade or downgrade activity starts. You can view the activity status on the **Software Update** page. For more information about using the cnMaestro X UI and options available on the **Software Update** page, refer to the latest *cnMaestro User Guide*.

Tools

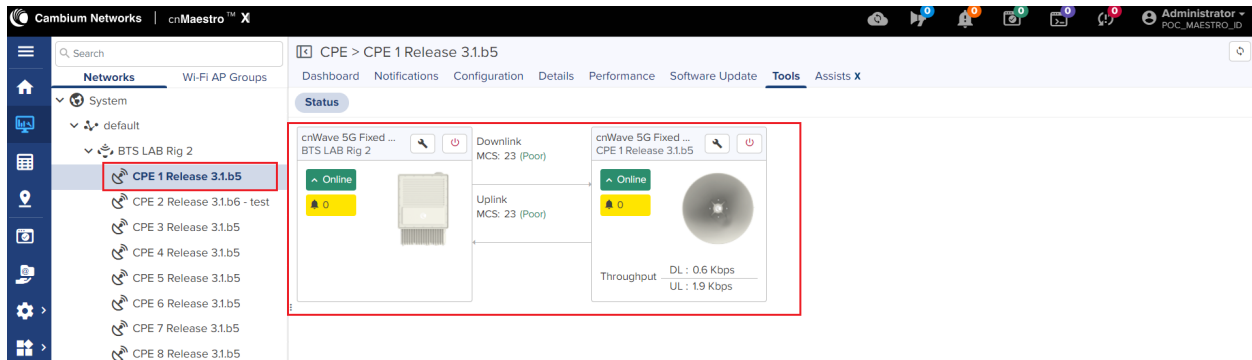
The **Tools** page contains the following tabs:



- [Status](#)
- [Link Test](#) (applicable only to BTS)

Status

The **Status** page displays device connection state (online or offline) for the BTS and a CPE. [Figure 88](#) is an example of the CPE connection state

Figure 88: *The Tools page for an individual CPE*



Use the  icon to download the Tech Support file, if required. To reboot the BTS or CPE device from the Tools page, use the  icon.

Link Test

The **Link Test** page allows you to test the links (uplink, downlink, or both), and analyze the link performance for a CPE. The test output helps in managing the traffic and troubleshooting the links for the selected CPE.

The **Link Test** page is available only when you select the BTS network on the left column, as highlighted in [Figure 89](#).

To test the link performance of a CPE, perform the following steps:

- On the **Link Test** page of cnMaestro UI, select the required CPE name from the **CPE** drop-down list.
- In the **Duration** text, provide an appropriate value (in seconds) to run the test.

The **Duration** parameter supports values from 0 to 60 (in seconds).

3. From the **Direction** parameter options, select the direction of transmission of the traffic that you want to test.

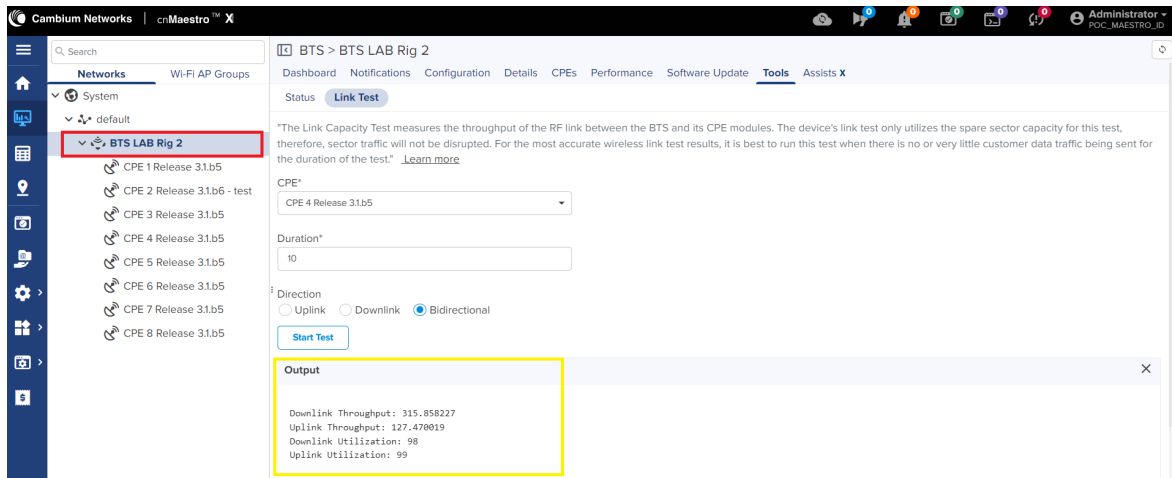
The Direction parameter supports the following options:

- Uplink
- Downlink
- Bidirectional

4. Click **Start Test**.

The **Output** section displays the test result, as shown in [Figure 89](#).

Figure 89: The Links Test page - cnMaestro X UI

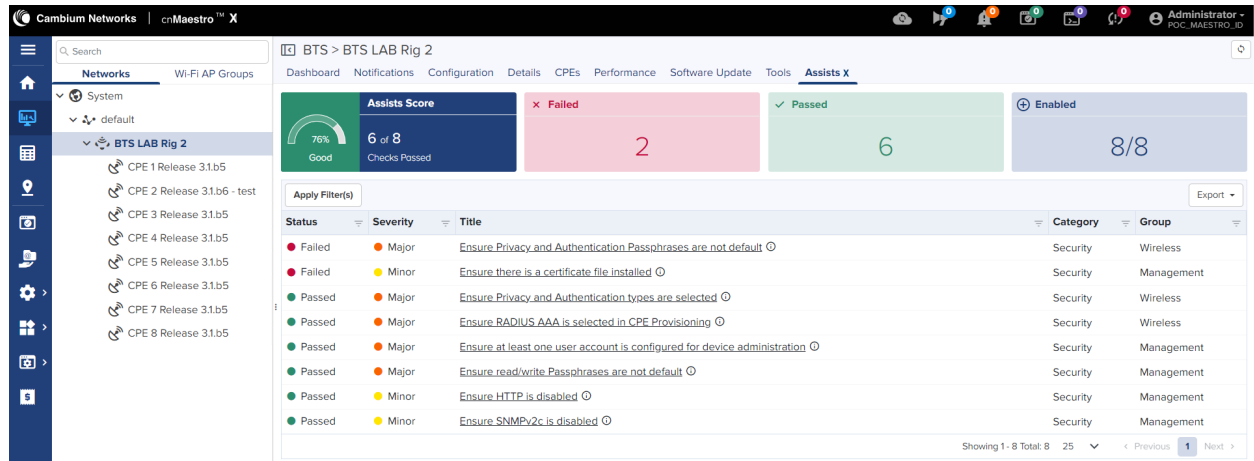


You can also test the link capacity of a CPE using the B1000 UI (BTS). For more information, refer to the [Link Capacity Test](#) section.

Assists X

The Assists X page displays statistics of failed and passed events for the BTS and CPEs. [Figure 90](#) is an example of failed and passed event statistics for BTS.

Figure 90: The Assists X page



Generating data reports

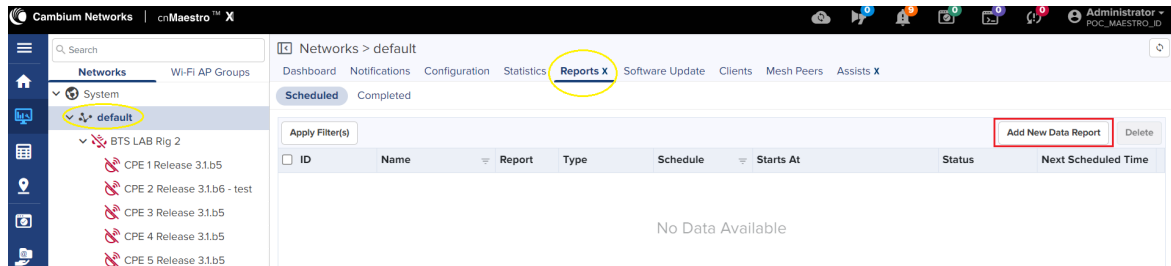
You can generate time-based data reports for cnWave 5G Fixed devices using the **Reports X** page in cnMaestro X UI. These reports help in administering and managing BTS and CPE devices.

To generate a data report, perform the following steps:

1. On the home page of cnMaestro X UI, Select **Monitor and Manage > default** (under the Networks group) > **Reports X**.

The **Reports X** page appears, as shown in [Figure 91](#).

Figure 91: The Reports X page in the cnMaestro X UI

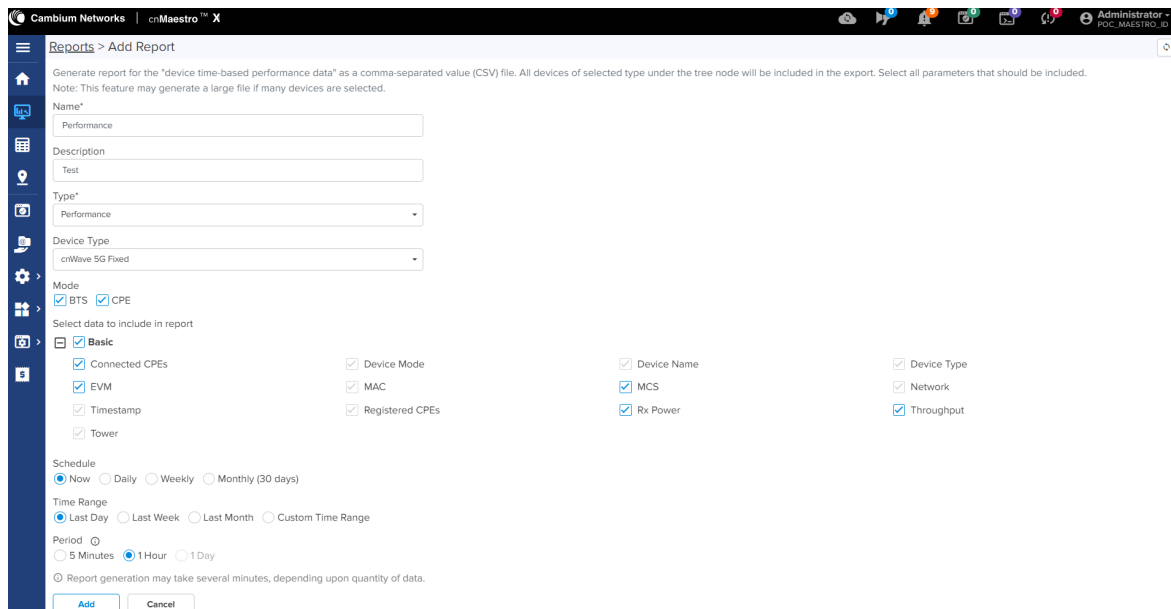


2. On the **Reports X** page, click **Add New Data Report**.

The **Reports > Add Report** page appears. This page allows you to select device-specific parameters and period (for example, daily or weekly) for generating a report.

3. Set the values for parameters, for example, as shown in [Figure 92](#).

Figure 92: Parameters on the Add Report page



[Table 47](#) lists and describes the parameters on the **Add Report** page.

Table 47: Parameters for generating a report

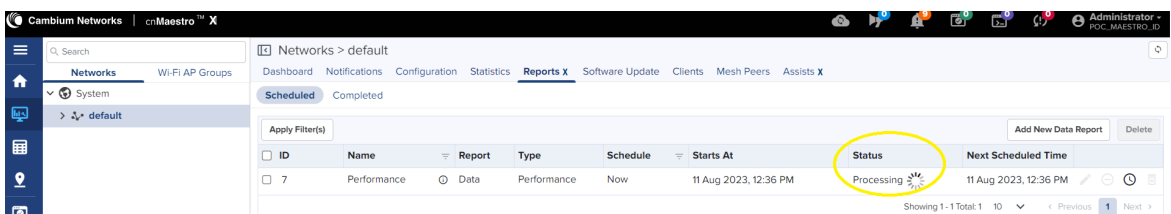
Parameter	Description
Name	<p>Name of the report that you want to generate.</p> <p>This is a mandatory field.</p> <p>Provide an appropriate name in the text box. Example: Performance</p>
Description	A brief description of the report.
Type	<p>The report type that you want to generate.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Devices • Performance • Active Alarms • Alarm History • Events • Clients • Mesh Peers <p>Select the required report type from the drop-down list. This is a mandatory field.</p>
Device Type	<p>The device for which you want to generate the report.</p> <p>The value of this parameter must always be cnWave 5G Fixed.</p> <p>Select the device name from the drop-down list.</p>
Mode	<p>The device mode for which you want to generate the report.</p> <p>Select BTS, CPE or both (if required).</p>
Select data to include in report	<p>Check the device-specific parameters that you want to include in the report.</p> <p>Example: Connected CPEs, EVM.</p> <p>The report, when generated, displays these parameters in CSV format.</p>
Schedule	<p>Time at when you want to generate the report.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Now • Daily • Weekly • Monthly <p>Choose the period.</p>

Parameter	Description
	Note: When you select Daily, Weekly, or Monthly, ensure to specify start date, start time, end, and number of occurrences (1-100). For more details on the schedule specific options, refer to the latest cnMaestro User Guide .
Time Range	The time range for which you want to generate the report. Following options are supported: <ul style="list-style-type: none"> Last Day Last Week Last Month Custom Time Range Choose the required time range.
Period	Duration for which you want to generate and view the report. Following options are support: <ul style="list-style-type: none"> 5 Minutes 1 Hour 1 Day Choose the required period.

4. Click **Add**.

The report is scheduled, processed, and generated. The **Reports X** page displays the status while generating the report, as shown in [Figure 93](#).

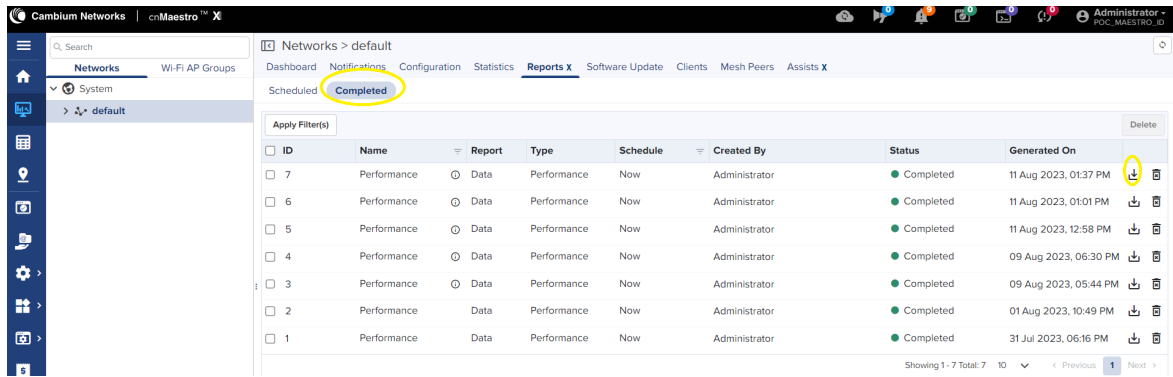
Figure 93: *The report scheduled status*




5. To download and view the report, select the **Completed** tab on the **Reports X** page.

The **Reports X** page displays all reports that are scheduled, as shown in [Figure 94](#).

Figure 94: The Completed tab on the Reports X page



You can also view the same report using the **Administration > Jobs > Reports X** page.

6. Use the  icon to download the data report (in .xls format).

You can view and modify this report locally.

Appendix 2: Acronyms and Abbreviations

Table 48 lists acronyms and abbreviations used in this guide.

Table 48: List of acronyms and abbreviations

Term	Definition
5G NR	5G New Radio (From Release 15, the 3GPP consortium refers to the air interface as 5G New Radio)
BTS	Base Transceiver Station
CIR	Committed information rate
C-RNTI	Call-Radio Network Temporary Identifier
CIR	Committed information rate
CPE	Customer Premise Equipment
dBm	Decibel relative to a milliwatt
DNS	Domain Name System
DL	Downlink
EIRP	Effective Isotropic Radiated Power
ESN	Electronic Serial Number
EVM	Error Vector Magnitude
FQDN	Fully qualified domain name
GHz	Gigahertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
LoS	Line of Sight
LPU	Lightning Protection Unit
MAC	Media access control
MCS	Modulation and Coding Scheme
MHz	megahertz
MSN	Manufacturer Serial Number
MU-MIMO	Multi- user multi-input-multi-output (MU-MIMO)
ms	Millisecond
NTP	Network Time Protocol
OFDMA	Orthogonal Frequency Division Multiple Access
ODU	Outdoor Unit
PC	Personal computer

Term	Definition
PDSCH	Physical Downlink Shared Channel
PDCCH	Physical Downlink Control Channel
PMP	Point-to-MultiPoint
POC	Proof of Concept
PoE	Power over Ethernet
PPS	Pulse Per Second
PSS	Primary Synchronization Signal
PSU	Power Supply Unit
PUSCH	Physical Uplink Shared Channel
PUCCH	Physical Uplink Control Channel
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RACH	Random Access Channel
RADIUS	Remote Authentication Dial-In Service
RSSI	Receiver Signal Strength Indication
SFP	Small form-factor pluggable (transceiver)
SIM	Subscriber Identification Module
SI-RNTI	System Information-Radio Network Temporary Identifier
SNR	Signal-to-Noise Ratio
SKU	Stock Keeping Unit
SNMP	Simple Network Management Protocol
TDD	Time Division Duplexing
UI	User Interface
UL	Uplink
VLAN	Virtual Local Area Network

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified ConnectedPartners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Installation and Configuration Guides	http://www.cambiumnetworks.com/guides
Technical training	https://learning.cambiumnetworks.com/learn
Support website (enquiries)	https://support.cambiumnetworks.com
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list to contact	http://www.cambiumnetworks.com/contact-us/
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

© Copyright 2024 Cambium Networks, Ltd. All rights reserved.