Cambium Networks™

CONFIGURATION GUIDE

cnWave™ 5G Fixed

Release 4.2

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 to 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

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 ISEDC '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).

- Cambium Networks complies with the European Regulation 2023/988 of 10 May 2023 on General Product Safety. EU Authorized Representative: Cambium Networks Europe B.V., Muiderstraat 1, 1011PZ Amsterdam, Netherlands. Contact Information: GPSR@cambiumnetworks.com.

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 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.

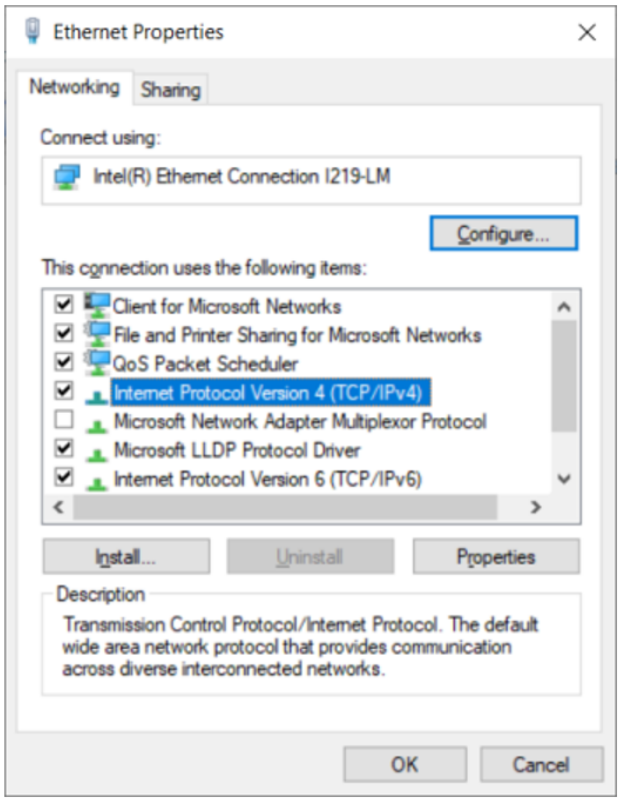
2. Select **Ethernet** > **Change adapter settings**.

   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*



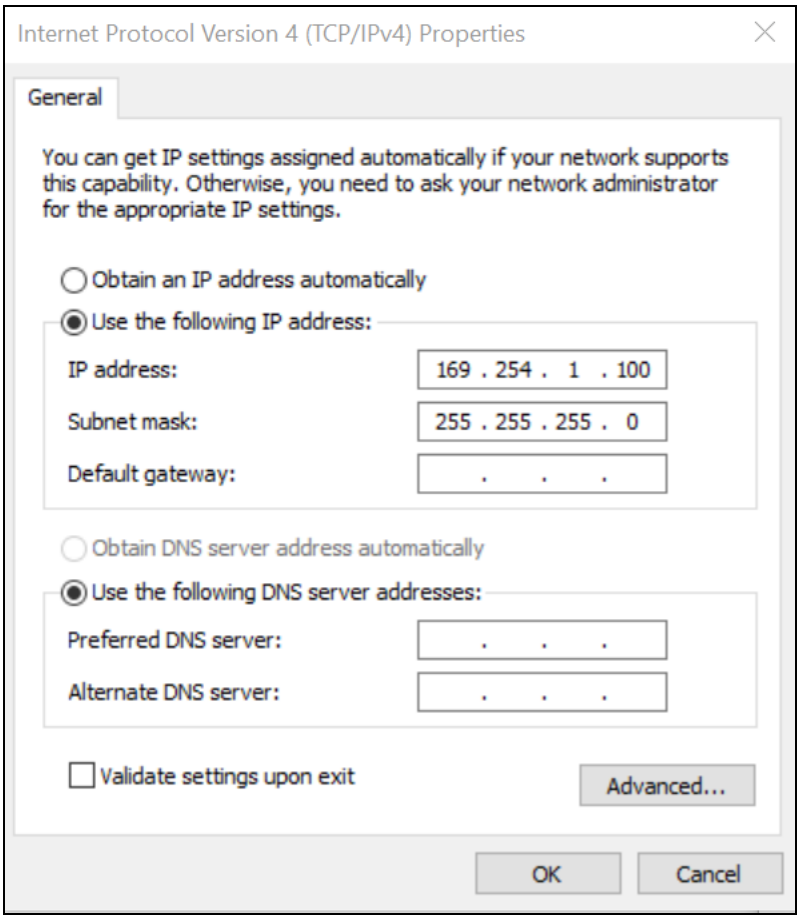
   By default, the **Networking** tab is selected.

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.

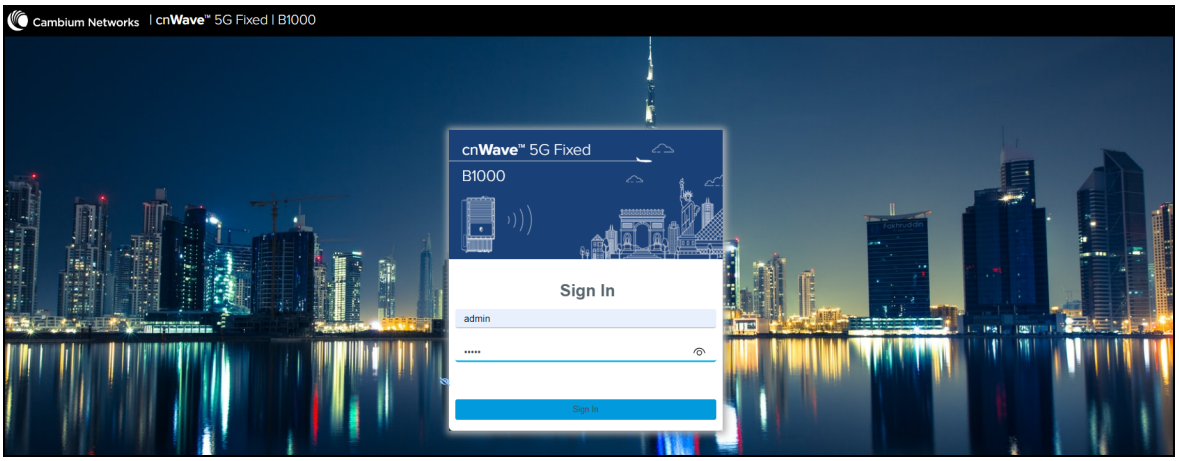
Accessing the B1000 UI

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

   You can use the show-password eye icon (👁) to view the password characters.

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*

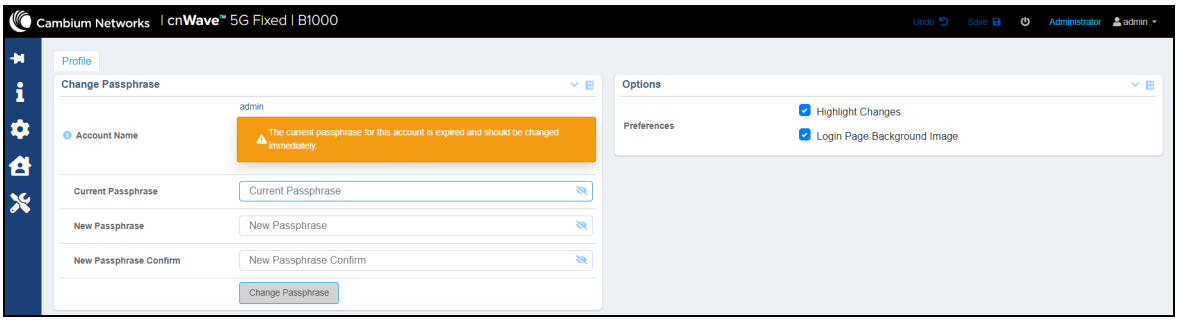


Table 1 lists and describes the parameters available on the **Profile** page.

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 a 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: `admin`
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. The following options are supported: • **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 quickly monitor 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 required options.

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

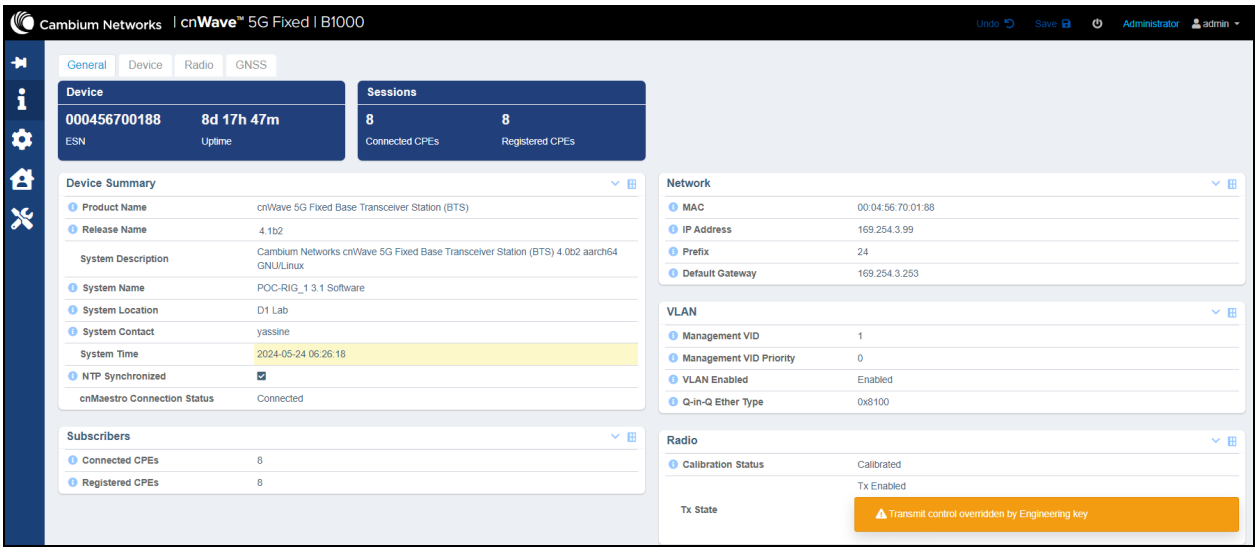
UI Control	UI Control name	Description
	Dashboard	To open the main dashboard page of the required product. Applicable to both B1000 and C100 UIs.
	System	To configure the required system settings of cnWave™ 5G Fixed platform of products. **For BTS**: • General • Management • Radio • Interface • SFP Module • CPE Provisioning • Synchronisation • Syslog **For CPE**: • General • Management • Radio

UI Control	UI Control name	Description
		• Interface • Session • RADIUS Authentication Applicable to both B1000 and C100 UIs.
	Subscribers	To view (read-only) all the data related to CPE subscribers. 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, VLAN, radio, and other system-related details of the BTS. 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 checkbox 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.

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

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*

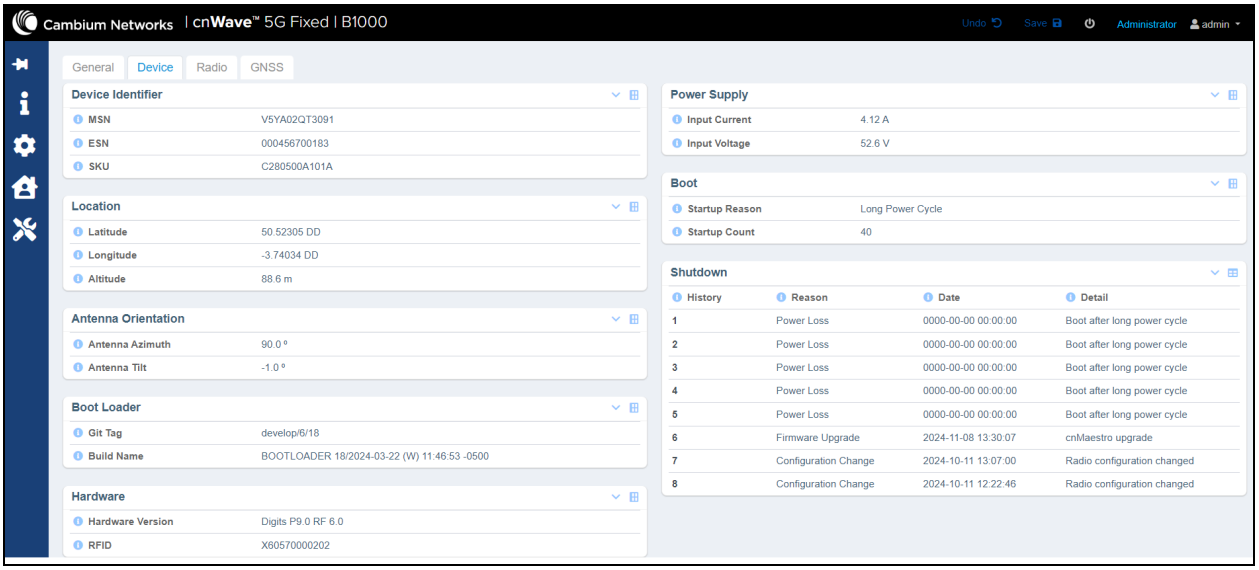


Table 4 lists and describes parameters available on the **Device** page.

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) indicate 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.

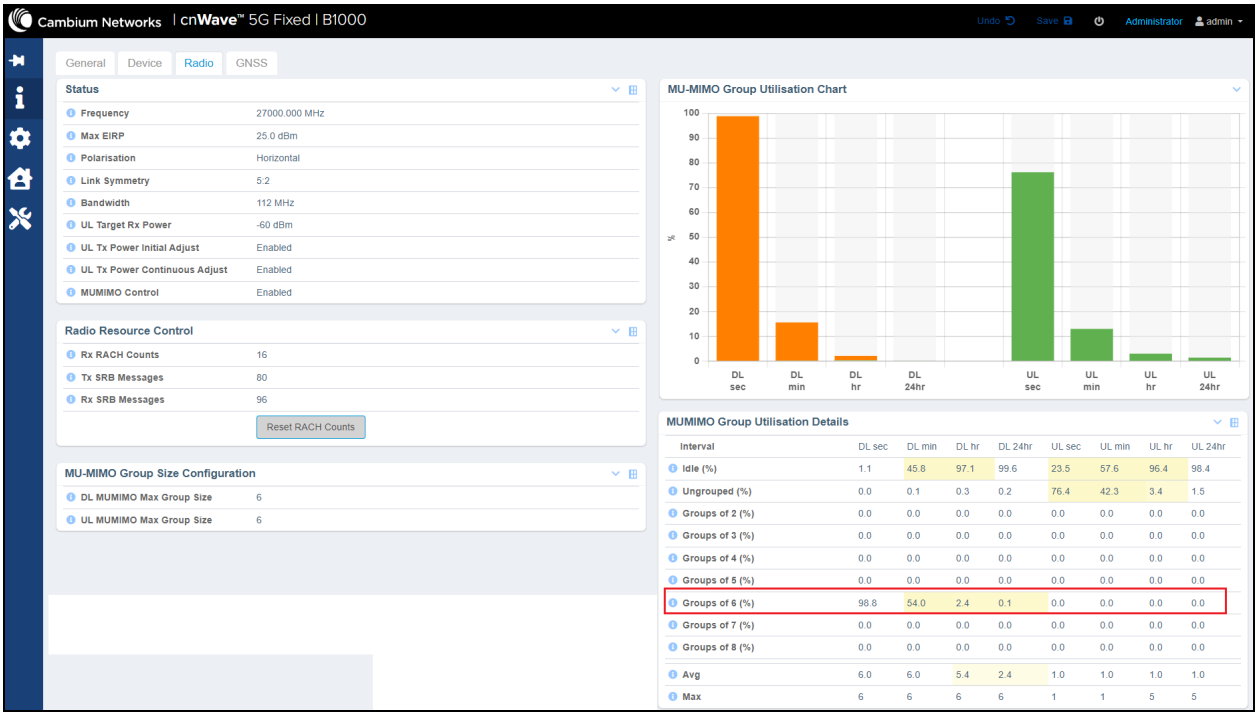
Parameter	Description
Altitude	Altitude (in m) of the geographical location relative to mean sea level (MSL).
Antenna Orientation	
Antenna Azimuth	The direction in azimuth that the BTS is pointing towards. 0.0, 90.0, 180.0, and 270.0 values (in degrees) correspond to magnetic North, East, South, and 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. 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.
Power Supply	
Input Current	The device measured input current (BTS only).
Input Voltage	The device measured input voltage (BTS only).
Boot	
Startup Reason	Indicates the reason for the previous system reboot. The following reasons are supported: • 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 increments each time the device starts.
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.

Parameter	Description
Reason	Reasons specified for each boot history. The following boot reasons are supported: • 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.
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.
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.

Parameter	Description
	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). Note: When you place the cursor on the chart, you can view the details of the MUMIMO group utilisation.	

Parameter	Description
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*

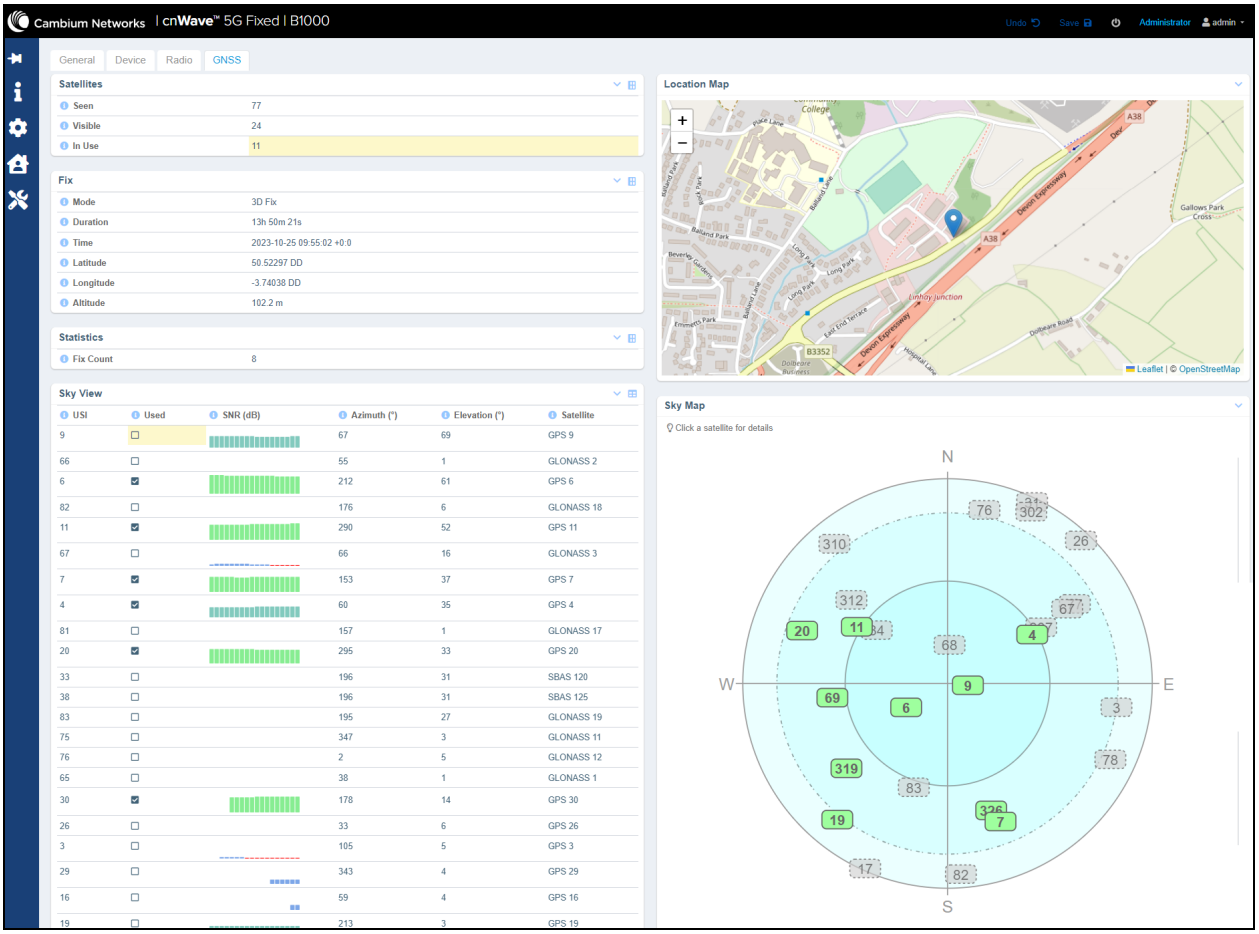


Table 5 lists and describes parameters available on the **GNSS** page.

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).

Parameter	Description
Fix	
Mode	Indicates the GPS fix mode. 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) indicate 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.

Parameter	Description
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.
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 in 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.

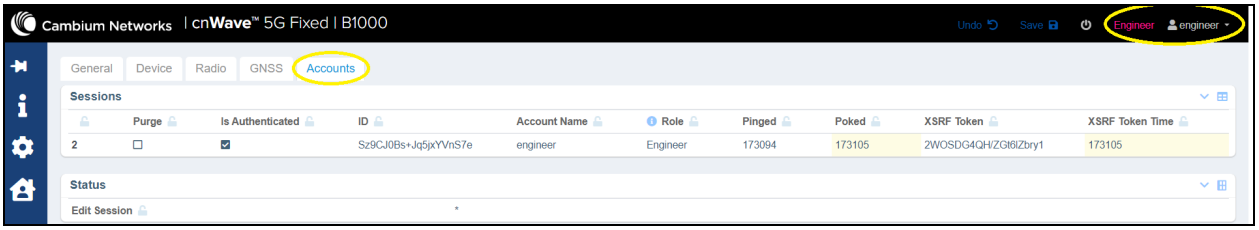
Accounts

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 (CPE) 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
- QoS
- SFP Module
- CPE Provisioning
- Synchronisation
- Syslog

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:

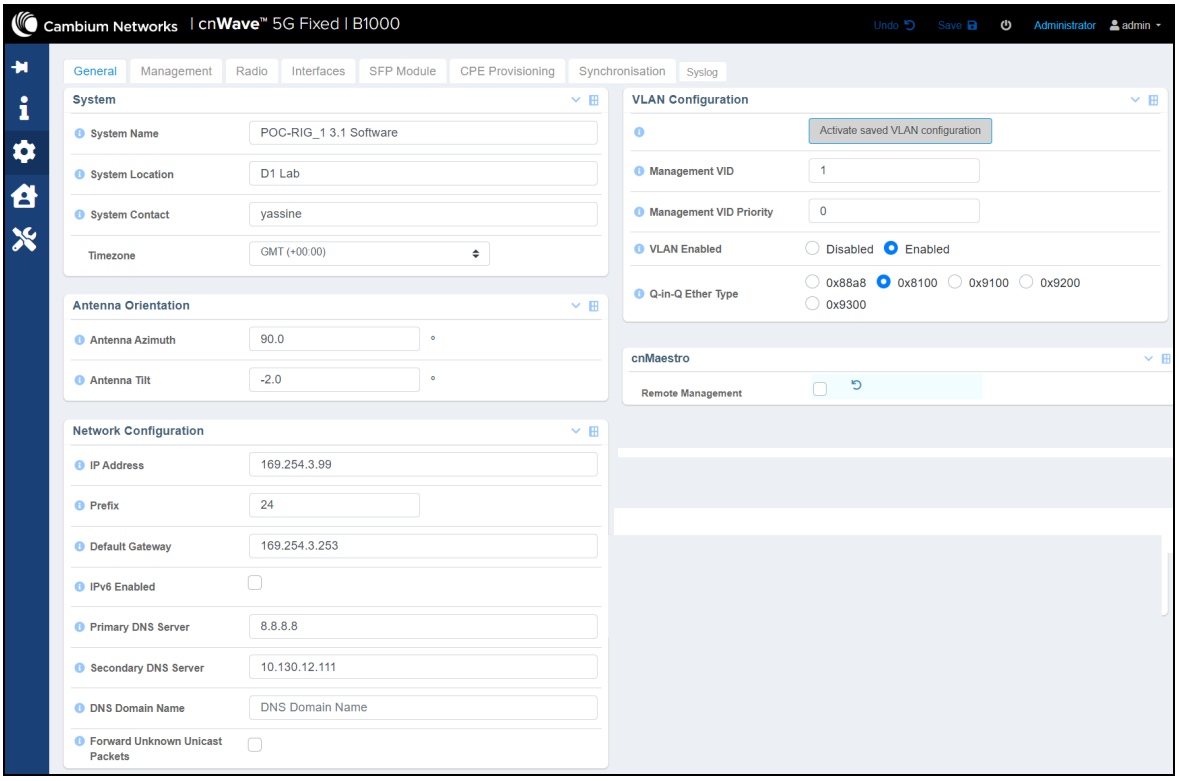
1. Log on to the B1000 UI (as described in Accessing the B1000 UI).

   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	

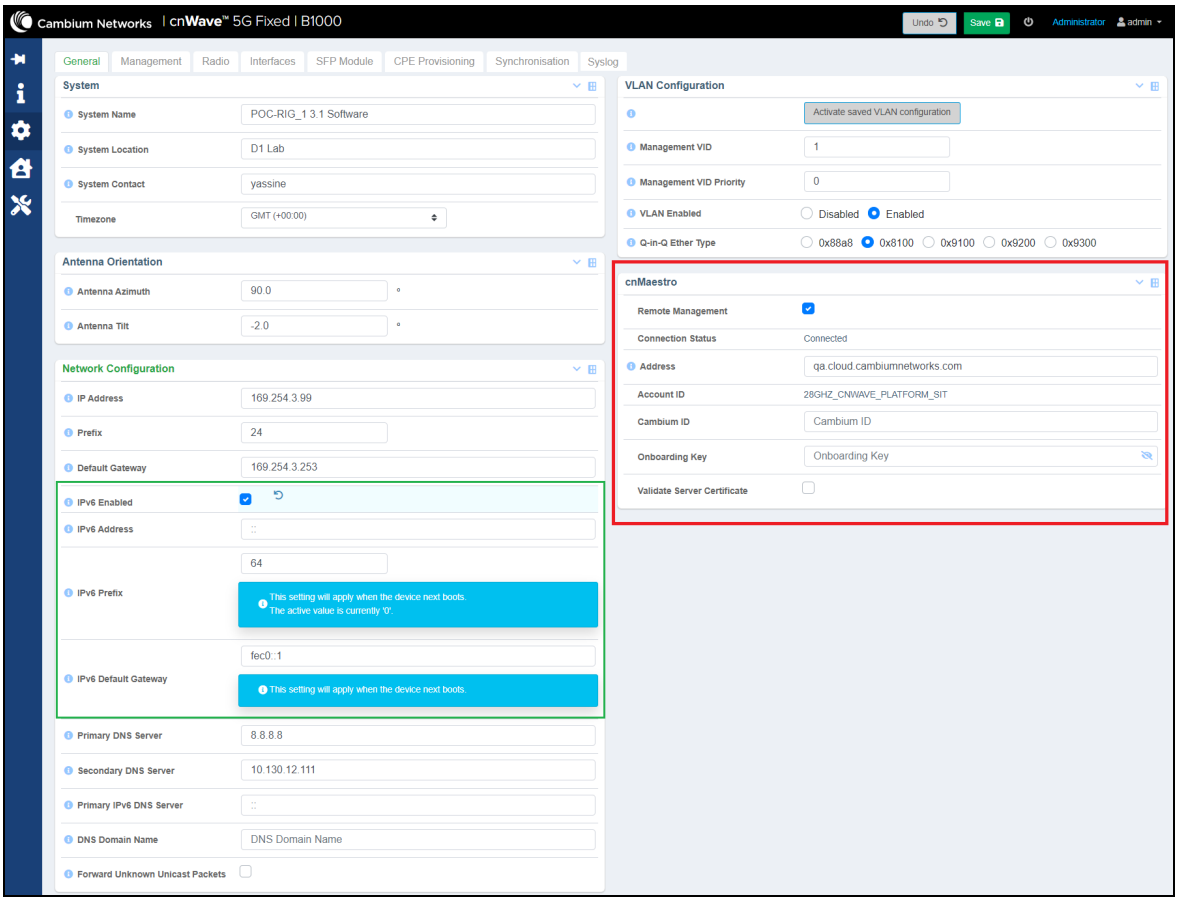
Parameter	Description
Antenna Azimuth	The direction in azimuth that the BTS is pointing towards. 0.0, 90.0, 180.0, and 270.0 values (in degrees) correspond to magnetic North, East, South, and West, respectively. **Note**: The radio does not use this value but reports the value to cnMaestro.
Antenna Tilt	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 IPv4 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 IPv4 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 IPv4 address of the default gateway (if any used for managing the device. Type an appropriate value in the text box.
IPv6 Enabled	Determines whether IPv6 is enabled for BTS management (in addition to the always enabled IPv4 management access). By default, this parameter is disabled. Select the checkbox to enable IPv6 for device management. **Note**: When the select the **IPv6 Enabled** checkbox, the following IPv6-specific parameters appear (as shown in Figure 11): • IPv6 Address • IPv6 Prefix • IPv6 Default Gateway
IPv6 Address	This parameter appears when the **IPv6 Enabled** checkbox is selected. Indicates the IPv6 address assigned to the network interface that is used for the device management. Enter a valid IPv6 address.

Parameter	Description
Pv6 Prefix	This parameter appears when the **IPv6 Enabled** checkbox is selected. Indicates the IPv6 network prefix assigned to the network interface that is used for the device management. Enter an appropriate value. **Note**: Any change to this setting is applicable when the device reboots next. The active value of this setting is currently 0.
IPv6 Default Gateway	This parameter appears when the **IPv6 Enabled** checkbox is selected. Indicates the IPv6 default gateway address used for the device management. Enter an appropriate value. **Note**: Any change to this setting is applicable when the device reboots next.
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.
Secondary DNS Server	The IP address that is assigned to the secondary DNS Server (if any). This IP address is used for managing the device. Type an appropriate value in the text box.
DNS Domain Name	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. Type an appropriate value in the text box.
Forward Unknown Unicast Packets	Determines whether the BTS forwards the Ethernet packets to CPEs on receiving the packet with a unicast destination address. By default, the checkbox 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. If you select the checkbox, 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.
VLAN Configuration	
Activate saved VLAN configuration	An action that updates the live VLAN configuration for using the currently saved settings unless they are overridden by RADIUS.

Parameter	Description
	Note: If you have changed **Management VID**, then you will lose contact with the device until you make the corresponding changes.
Management VID	The VLAN ID that is used to communicate with BTS and CPE for management purpose. Default value: 1 - which implies that there is no VLAN in the system. You can set up an ID value between 2 and 4094. Type an appropriate value in the text box. To understand the concept of VLAN, refer to the VLAN section.
Management VID Priority	The priority value that is set for the management VLAN ID.
VLAN Enabled	Determines whether the VLAN functionality for the BTS and all linked CPEs is enabled. Default value: Disabled Select the required option. If you change the value of this parameter, reboot the device for applying the change. **Note**: If this parameter is disabled, then you cannot configure VLAN-related parameters on the C100 UI (CPE).
Q-in-Q Ether Type	The Ether type values used for Q-in-Q (802.1ad) and outer tag (S-Tag). The following values are supported: • 0x88a8 • 0x8100 • 0x9100 • 0x9200 • 0x9300 Default value: 0x88a8 Select the required Ether type tag. If you change the value of this parameter, reboot the device for applying the change.

Parameter	Description
	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.
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.	
cnMaestro	
Remote Management	Determines whether the remote management of the BTS system through cnMaestro X is enabled. Select the checkbox if you want to manage the BTS system remotely through cnMaestro X. When you select the checkbox, cnMaestro X-specific parameters appear as shown in Figure 11.

Figure 11: *An example of IPv6 Enabled and cnMaestro-specific parameters*



The following parameters (as listed in Table 8) appear only if you select the **Remote Management** checkbox in the **cnMaestro** section:

Table 8: Parameters required for the cnMaestro configuration

Parameter	Description
cnMaestro	
Connection Status	Indicates the connection status of the BTS device with the cnMaestro X server. When you select the **Remote Management** checkbox, the BTS device tries to connect to the required cnMaestro X server and onboard automatically. During this connecting and onboarding process, this parameter displays the connection status messages, as described: • 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**. • When BTS connects to the cnMaestro X server and onboards successfully, then this parameter displays the status as **Connected**.
Address	The IP address or the domain name of the required cnMaestro X server. Type an appropriate address in the text box. **Note**: The address can be either an IP or URL of the cnMaestro On-Premises instance.
Account ID	The account ID of the required cnMaestro X server. This is a read-only parameter that displays the value when BTS connects to the required cnMaestro X server.
Cambium ID	The user account ID that is assigned and associated with the cnMaestro X server. 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. Type an appropriate value in the text box.

Parameter	Description
Onboarding Key	The license key (or a password) that is set on purchasing the BTS device. You can set the onboarding key using the **Onboard** > **Settings** page of the cnMaestro UI. For more information, refer to the cnMaestro Configuration section. Type an appropriate value in the text box.
Validate Server Certificate	Indicates whether a server certificate is installed at the customer site for the validation purpose. Select the checkbox if the server certificate is installed at the customer site.

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

VLAN

A V**irtual 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

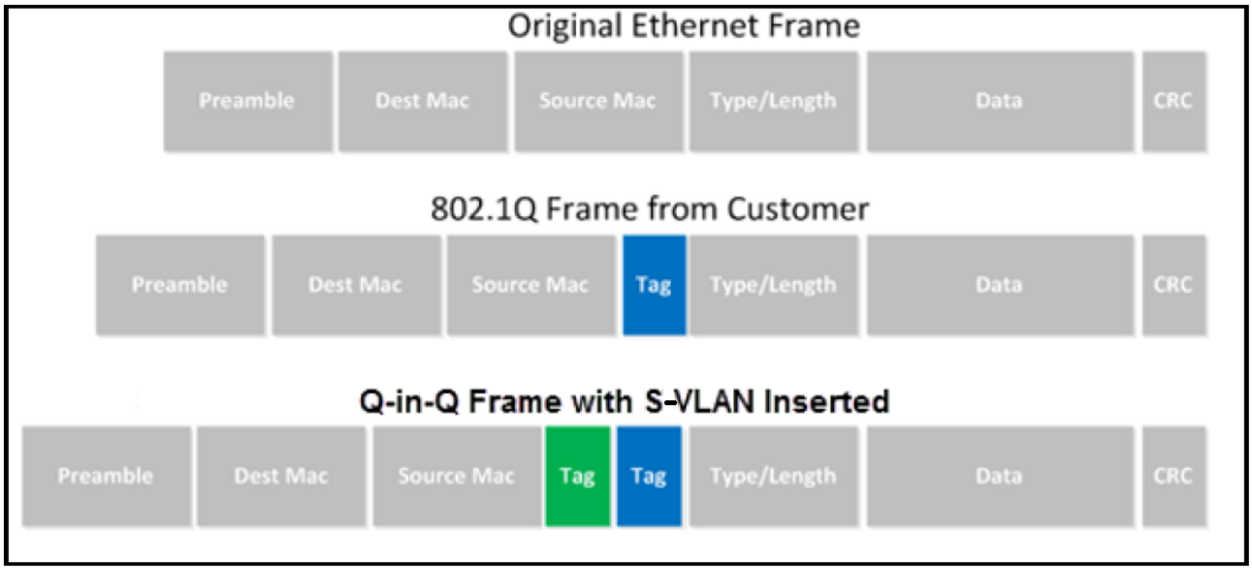
Q-in-Q (also known as double tagging or 802.1ad) is a networking technology that extends the capabilities of VLAN tagging. It's used for addressing some limitations of standard VLAN tagging, especially when dealing with service provider networks or complex network architectures.

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 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

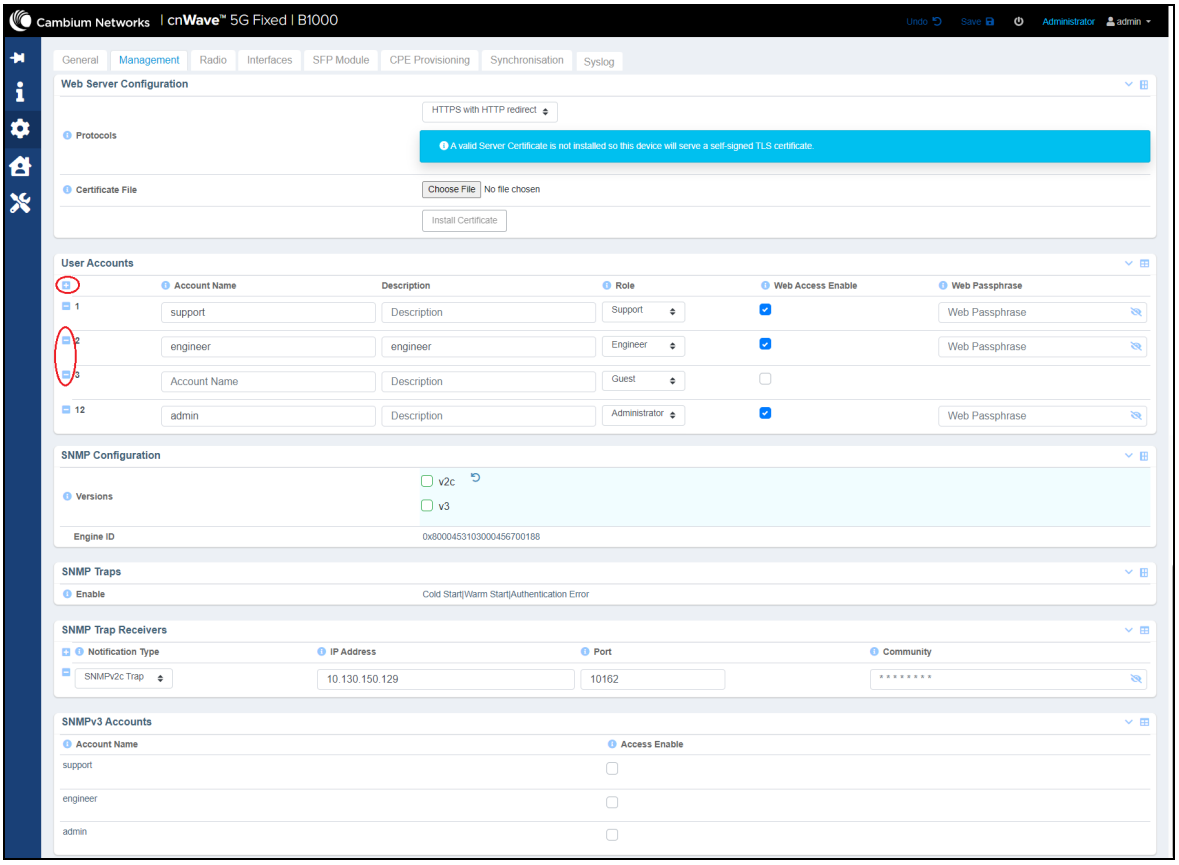
The **Management** page allows you to set multiple user accounts and SNMP configuration related information. This configuration allows the users to manage the B1000 dashboard (web UI) and BTS using SNMP.

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	Type of protocol that must be configured for accessing and managing the web UI of BTS. This parameter supports the following options: • **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.

Parameter	Description
	• **HTTPS with HTTP redirect**: Indicates that both HTTP and HTTPS are available, but an incoming HTTP connection is automatically redirected to HTTPS. Default value: HTTPS with HTTP redirect Select the required protocol from the drop-down list. **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.
Certificate File	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). To upload a certificate file (.PEM) from the desired location locally, perform the following steps: a. Click **Choose File**. A file folder appears. b. Browse the location where you have saved the required certificate file (.PEM) on your machine. c. Click **Open**. The certificate file is selected, and the file name appears next to the **Choose File** button. d. Click **Install Certificate**. The selected certificate file is installed, which is authenticated and encrypted.
User Accounts	
Account Name	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. Provide an appropriate name in the text box. Example: admin or user1 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.

Parameter	Description
	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.
Description	A brief description of the account. Provide a brief description for the user account that you want to add. Example: Super admin
Role	Specifies the role of the user who wants to access the device. This parameter supports the following roles, which have different capabilities and serve different functions: • **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 roles 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. Select an appropriate option from the drop-down list.

Parameter	Description
Web Access Enable	Determines whether the access for web UI of the BTS device is enabled for the selected role. Select the checkbox if you want to enable web access for the required user role. **Note**: Multiple users are allowed to access the UI simultaneously.
Web Passphrase	The passphrase (password) that is assigned to the user role of this account for accessing the web UI. Type an appropriate password in the text box.
SNMP Configuration	
Versions	The version of the SNMP protocol that is supported by the agent running on this BTS device. The SNMP protocols are used for managing and monitoring the network devices. The following SNMP protocol versions are supported: • V2c : A standard and simpler community-based security model. It is an obsolete version with weak security. • V3: An advanced version designed to address security, access control, privacy, and authentication issues. Choose the required SNMP version.
Engine ID	Unique ID that is used by the SNMP agent. It is used as part of the SNMPv3 security framework that includes authentication and encryption.
Note: A message is visible after the **Engine ID** 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.	
Port	This parameter appears only when you select an SNMP version (V2c or V3). Indicates the network port number assigned to the SNMP agent, which is running on the device. Default value: 161 Provide an appropriate value in the text box.
The following parameters appear only when you set V2c in the **Versions** field, as shown in Figure 14.	
Read-Only Community	Name of the SNMP V2c community for read-only access to the device.

Parameter	Description
	Provide an appropriate value in this text box.
Read/Write Community	Name of the SNMP V2c community for read-write access to the device. Provide an appropriate value in this text box.
SNMP Traps	
Enable	Indicates the categories of SNMP traps sent by the device. This is a ready-only parameter. **Note**: This is a Read-Only Community string used by the SNMP agent. It is recommended to choose a random string for security reasons. This string must be different from the Read-Write Community string.
SNMP Trap Receivers	
Notification Type	The type of notification that the BTS device sends to the trap receiver. The following options are supported: • disabled: SNMP notifications are not sent to the trap receiver. • SNMPv2c Trap • SNMPv2c Inform • SNMPv3 Trap • SNMPv3 Inform If **Trap**-specific notification is set, the BTS device sends the trap notification only once and does not wait for the trap receiver's acknowledgment. If **Inform**-specific notification is set, then the BTS device sends the information few times until it receives an acknowledgment from the receiver (such as password check). By default, the **disabled** option is selected. Select the required notification type from the drop-down list. To add a notification, click the + icon beside the **Notification Type** parameter column. To delete a notification, click the - icon. **Note**: This is a Read-Write Community string used by the SNMP agent. It is recommended to choose a random string for security reasons. This string must be different from the Read-Only Community string.

Parameter	Description
When you select a value (except for disabled) from the **Notification Type** drop-down list, the following parameters appear (as shown in Figure 15):	
IP Address	The IP address assigned to the server that receives SNMP traps. All enabled SNMP traps are sent to this address. Enter a valid IP address of the server.
Port	The network port assigned to the server that receives SNMP traps. Enter a valid network port number. **Note**: The zero (0) value is not valid.
Community	Applicable only when you select `SNMPv2c Trap` or `SNMPv2c Inform` from the **Notification Type** drop-down list. Indicates the SNMPv2c community name for providing access to the trap receiver. Enter an appropriate value in the text box. **Note**: A community name must contain at least eight characters in length.
Account Name	Applicable only when you select `SNMPv3 Trap` or `SNMPv3 Inform` from the **Notification Type** drop-down list. Specifies the account name used for authentication to the BTS device. **Note**: The account name must be unique and contain lower case letters, numbers, and hyphens. In addition, the account name must start with a letter. Enter a valid value in the text box.
Authentication Type	Applicable only when you select `SNMPv3 Trap` or `SNMPv3 Inform` from the **Notification Type** drop-down list. Indicates the authentication type to use. This parameter supports the following options: • None • MD5 • SHA1 Select the required option from the drop-down list.
Authentication Passphrase	Applicable only when you select `SNMPv3 Trap` or `SNMPv3 Inform` from the **Notification Type** drop-down list.

Parameter	Description
	Indicates the authentication passphrase assigned to the trap receiver. The parameter can contain any combination of ASCII characters. The value must contain eight characters in length. Type a valid value in the text box.
Privacy Protocol	Applicable only when you select `SNMPv3 Trap` or `SNMPv3 Inform` from the **Notification Type** drop-down list. Indicates the protocol that must be used for account privacy. This parameter supports the following options: • None • DES • AES Select the required option from the drop-down list. **Note**: If the value is set to None, the **Privacy Passphrase** parameter value is ignored.
Privacy Passphrase	Applicable only when you select `SNMPv3 Trap` or `SNMPv3 Inform` from the **Notification Type** drop-down list and **Privacy Protocol** is not set to `None`. Specifies the privacy passphrase assigned to the trap receiver. The value of this parameter can contain any combination of ASCII characters. The value must consist of eight characters in length. Type a valid value in the text box. **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.
SNMPv3 Accounts - This section allows you to set access control, authentication, and privacy-related properties for the roles selected in the **User Accounts** section.	
Account Name	The account name that is used for authentication to the BTS device. This is read-only parameter that contains account names, which you added in the **User Accounts** section.
Access Enable	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).

Parameter	Description
	Select the checkbox for the required account name. This setting permits the user account to access the BTS device using SNMP. **Note**: To modify this parameter, you must enable V3 using the **Versions** parameter in the **SNMP Configuration** section.
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 16):	
Authentication Type	Indicates the authentication type to use. This parameter supports the following options: • None • MD5 • SHA1 Select the required option from the drop-down list.
Authentication Passphrase	The authentication passphrase assigned to the user role. This passphrase must be same as the one that is set at the SNMP site for this user role. The value of this parameter can contain any combination of ASCII characters. The value must consist of eight characters in length. Type a valid value in the text box.
Privacy Protocol	The protocol that must be used for account privacy. This parameter supports the following options: • None • DES • AES Select the required option from the drop-down list. **Note**: If the value is set to None, the **Privacy Passphrase** parameter value is ignored.
Privacy Passphrase	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. The value of this parameter can contain any combination of ASCII characters. Also, the value must consist of eight characters in length. Type a valid value in the text box.

Parameter	Description
	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.

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*

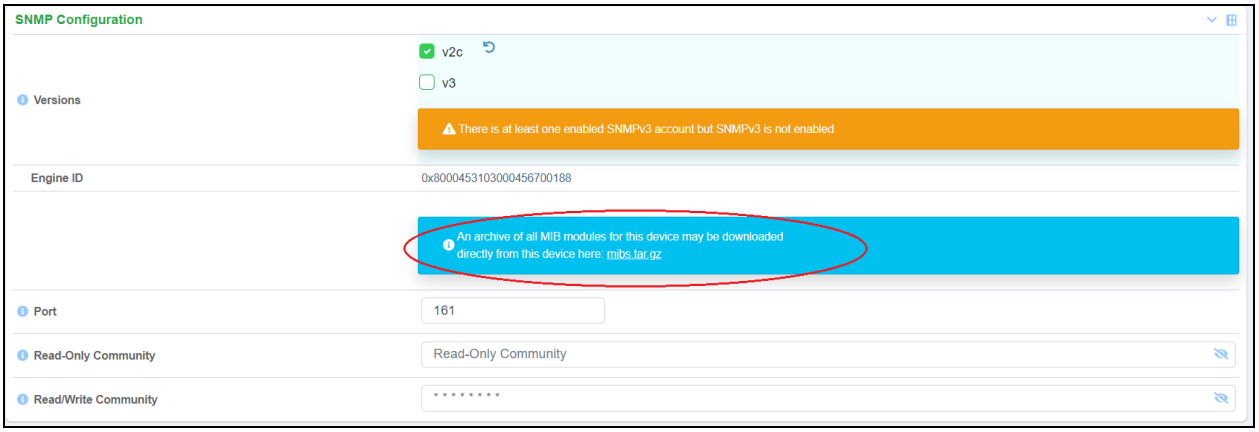


Figure 15 is an example of the **SNMP Trap Receivers** settings.

Figure 15: *The SNMP Trap Receivers section*

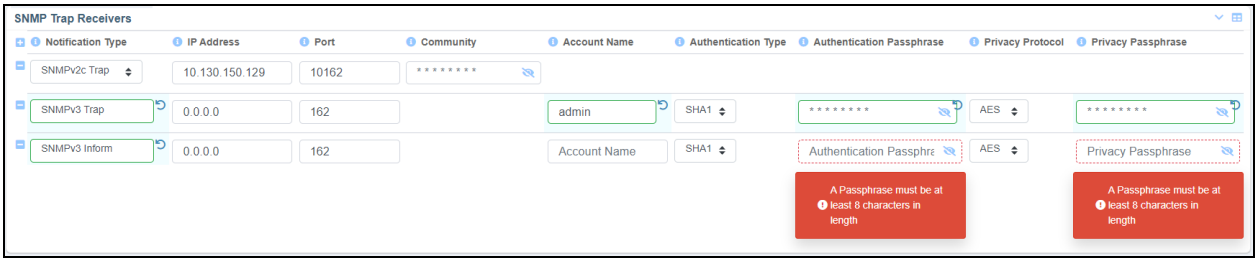
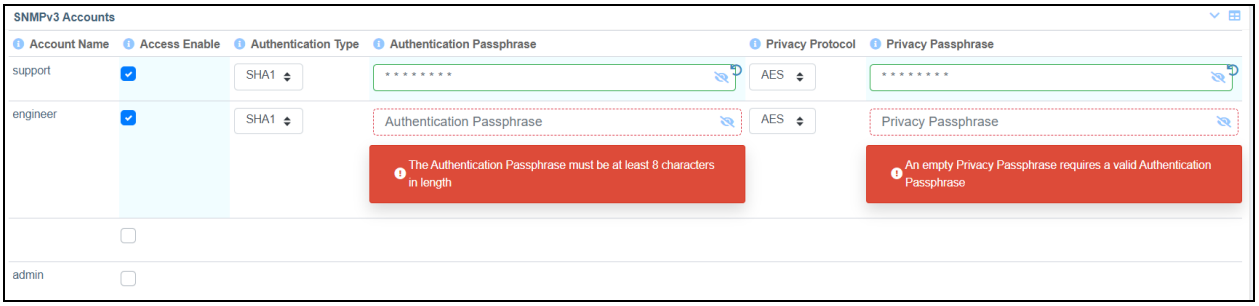


Figure 16 is an example of configuring the **User Accounts** section in the **Management** page.

Figure 16: *The User Accounts section settings*



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

Radio

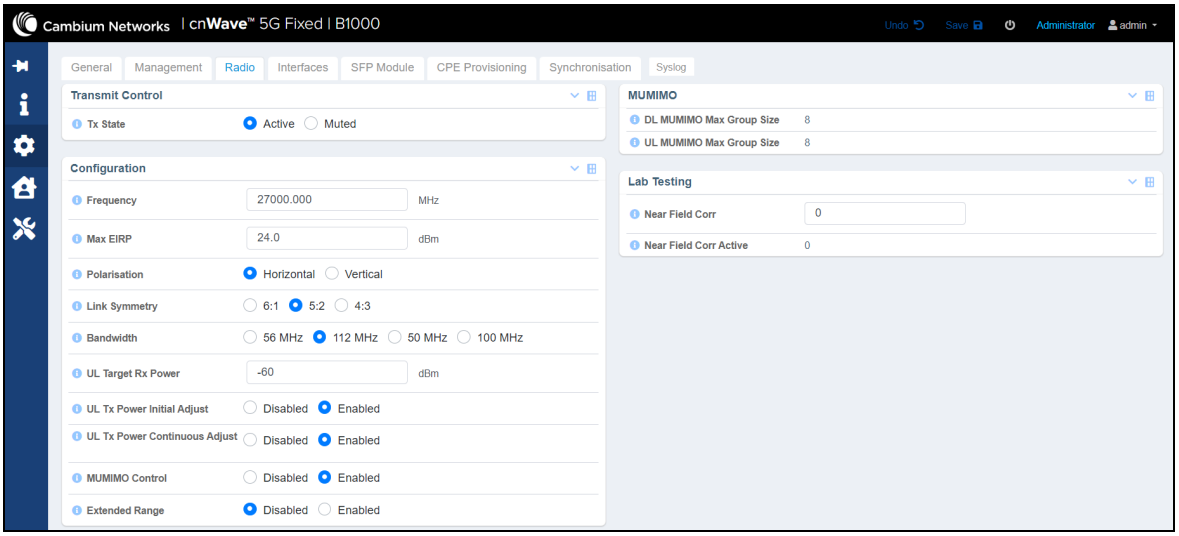
The Radio page allows you to configure transmit control and other radio settings. You can also enable or disable Multi-user Multiple Input Multiple Output (MU-MIMO) and Extended Range parameters.

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 17.

   Figure 17: *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	Determines whether the transmitter is active or muted on the BTS. This parameter supports the following options: • Active • Muted 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. Select the required option.
Configuration	
Frequency	The operating frequency (in MHz) of the radio bearer.

Parameter	Description
	Type an appropriate value in the text box. **Note**: Ensure that the value must be greater than or equal to 24250.000 MHz (or 24.25 GHz).
Max EIRP	The maximum Effective Isotropic Radiated Power (EIRP) value in milliwatts (dBm). This depends on the regulatory conditions of the country of operation. Type an appropriate value in the text box. **Note**: Ensure that the value is greater than 20 or equal to 48.
Polarisation	Determines the antenna polarisation settings. This parameter supports the following polarisation settings: • Horizontal • Vertical Select the required polarisation for the antenna. 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. **Note**: When you change the value of this parameter, the connected CPEs get disconnected and prompts you to reboot the system.
Link Symmetry	The downlink (DL) or uplink (UL) ratio (symmetry) used for controlling the usage of signal slots. BTS and CPE exchange data with each other by using the defined link symmetry. This parameter supports the following options: • 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 Select the required symmetry option. **Note**: When you change the value of this parameter, the **Enable Reboot** parameter appears.

Parameter	Description
Bandwidth	Indicates the bandwidth (in MHz) of the radio channel spacing. Set the required bandwidth value. This parameter supports the following values. • 50 MHz • 56 MHz • 100 MHz • 112 MHz Select the required bandwidth value. **Note**: When you change the value of this parameter, the connected CPEs get disconnected and prompts you to reboot the system.
UL Target Rx Power	The UL target receive power in dBm. Type an appropriate value in the text box. This parameter supports values between -120 and 0. Typically, the best value for this parameter is -50.
UL Tx Power Initial Adjust	Determines the initial power adjust mode of CPEs. This parameter supports the following modes: • Disabled • Enabled Select the required mode. **Note**: In case of first installation, it is recommended to select **Enabled**.
UL Tx Power Continuous Adjust	Determines the continuous power adjust mode of CPEs. This parameter supports the following modes: • Disabled • Enabled Select the required mode. **Note**: It is recommended to set to **Enabled**.
MUMIMO Control	Determines the multi user-multiple input and multiple output (MU-MIMO) control mode of CPEs. This parameter supports the following modes: • Disabled

Parameter	Description
	• Enabled Select the required mode. **Note**: When you enable this parameter, the B1000 UI provides DL utilisation during the MUMIMO operation.
Extended Range	Determines whether the maximum distance range between a CPE and the BTS is extended up to 10 Km. This parameter supports the following options: • 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. Select the required option.
Enable Reboot	An option to reboot the system when you change polarisation, bandwidth, and link symmetry parameters. Select the checkbox to enable the system reboot. 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

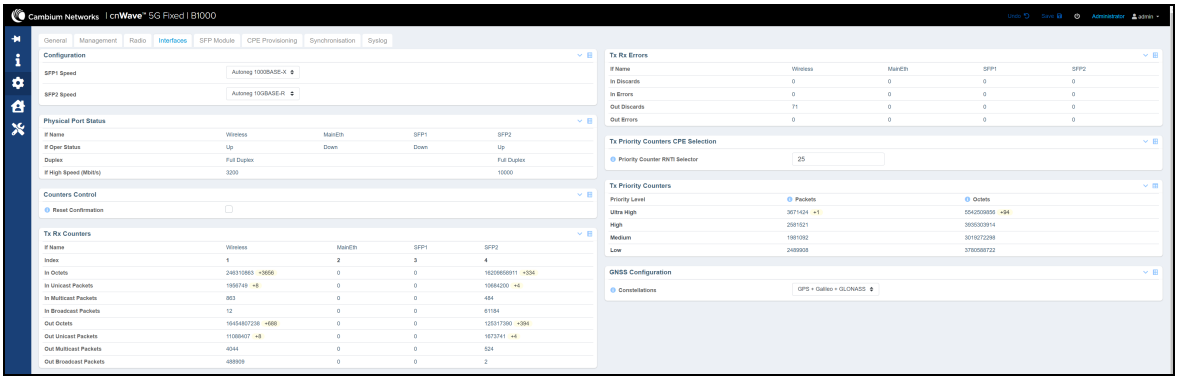
The **Interfaces** page provides statistical information on all the BTS interfaces (for example, Copper or RJ45 MAIN, Small form-factor pluggable (SFP), Global Positioning System (GPS), Power ports, and Tx priority counters). The page also allows you to configure GNSS.

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 18.

   Figure 18: *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	Data speed (10 Gbps) of the optical fiber port1. The following options are supported: • Autoneg 1000BASE-X • Forced 1000BASE-X • Autoneg 10GBASE-R Select the required option from the drop-down list. **Note**: The auto negotiated (Autoneg) option is recommended for both 1000BASE-X and 10GBASE-R. The **Forced 1000BASE-X** option should be used only if it is specifically recommended by Cambium Networks.
SFP2 Speed	Data speed (10 Gbps) of the optical fiber port2. The following options are supported:

Parameter	Description
	• Autoneg 1000BASE-X • Forced 1000BASE-X • Autoneg 10GBASE-R Select the required option from the drop-down list. **Note**: The auto negotiated (Autoneg) option is recommended for both 1000BASE-X and 10GBASE-R. The **Forced 1000BASE-X** option should be used only if it is specifically recommended by Cambium Networks.
Physical Port Status	
If Oper Status	Indicates the working status (up or down) of wireless, Main Ethernet, or fiber ports for BTS.
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 checkbox if you want to reset. **Note**: When you select the checkbox, the **Reset Counters** button is available. You can use this button to reset the SNMP MIB-II interface counters.
Tx Rx Counters - Applicable to all data ports and wireless. The data report is listed in the following columns: • **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.

Parameter	Description
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.
Tx Rx Errors - Applicable to all data ports and wireless. The data report is listed in columns, as described in Tx Rx Counters.	
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.
Out Errors	Number of outgoing data packets (from BTS) that contain errors.
Tx Priority Counters CPE Selection	
Priority Counter RNTI Selector	The index of the bearer for which the per-priority Transmit counters are displayed.
Tx Priority Counters	
Priority Level	Displays the priority level of the bearer relevant to each Transmit counter. This parameter displays the following priority levels: • Ultra High • High • Medium • Low You can view the number of packets and octets transmitted at each priority level.
Packets	Number of packets successfully delivered to the far end of the link based on priority.
Octets	Number of Octets successfully delivered to the far end of the link based on priority.
GNSS Configuration	

Parameter	Description
Constellations	An option to choose a suitable combination of GNSS satellite constellation for the location of this device. Several combinations of GNSS satellite constellations can be used. Select the required combination from the drop-down list. **Note**: You can monitor the satellites using the **GNSS** tab on the B1000 dashboard page. For more information, refer to the GNSS section.
The following parameters specific to GNSS configuration are visible only to engineers who log in to the B1000 UI with an engineer user role: • 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.

QoS

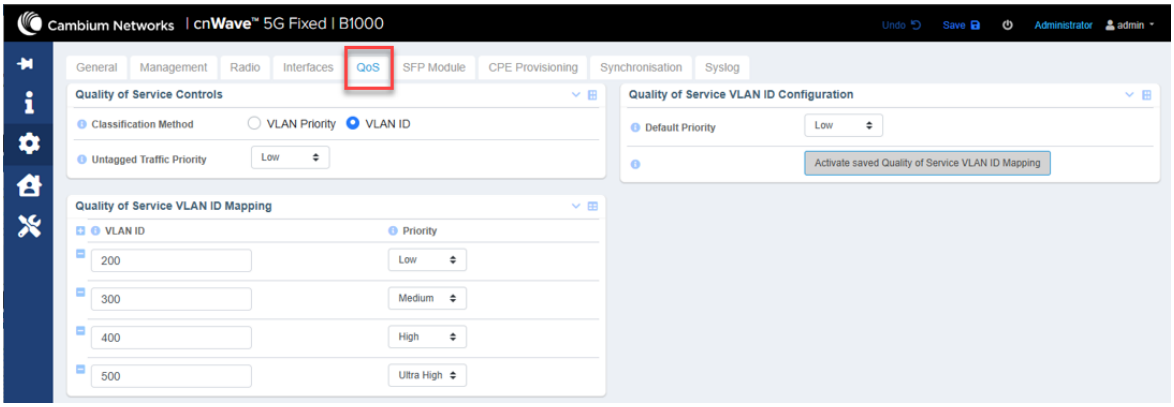
The **QoS** page allows you to configure Quality of Service (QoS) settings for the BTS device.

To view the QoS settings, perform the following steps:

1. From the main B100 dashboard page, navigate to **System** > **QoS.**

   The QoS page appears as shown in Figure 19.

   Figure 19: *The QoS page*



2. View or configure the **QoS Classification** settings.

Table 12 lists and describes each parameter on the **QoS** page.

Table 12: List of parameters in QoS page

Parameter	Description
Quality of Services Controls	
Classification Method	This controls which field within the VLAN header is used to perform the packet classification. The following options are supported: • VLAN Priority • VLAN ID If **VLAN Priority** is selected, the packets transmitted over-the-air by the BTS are classified using the 3-bit **Priority** field of the VLAN ID, with the mapping from the Priority bit to the priority within the B1000 being as follows: • 0 or 1 -> Low Priority • 2 or 3 -> Medium Priority • 4 or 5 -> High Priority • 6 or 7 -> Very High Priority If **VLAN ID** is selected, the packets transmitted over the air by the BTS are classified using the VLAN ID to the Priority level as defined below by the **Quality of Service VLAN ID Mapping**.
Untagged Traffic Priority	This controls which priority the BTS must assign to untagged traffic. The following options are supported: • Low • Medium • High • Very High
Quality of Services VLAN ID Mapping	
VLAN ID and Priority	This section is only visible and relevant if the **Classification Method** above is set to “VLAN ID”. This is a dynamic table that defines which priority to assign to a VLAN packet based on its VLAN ID. Up to 32 entries can be specified. For each entry, a VLAN ID value between 1 and 4095 must be specified and a priority level of Low, Medium, High, and Very High must be selected for that VLAN ID.

Parameter	Description
Quality of Services VLAN ID Configuration	
Default Priority	This section is only visible and relevant if the **Classification Method** above is set to **VLAN ID**. This controls what level of priority must be assigned to VLAN packets for which the VLAN ID could not be matched in the list provided in the **VLAN ID** and **Priority** section above. The following options are supported: • Low • Medium • High • Very High
Activate saved Quality of Service VLAN ID Mapping	This button is only visible and relevant if the **Classification Method** above is set to **VLAN ID**. It activates the Quality of Service VLAN ID Mapping entered in the section above. Please remember to click this button once you have made changes to the **VLAN ID and Priority** or **Default Priority** above.

SFP Module

The **SFP Module** page provides information about the Small Form-Factor Pluggable (SFP) module used for the BTS device. This SFP module information helps you to monitor performance, analyze speed efficiency, and read other network related settings.

To view the SFP module information, perform the following steps:

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

   The SFP Module page appears, as shown in Figure 20.

Figure 20: *The SFP Module page*

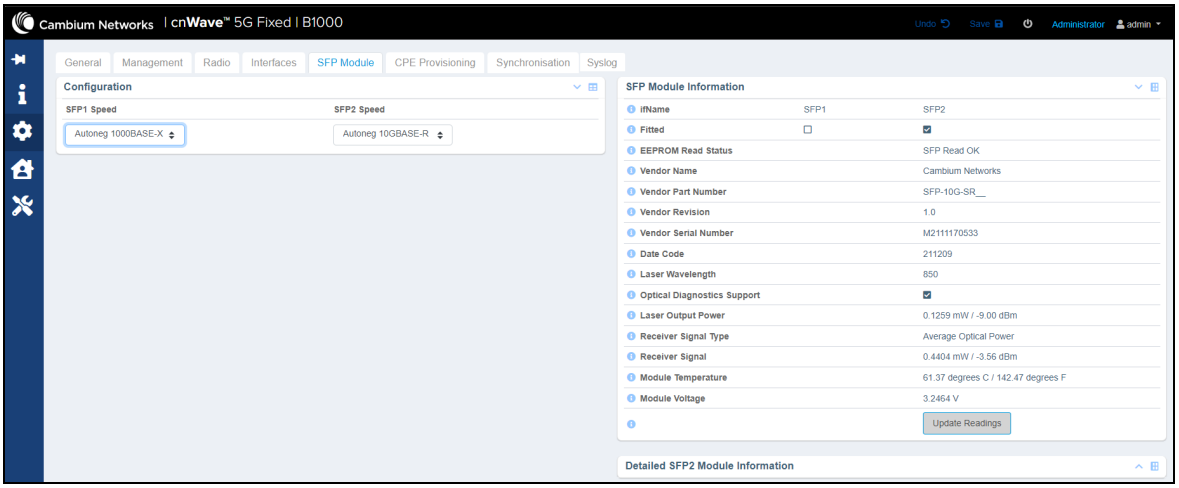


Table 13 lists and describes the parameters on the **SFP Module** page.

Table 13: List of parameters in the SFP Module page

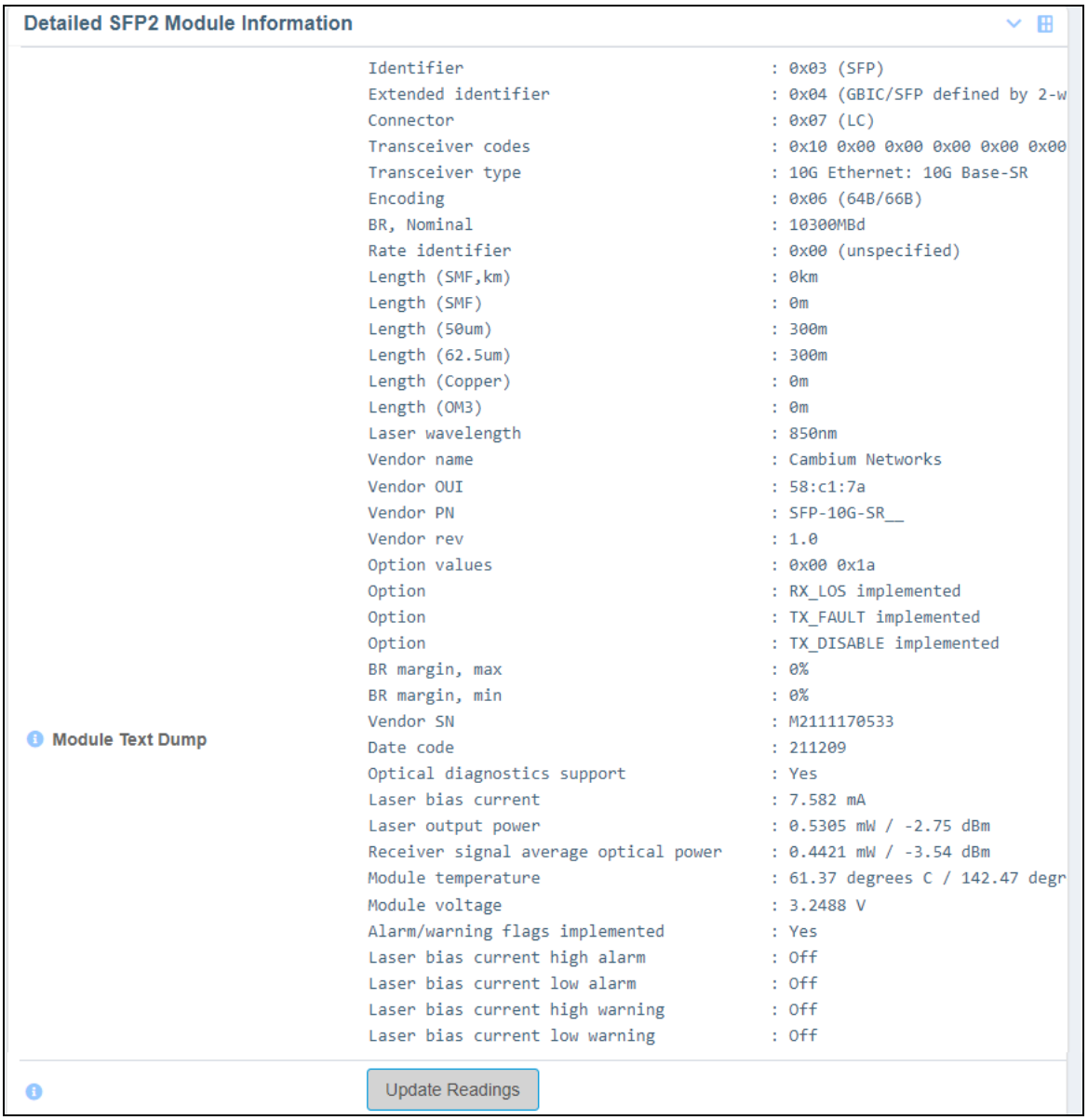
Parameter	Description
Configuration	
SFP1 Speed	Data speed (10 Gbps) of the optical fiber port1. The following options are supported: • Autoneg 1000BASE-X • Forced 1000BASE-X • Autoneg 10GBASE-R Select the required option from the drop-down list. When you modify the value of this parameter, the changes are not applicable until the device is rebooted. **Note**: The auto negotiated (Autoneg) option is recommended for both 1000BASE-X and 10GBASE-R. The **Forced 1000BASE-X** option should be used only if it is specifically recommended by Cambium Networks.
SFP2 Speed	Data speed (10 Gbps) of the optical fiber port2. The following options are supported: • Autoneg 1000BASE-X • Forced 1000BASE-X • Autoneg 10GBASE-R Select the required option from the drop-down list.

Parameter	Description
	When you modify the value of this parameter, the changes are not applicable until the device is rebooted. **Note**: The auto negotiated (Autoneg) option is recommended for both 1000BASE-X and 10GBASE-R. The **Forced 1000BASE-X** option should be used only if it is specifically recommended by Cambium Networks.
SFP Module Information	
IfName	Name of the SNMP MIB2 fixTable corresponding to this SFP module (SFP1 or SFP2) columns.
Fitted	Indicates whether the SFP1 or SFP2 module was fitted and detected at the boot time.
EEPROM Read Status	Indicates the status of reading the SFP EEPROM.
Vendor Name	The vendor's name read from the SFP module.
Vendor Port Number	The vendor port number read from the SFP module.
Vendor Revision	The vendor revision number read from the SFP module.
Vendor Serial Number	The vendor serial number read from the SFP module.
Date Code	The date code read from the SFP module.
Laser Wavelength	The laser wavelength (in mm) read from the SFP module.
Optical Diagnostics Support	Indicates whether the installed SFP module supports optical diagnostics.
Laser Output Power	The laser output power read from that SFP module. This parameter displays the value in both mW and dBm.
Receiver Signal Type	The Receiver signal type read from the SFP module. This parameter displays the value as OMA or Average Optical Power.
Receiver Signal	The Receiver signal read from the SFP module. This parameter displays the value in both mW and dBm.
Module Temperature	The module temperature read from the SFP module. This parameter displays the value in both degrees C and degrees F.
Module Voltage	The module voltage read from the SFP module.
Update Readings	An option to trigger a re-read of the EEPROM for the SFP module. When you click the Update Readings button, the dynamic readings are updated.

2. To view the detailed SFP2 module information, click the ^ icon in the **Detailed SFP2 Module Information** section.

   The Detailed SFP2 Module Information section displays the **Module Text Dump** parameter with detailed readings. This parameter displays a text dump of all the settings read from the SFP module (as shown in Figure 21). The output format is dependent on the features implemented by the SFP module.

   Figure 21: *An example of the Module Text Dump output*



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.

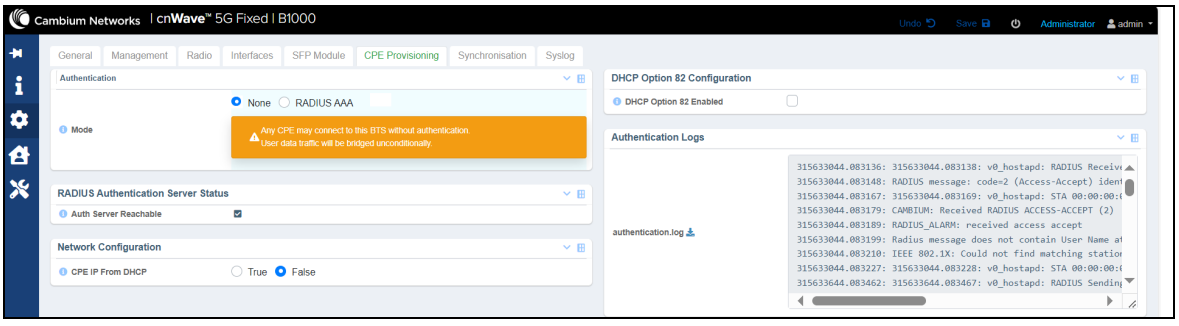
  - Remote ID: Used for identifying the remote device that sends the DHCP request.

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 22 (if RADIUS AAA settings are not set).

   Figure 22: *The CPE Provisioning page with no RADIUS AAA settings*



2. Set the required parameter, as described in Table 14.

Table 14: List of parameters in the CPE Provisioning page

Parameter	Description
Authentication	
Mode	Determines the connection mode of CPEs. This parameter supports the following options: • 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. Choose the required mode. You can use to revert to **None** from the **RADIUS AAA** mode.
RADIUS Authentication Server Status	
Auth Server Reachable	This is a read-only parameter. Indicates whether at least one of the configured authentication servers is currently reachable. The authentication servers are polled every 10 minutes to update this status.
Network Configuration	
CPE IP From DHCP	Determines whether the CPE IP network configuration is supplied by a DHCP server. The following values are supported: • True: When enabled, the CPE IP network configuration is supplied by a DHCP server. • False: When disabled and if the Authentication Mode is **RADIUS AAA**, the CPE IP network configuration is supplied by the configured RADIUS server. When disabled and if the Authentication Mode is **None**, the CPE IP network configuration is set locally at each CPE. Select the required option.
CPE Use Local VLAN Config	Determines whether the CPE uses the local VLAN configuration or the RADIUS-supplied VLAN settings. This parameter is applicable only when you choose RADIUS AAA as the authentication mode.

Parameter	Description
	The following options are supported: • 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**. Select the required option.
CPE Use Local QoS Config	Determines whether the CPE uses the local QoS configuration or the RADIUS-supplied QoS settings. This parameter is applicable only when you choose RADIUS AAA as the authentication mode. The following options are supported: • 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**. Select the required option.
DHCP Option 82 Configuration	
DHCP Option 82 Enabled	Determines whether the DHCP Option 82 feature is enabled. 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. Select the checkbox if you want to enable this feature. **Note**: When you enable the DHCP Option 82 parameter, the following Option 82- specific fields appear (as shown in Figure 23): • Circuit ID • Remote ID
Circuit ID	The circuit ID used for identifying the circuit (for example, interface or VLAN) on the node on which the request is received.

Parameter	Description
	When the **DHCP Option 82 Enabled** parameter is enabled, the system inserts this Circuit ID into the packet header. Default value: `$btsMAC$` **Note**: Use the following wildcards to configure **Circuit ID** and **Remote ID** fields: • `$btsMAC$`: 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. 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 `$` character.
Remote ID	The remote ID used for identifying the remote device that sends the DHCP request. When the **DHCP Option 82 Enabled** parameter is enabled, the system inserts this Remote ID tino the packet header. Default value: `$cpeMAC$` For information about the supported wildcards, check the Circuit ID field description. **Note**: You can combine multiple wildcards. The total length of the option (after replacing wildcards with corresponding values) must not exceed 255 characters. You can also configure a custom string, which **must not** start with a `$` character.
DHCP Option 82 Statistics	Displays the count of DHCP Option 82-specific requests and replies that are received, discarded, and relayed, including other message discards. This section appears only when you select the **DHCP Option 82 Enabled** checkbox. This section displays the following statistics:

Parameter	Description
	• **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	An option to view and download the authentication logs from the UI. Click the icon to download the authentication logs.
The following parameters appear only when you select the **RADIUS AAA** mode (as shown in Figure 24):	
RADIUS Configuration	
Accounting	Used for billing purposes. 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 24).

Parameter	Description
	You must set these RADIUS accounting-specific parameters with appropriate values by configuring with at least one primary accounting server (as shown in Figure 24).
RADIUS Accounting Server - This section appears only when you select the **Accounting** checkbox.	
Role	An option to designate one RADIUS server as primary and the others (if required) as secondary accounting servers. This parameter supports the following options: • Primary • Secondary • None Select the required option from the drop-down list. **Note**: Ensure that at least one primary accounting server is configured (as shown in Figure 24).
Inet Address	The IP address assigned to the server that performs RADIUS accounting. Type an appropriate value in the text box.
Port	The network port assigned to the server that performs RADIUS accounting. Default value: 1813
Secret	The shared secret that is used to authenticate transactions between the BTS device and the RADIUS accounting server. Provide an appropriate value in the text box.
RADIUS Authentication Server	
Role	An option to designate one RADIUS server as primary and the others (if required) as secondary authentication servers. This parameter supports the following options: • Primary • Secondary • None Select the required value from the drop-down lists.
Inet Address	The IPv4 address of the RADIUS server used for identifying in standard dot notion. Type an appropriate value in the text box.

Parameter	Description
Port	The destination port used by the device for RADIUS communication, authorization, and configuration. Default value: 1812
Secret	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. The shared secret(s) must match those shared secret(s) configured in the RADIUS server(s) `clients.conf` file. For more information about the `clients.conf` file settings, refer to An example of configuring an Authentication Server. Provide an appropriate value in the text box.

Figure 23 shows the parameters specific to the DHCP Option 82 configuration.

Figure 23: *DHCP Option 82 configuration and statistics*

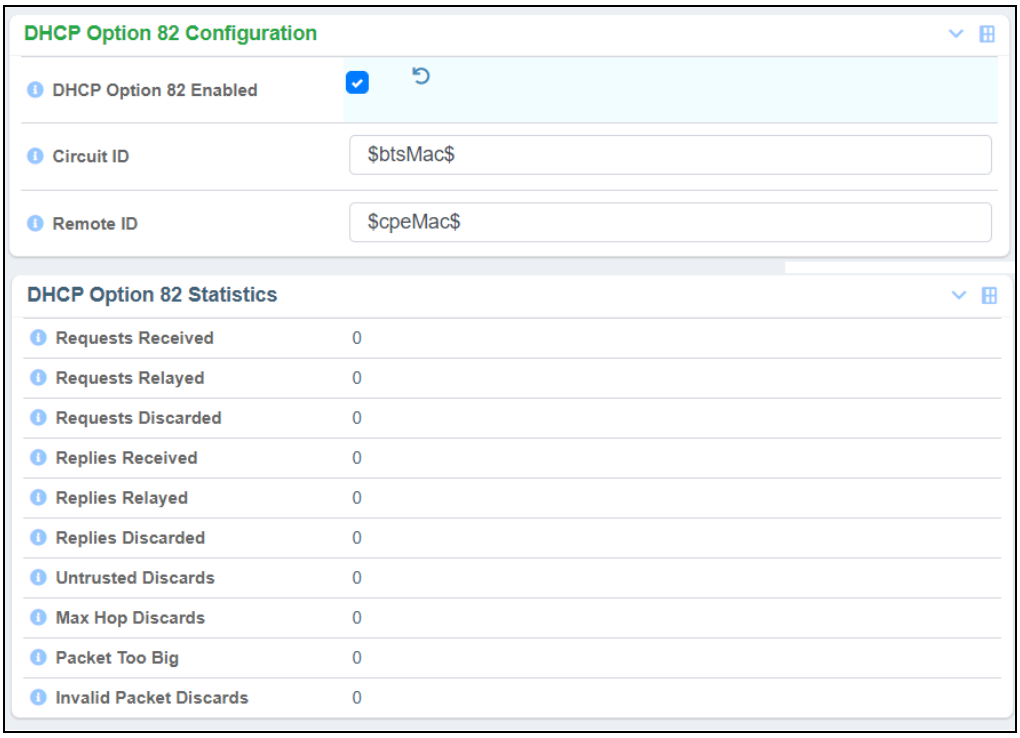
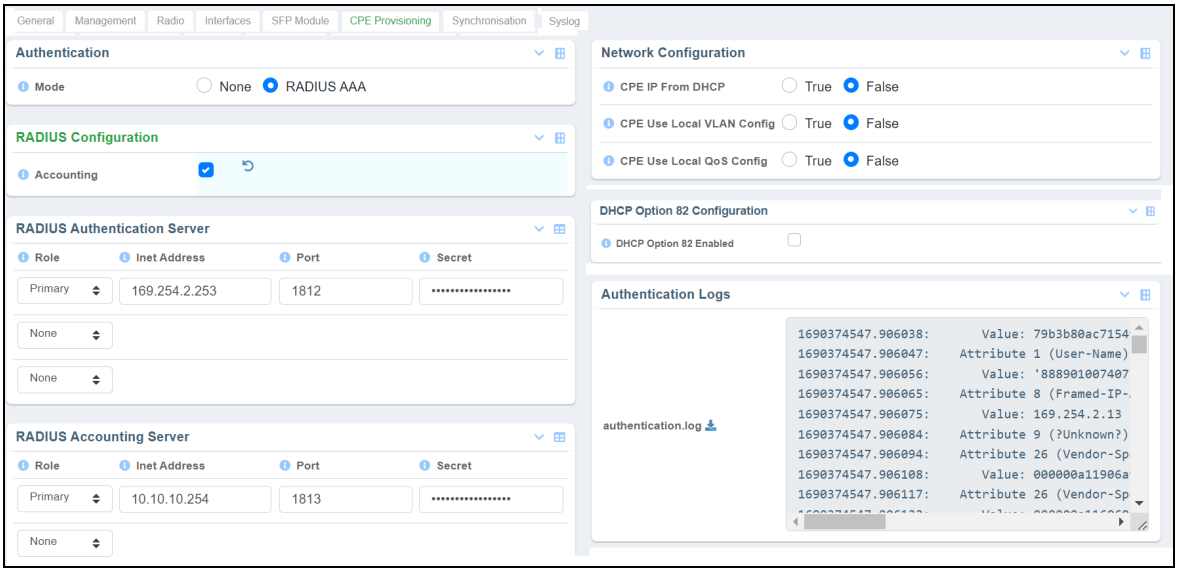


Figure 24 is an example of the **CPE Provisioning** page when the CPE connection mode is set to RADIUS AAA.

Figure 24: *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).

The 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/`

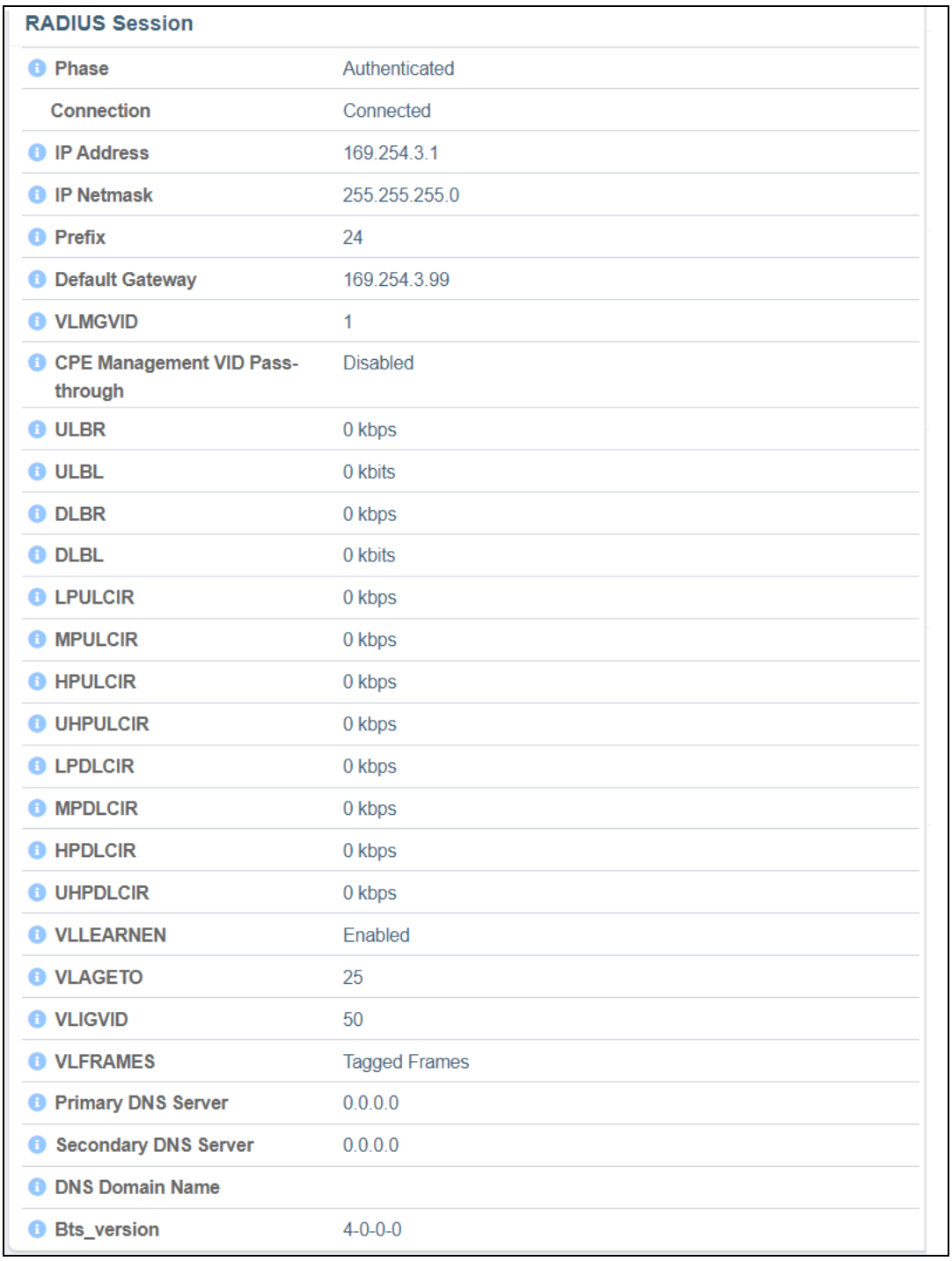
Figure 25 is a screenshot of a section taken from an authorize file for a CPE with an IMSI - 208920007405736.

Figure 25: *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 26 shows various fields that indicate how the CPE uses RADIUS authentication to communicate with BTS.

Figure 26: *RADIUS authentication details in the C100 (CPE) dashboard*



Details of RADIUS authentication-specific parameters (as shown in Figure 26) are described in Table 36 (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.

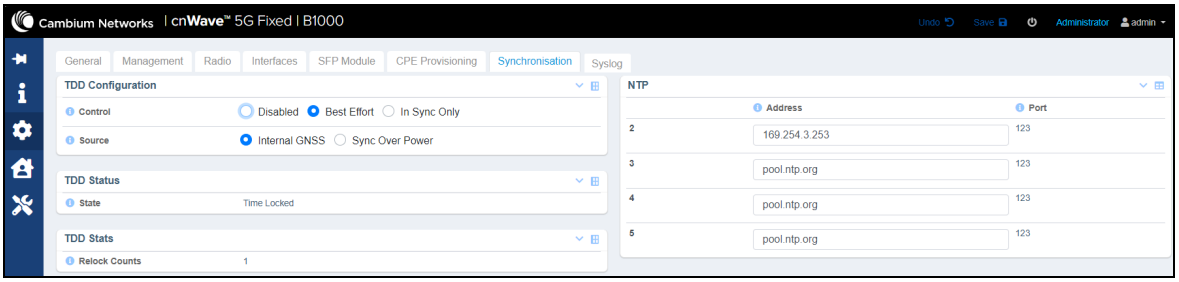
For more information about the TDD Synchronization and how to check the BTS installation using satellite details, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

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 27.

   Figure 27: *The Synchronisation page*



2. Set the value of each parameter, as described in Table 15.

   Table 15: List of parameters in the Synchronisation page

Parameter	Description
TDD Configuration	
Control	Determines the use of internal or external reference signal for TDD synchronisation. This parameter supports the following options: • 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. 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. **Note**: When you select Best effort or In Sync only, the icon appears indicating to select the Disabled option.

Parameter	Description
Source	The sync source for TDD. This parameter supports the following options: • 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. Select the required option. **Note**: When you select **Sync Over Power**, the  icon appears indicating to select the **Internal GNSS** option.
TDD Status	
State	Indicates the state of TDD synchronisation process, which is reported by TDD Sync state. The BTS device can be synchronised to a one PPS source. The synchronisation process involves detecting a valid one PPS reference signal, acquiring frequency lock, and then acquiring and maintaining time lock. When a PPS is detected, the frequency is locked and the TDD is synchronized (which is indicated by the **Time Locked** state). **Note**: The **Local** state indicates that the local reference is used, and no PPS input is detected.
TDD Stats	
Relock counts	Indicates the number of times the TDD Sync has entered the locked condition.
NTP - Stands for Network Time Protocol (NTP). 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.	
Address	IP address of the NTP server or a Domain Name System (DNS) name (using which the device is configured to use DNS). Enter the required addresses or DNS names of the system in the text boxes.
Port	The network port number that is assigned to the NTP server. **Note**: The 0 value is not valid.

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

Syslog

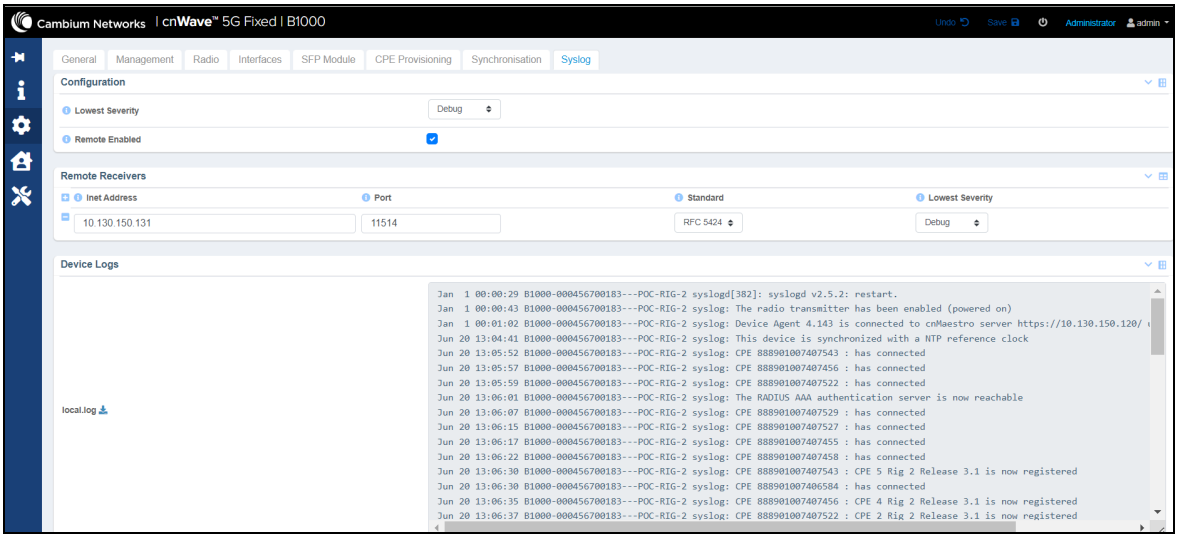
The **Syslog** page allows you to allocate the lowest syslog severity level and enable the remote syslog specific parameters for the BTS device. The syslog configuration helps you to record and view all events of the BTS device. Example: CPE connected or BTS connected to cnMaestro.

To configure and view the **Syslog** page, perform the following steps:

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

   The **Syslog** page appears, as shown in Figure 28.

   Figure 28: *The Syslog page*



2. Set the value of each parameter, as described in Table 16.

   Table 16: List of parameters in the Syslog page

Parameter	Description
Configuration	
Lowest Severity	Allows you to configure the lowest syslog severity that is logged locally on the BTS device. The following syslog severity levels are supported: • Emergency - means system is unusable. • Alert - means action must be taken immediately. • Critical - means critical conditions. • Error - means error conditions. • Warning - means warning conditions. • Notice - means normal but significant conditions.

Parameter	Description
	• Information - means informative messages. • Debug - means debug-level messages. Select the required severity from the drop-down list.
Remote Enabled	When you enable this remote syslog parameter, important system events are sent to the configured remote syslog receivers. Syslog facilities include `syslog`, `auth`, and `local0 thro local7`. When you select the **Remote Enabled** checkbox, the **Remote Receivers** section appears with the following parameters: • Inet Address • Port • Standard • Lowest Severity
Remote Receivers	
Inet Address	IP address that is assigned to the remote syslog receiver. All enabled severity levels of syslog messages are sent to this address. Type an appropriate value in the text box.
Port	The network port that is assigned to the remote syslog receiver. Type a valid value in the text box. **Note**: The zero (0) value is not valid.
Standard	Indicates the syslog message format, which is determined by RFC 3164 and RFC 5424 standards. The following options are supported: • RFC 3164 • RFC 5424 Select the required option from the drop-down list.
Lowest Severity	Allows you to configure the lowest syslog severity message that is sent to the remote syslog receiver. The following syslog severity levels are supported: • Emergency - means system is unusable.

Parameter	Description
	• Alert - means action must be taken immediately. • Critical - means critical conditions. • Error - means error conditions. • Warning - means warning conditions. • Notice - means normal but significant conditions. • Information - means informative messages. • Debug - means debug-level messages. Select the required severity from the drop-down list.

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

   The **Device Logs** section displays the events of the BTS device for the selected severity level. You can view and download the logs (if required) using the icon.

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 29).

Figure 29: *The CPE Status page*

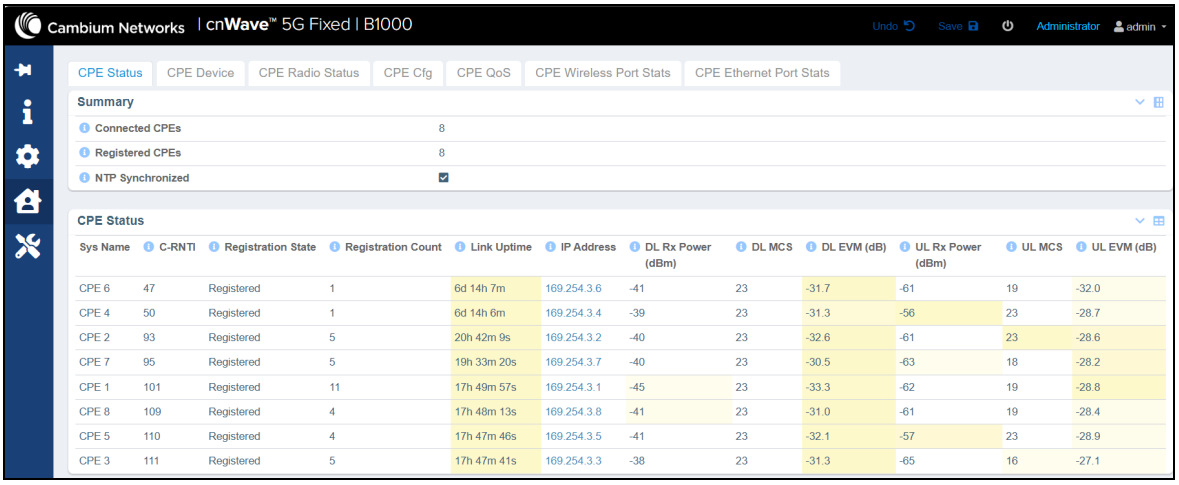


Table 17 lists and describes parameters available on the **CPE Status** page.

Table 17: 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	Stands for Call-Radio Network Temporary Identifier (C-RNTI). Unique ID used for identifying RRC connection and scheduling. Each CPE device is associated with a dedicated C-RNTI. BTS uses the C-RNTI to: • 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.

Parameter	Description
	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. **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. The RNTI is released when a CPE disconnects from the BTS. RNTI uniquely identifies a CPE connected to a given BTS or sector.
Registration State	Indicates whether the CPE has made any progress to enter to the network. This parameter supports the following device transition states: • 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	Number of times that the CPE has successfully registered with BTS. The value of this parameter is reset to 0 when the system starts up.
Link Uptime	Time period (in seconds) at which the last successful registration of the CPE found with BTS.
IP Address	The IP address that is assigned to the network interface. This IP address is used for managing the device.
DL Rx Power (dBm)	The downlink received signal power (in dBm).
DL MCS	The Modulation and Coding Scheme (MCS) index value of the downlink. For more information about MCS, refer to the Modulation section.
DL EVM (dB)	The EVM value (in dB) of the downlink.
UL Rx Power (dBm)	The uplink received signal power (in dBm).
UL MCS	The MCS index value of the uplink. For more information about MCS, refer to the Modulation section.

Parameter	Description
UL EVM (dB)	The EVM value (in dB) of the uplink.
The following parameters are visible only to engineers who log in to the B1000 UI 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

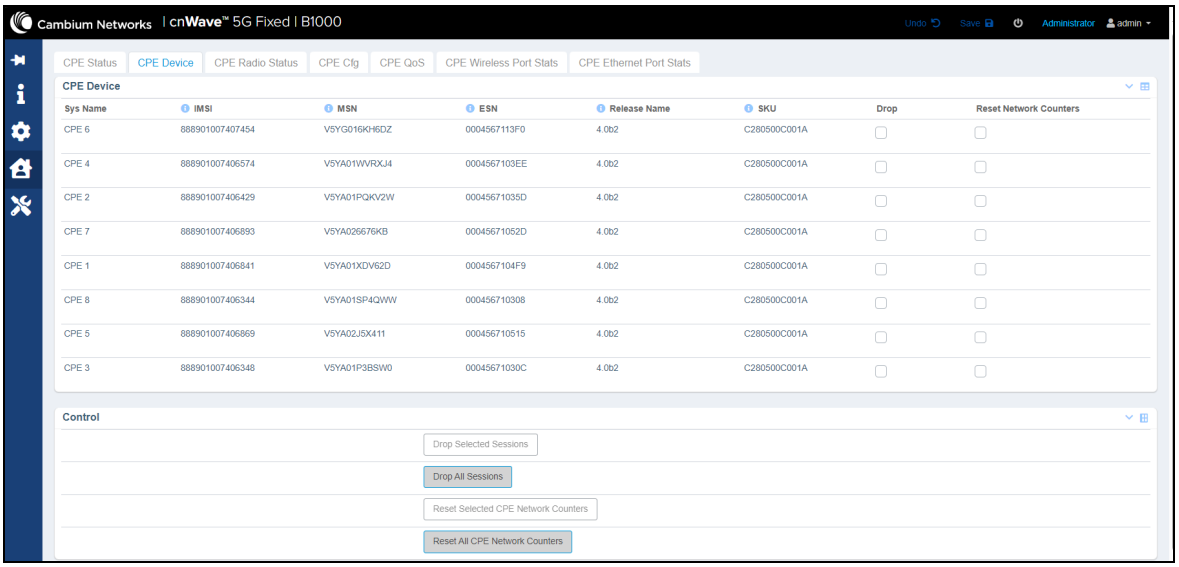
The **CPE Device** page provides information about the hardware device (CPE) that is connected to the BTS.

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 30.

   Figure 30: *The CPE Device page*



2. View the data of CPE device parameters, as described in Table 18.

   Table 18: List of CPE device parameters

Parameter	Description
Sys Name	Name of the CPE system.

Parameter	Description
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 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 checkbox 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 checkbox 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

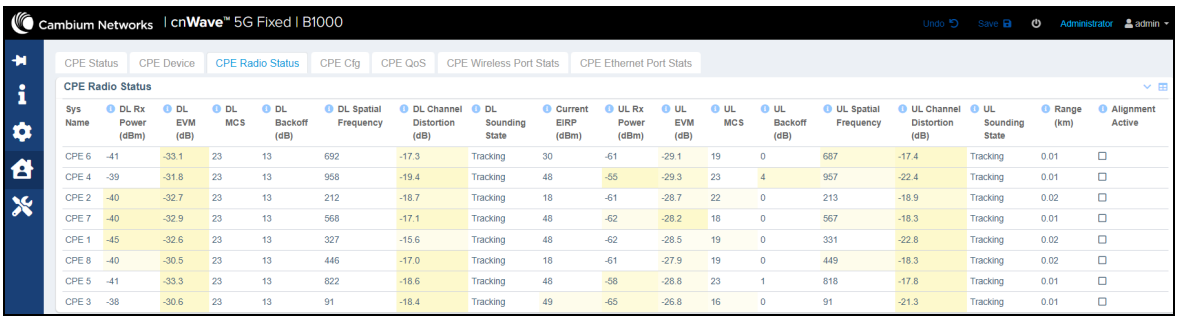
The **CPE Radio Status** page provides information that you can use to troubleshoot any issues with the radio link-related parameters at a deployment site.

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 31.

   Figure 31: *The CPE Radio Status page*



2. View the data of CPE radio parameters, as described in Table 19.

Table 19: 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: • 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).

Parameter	Description
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.
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: • ASSESSING • TRACKING
Range (Km)	Value (in kilometers) that indicates the measured distance between the BTS and the CPE.
Alignment Active	Determines whether the antenna alignment mode is active. This parameter supports the following options: • If the checkbox is selected, then it implies that the antenna alignment mode is active. • If the checkbox 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 Blocker Error Code (BLER).

Table 20 contains aggregate throughputs for each MCS mode and the Line of Sight (LoS)-specific theoretical ranges for the cnWave™ 5G Fixed products.

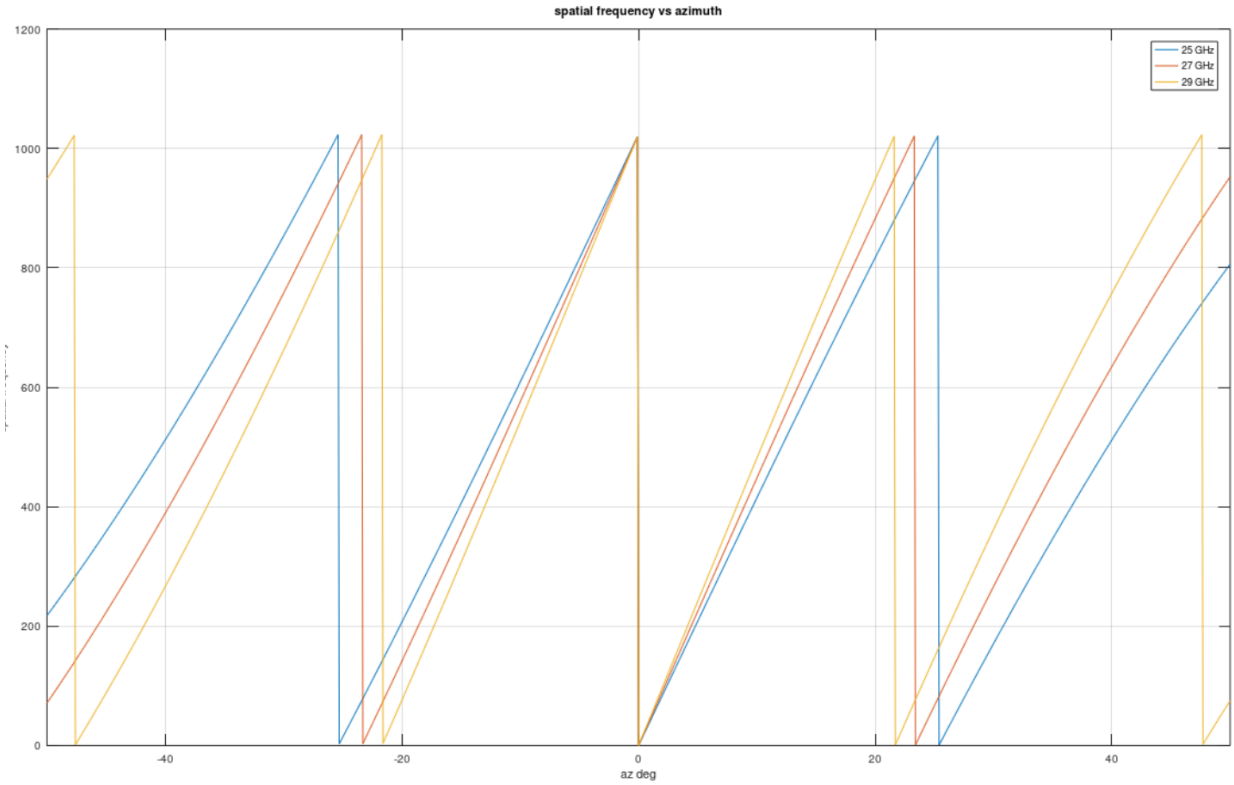
Table 20: MCS Modes and cnWave™ 5G Fixed throughputs

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
MSC 13	230.6	
MCS 12	212.9	106.4
MSC 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 32).

Figure 32: *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 < = Ang < 360 degrees, the spatial frequency is reported as (1024 x Ang/360 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

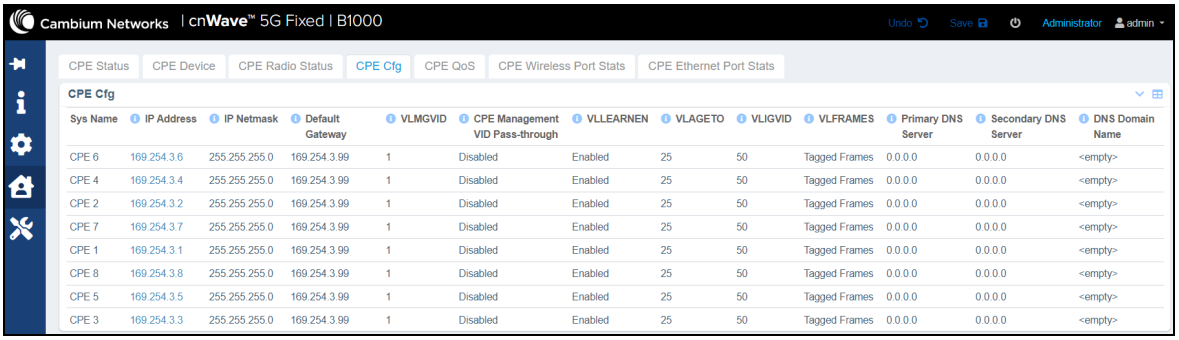
The **CPE Cfg** page provides information about the CPEs names and other network configuration-related data of connected and registered CPEs (subscribers).

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 33.

Figure 33: *The CPE Cfg page*



2. View the configuration data of CPEs, as described in Table 21.

Table 21: 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. This IP address of the default gateway (if any) is used for managing the subscriber data service.
VLMGVID	The 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.
VLLEARNEN	Determines whether the CPE must add the VLAN IDs (VIDs) of upstream frames to the VID table. The parameter supports the following values: • 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.

Parameter	Description
VLAGETO	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).
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
Primary DNS Server	IP address of the primary DNS server assigned by the RADIUS Server (if any).
Secondary DNS Server	IP address of the secondary DNS server assigned by the RADIUS Server (if any).
DNS Domain Name	Name of the DNS domain assigned by the RADIUS Server (if any).

CPE QoS configuration data

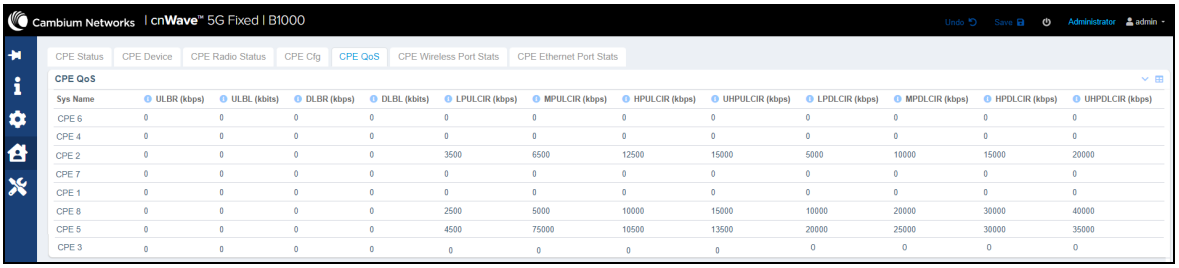
The **CPE QOS** page provides information about uplink and downlink related configuration data used for managing the services of CPEs.

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 34.

   Figure 34: *The CPE QOS page*



2. View the QoS configuration data of CPEs, as described in Table 22.

Table 22: 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 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

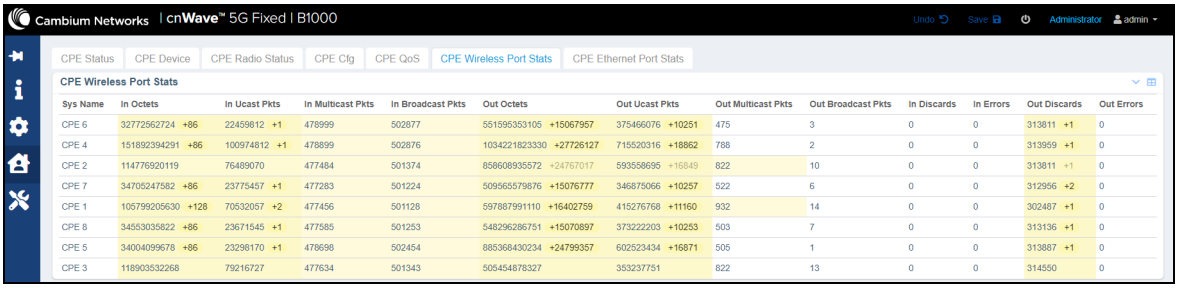
The **CPE Wireless Port Stats** page provides information about statistics of all the data transmitted on the wireless link when it is up.

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 35.

   Figure 35: *The CPE Wireless Port Stats page*



2. View the wireless port statistics for CPEs, as described in Table 23.

   Table 23: 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.

Parameter	Description
Out Discards	Number of outgoing data packets (from the CPE) that are marked or labeled as discarded by the CPE.
Out Errors	Number of outgoing data packets (from the CPE) that contain errors.

CPE Ethernet port statistics

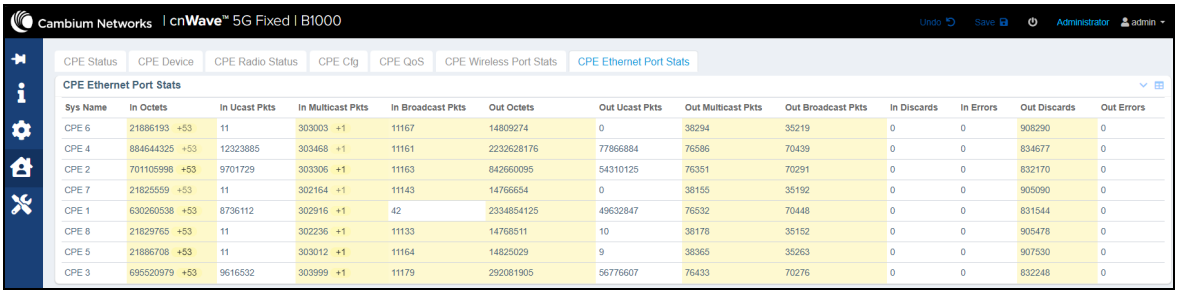
The **CPE Ethernet Port Stats** page provides statistics of the data that is entering the main Ethernet port.

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

1. 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 36.

   Figure 36: *The CPE Ethernet Port Stats page*



2. View the Ethernet port statistics for CPEs, as described in Table 23.

Configuring tools

The **Tools** page in the B1000 UI allows you to upload new firmware (software) or reboot the unit. There are sets 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
- MAC Learning Tables
- Engineering
- Logs

Firmware

The **Firmware** page allows you to upgrade or downgrade software firmware. This page also provides 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 the best results, the CPE software versions in 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 24: Compatibility matrix required for upgrade or downgrade

BTS	CPE							
	3.0	3.1	3.1.1	3.1.2	3.2	3.3	4.0	4.1
3.0	OK	OK	OK	OK	OK	OK	OK	OK
3.1	OK	OK	OK	OK	OK	OK	OK	OK
3.1.1	OK	OK	OK	OK	OK	OK	OK	OK
3.1.2	OK	OK	OK	OK	OK	OK	OK	OK
3.2	OK	OK	OK	OK	OK	OK	OK	OK
3.3	OK	OK	OK	OK	OK	OK	OK	OK
4.0	OK	OK	OK	OK	OK	OK	OK	OK
4.1	OK	OK	OK	OK	OK	OK	OK	OK

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

- Air interface changes due to which 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:
  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:

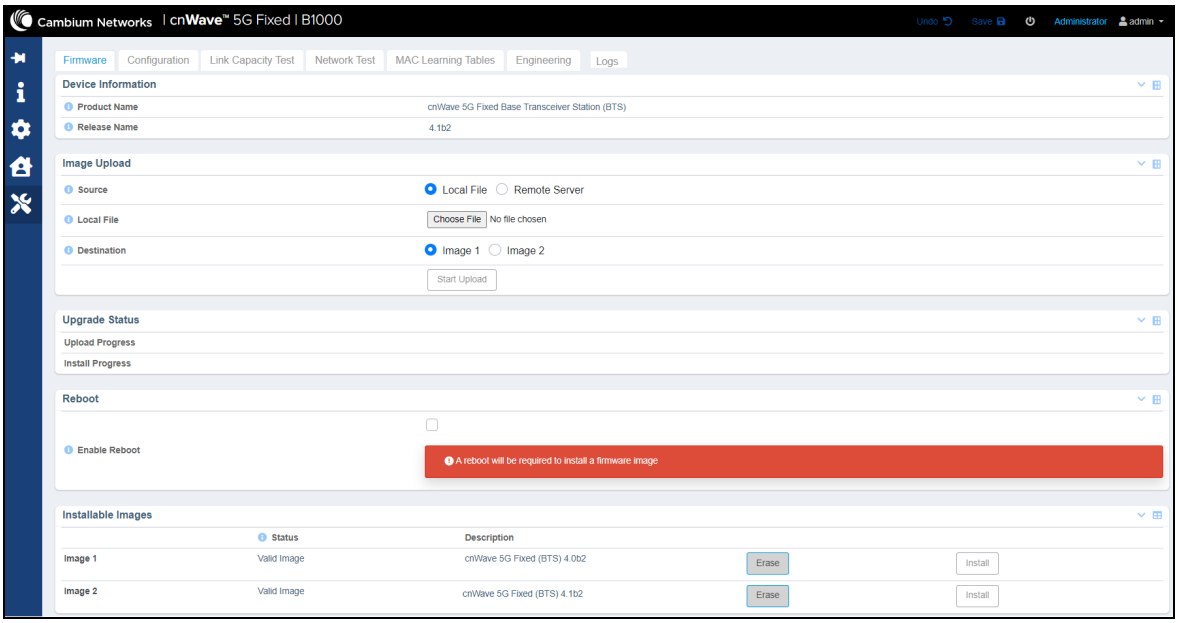
1. Log on to the B1000 UI (as described in the Accessing the B1000 UI section).

   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 37.

   Figure 37: *The Tool page - B1000 UI*



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

3. Set the required parameters, as described in Table 25.

Table 25: 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: • 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. 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.

Parameter	Description
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** checkbox 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: • **Status**: Displays one of the following supported statuses of the image: ◦ **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. To install an image file that you uploaded, click **Install** in the corresponding row of the required image file. To delete an image file that you uploaded, click **Erase** in the corresponding row of the required image file.

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

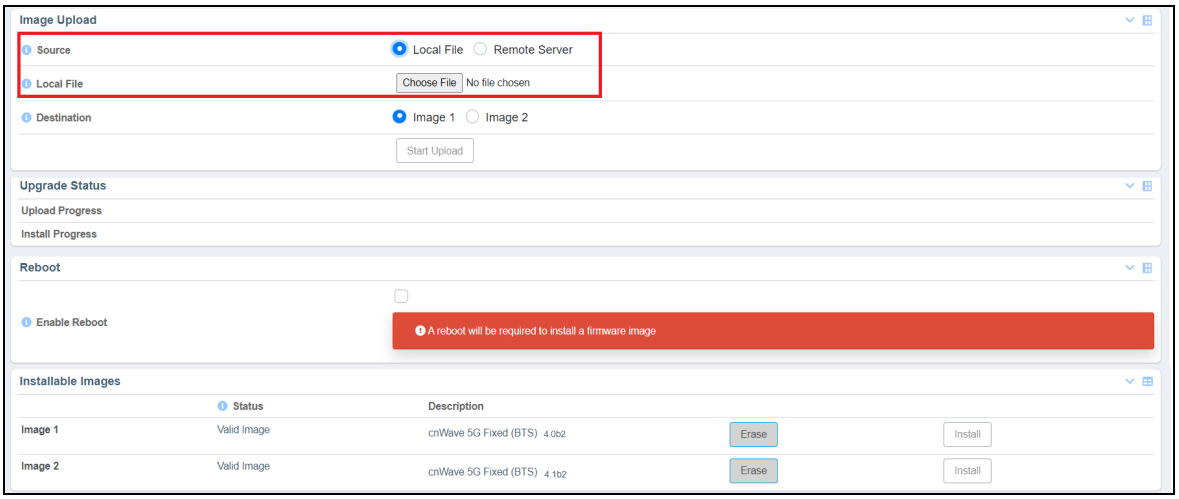
You must first upgrade the BTS software image file. You can follow the same process to upload or upgrade the CPE-specific image file using the **C100 Dashboard** > **Tools** > **Firmware** page.

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 38.

   Figure 38: *The Local File parameter in the Firmware page*



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 38. For more information about each parameter in the **Firmware** page, refer to Table 25.

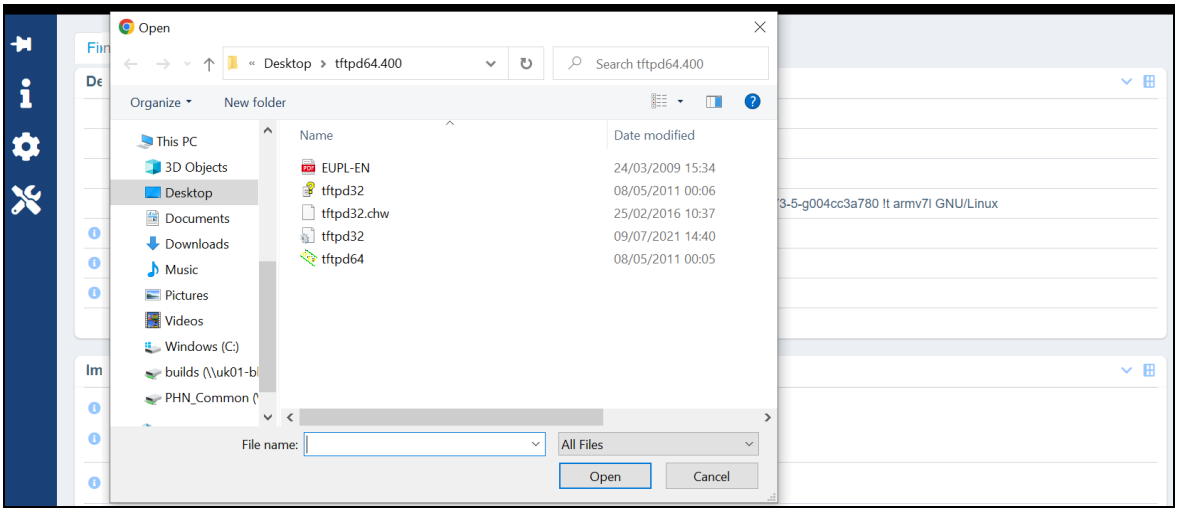
   Note

   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 39.

Figure 39: *A file browser window*

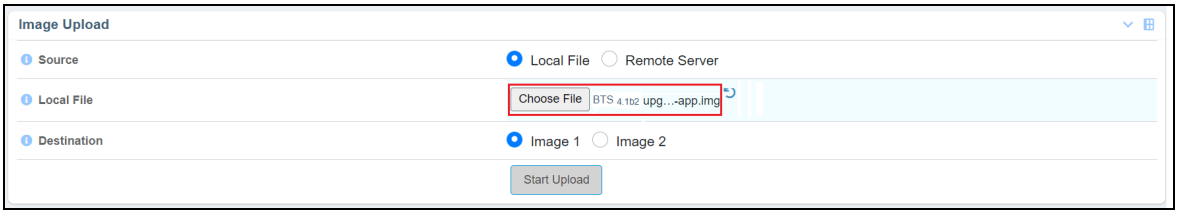


4. Browse the location where you have saved the required firmware image file on your machine, locally.

5. Select the required disc image file (for example, `BTS 4.1b2 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 40.

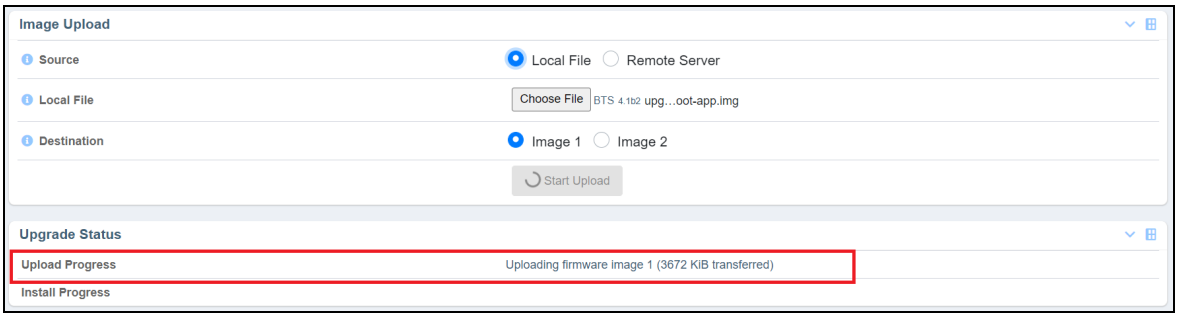
   Figure 40: *The image file name in the Local File field*



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 41.

   Figure 41: *Upload status details in the Upload Progress field*



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

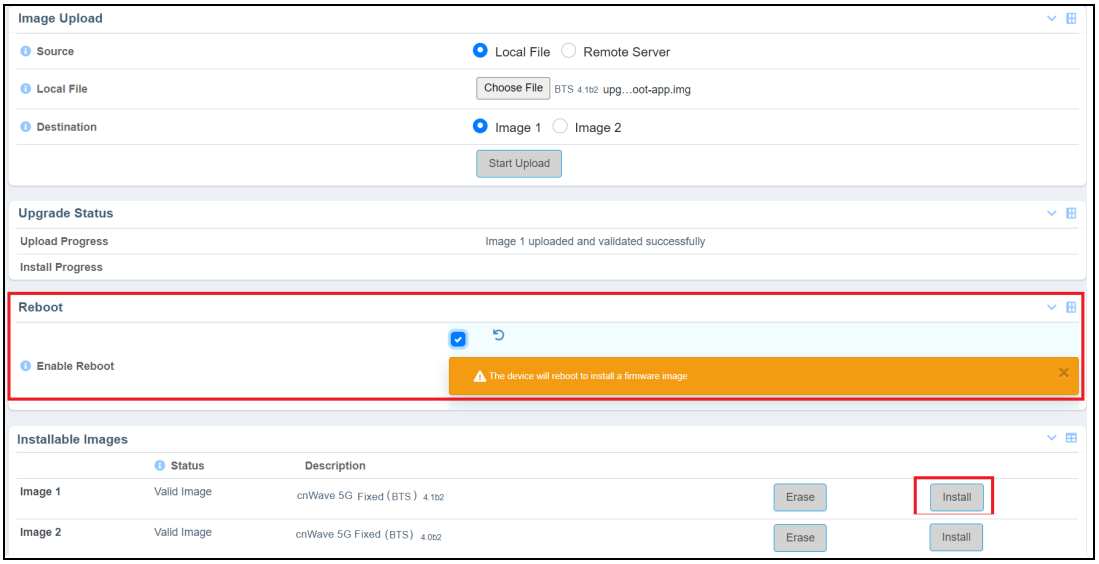
- When you upload a correct image file, a message appears indicating that the image is uploaded and validated successfully (as shown in Figure 42).
- When you upload an incorrect image file, a message appears indicating that the uploaded image is invalid.
- When you delete any image file from the **Installable 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** checkbox in the **Reboot** section, as shown in Figure 42.

   When you enable the reboot option, the **Install** button is enabled in the **Installable Images** section as shown in Figure 42. By default, the **Install** button is disabled.

   Figure 42: *The Enable Reboot and Install options*



   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

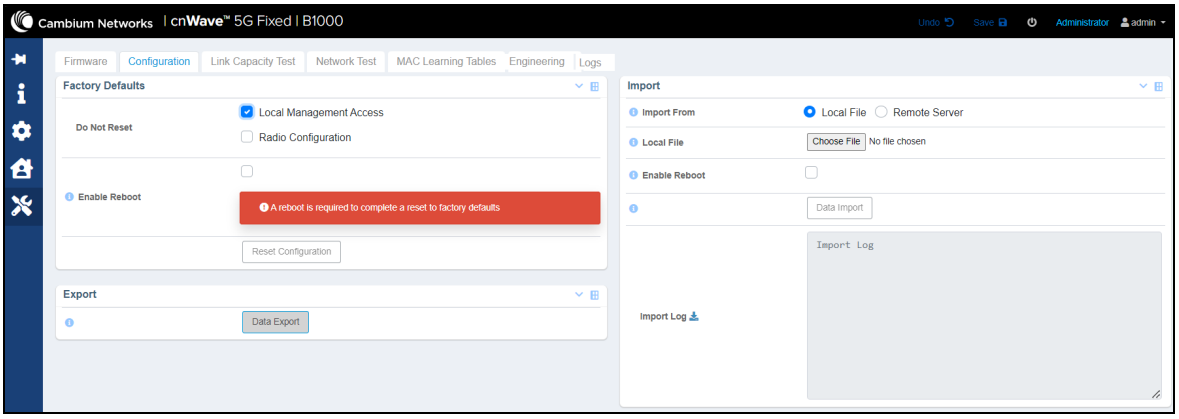
The **Configuration** page allows you to set the BTS to factory defaults. This page also allows you to import a saved configuration or export a BTS configuration for backup (restore). This Import feature exports or imports the date model configuration (and/or status) as a JSON file.

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 43.

   Figure 43: *The Configuration page - B1000 UI*



2. Set the values for parameters, as described in Table 26.

   Table 26: List of parameters in the Configuration page

Parameter	Description
Factory Defaults	
Do not reset	Determines whether you want to reset the device to factory defaults. The following options are supported: • Local Management Access • Radio Configuration By default, the **Local Management Access** checkbox is selected. If you do not select the **Local Management Access** checkbox, then all the configuration data, including IP address, is wiped out and reset to 169.254.1.1. 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. If you select **Radio Configuration**, then all the configuration data is wiped out, except for the frequency data and local IP address.
Enable Reboot	Determines whether the device is enabled to reboot to complete the process of reset to factory defaults. Select the checkbox to enable the reboot for the device.

Parameter	Description
Reset Configuration	An option to reset the system to factory defaults. Click **Reset Configuration** if you want to reset the device to factory defaults.
Export	
Data Export	An option to export the data model configuration (and/or) status as a JSON file for backup (restore). When you click the **Data Export** button, the data model configuration is downloaded by the device.
Import	
Import From	An option to select a location (stored) from where you want to import the required data configuration. This parameter supports the following options: • **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. Select the required option. **Note**: When you select **Remote Server**, the icon appears indicating to select the **Local File** option (if required).
Local File	To upload a local import file (internally), perform the following steps: a. Click **Choose File** in the Local File field. A file browser window appears. b. Browse the location where you have saved the import file (for example, a JSON file) on your machine locally. c. Select the file and click **Open**. The local import file is selected. d. To upload the import file, click **Data Import** in the **Configuration** page.
Server URL	This parameter is applicable only if you have selected **Remote Server** in the **Import From** field. To select the import file from a remote server, provide the server URL in the text box. Then, click the **Data import** button.
Enable Reboot	Determines whether the device is enabled to reboot to complete the import configuration.

Parameter	Description
	Select the checkbox to enable the reboot for the device. When you select the checkbox, a message appears indicating that the device may reboot immediately after the required configuration is imported. **Note**: Only some configuration changes require a reboot.
Data Import	An option to import the required data model configuration from a JSON 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

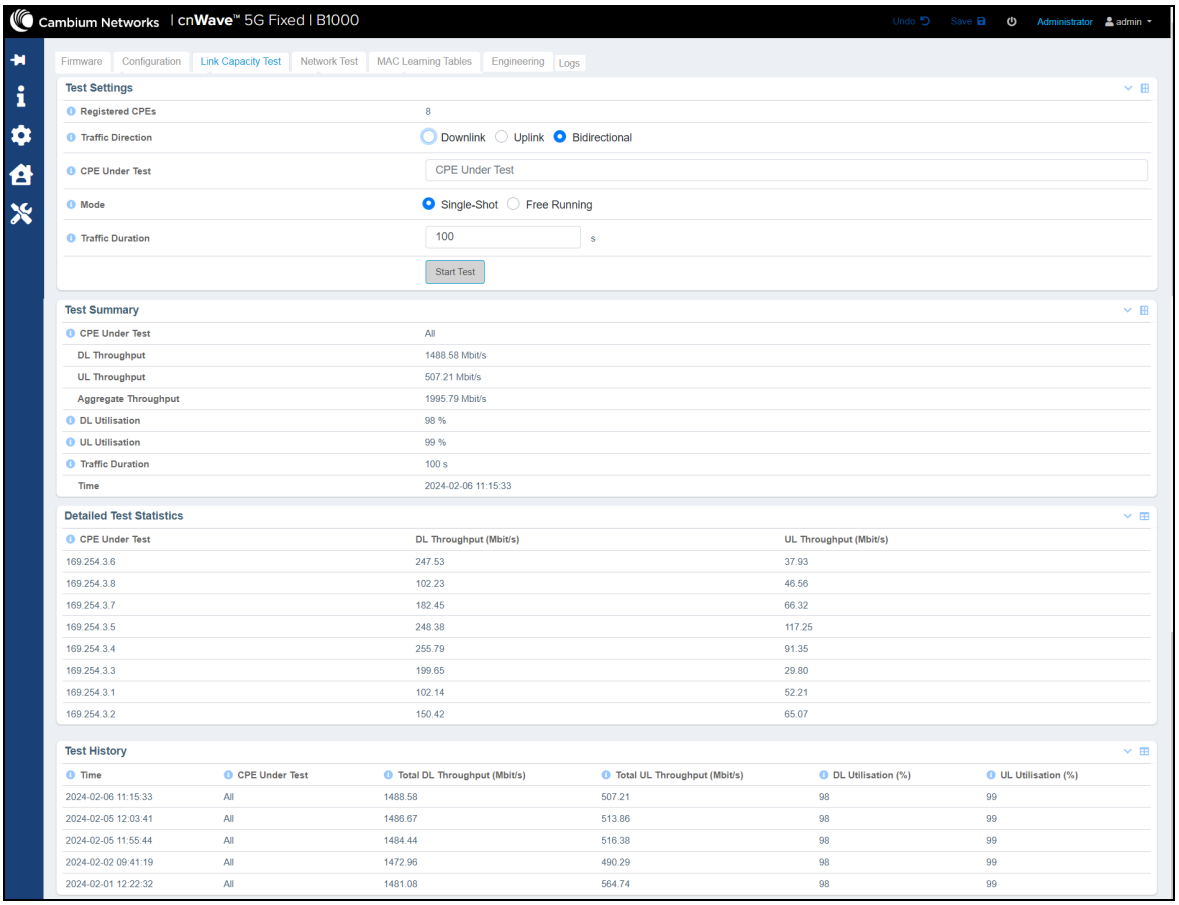
The **Link Capacity Test** page allows you to test the links (uplink, downlink, or both) and analyze the link performance for a subscriber (CPE). The test summary and statistics help in managing the traffic and troubleshooting the links for the subscriber.

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 44.

Figure 44: *The Link Capacity Test page*



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

2. To run the link capacity test, set the values of parameters as described in Table 27.

Table 27: 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	Direction of the transmission of the traffic that you want to test. This parameter supports the following options: • Downlink • Uplink

Parameter	Description
	• Bidirectional Select the required traffic direction.
CPE Under Test	IMSI or IP address of a registered CPE, which is used as the remote device, for which you want to test the link. Type an appropriate value in the text box. If you provide an incorrect value in the text box, a message appears, indicating that the provided value is unknown or invalid. **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, **Test Summary** and **Test History** sections display results for all the connected CPEs.
Mode	Determines the mode for testing the link traffic. This parameter supports the following options: • Single-Shot • Free Running By default, the **Single-Shot** option is selected. **Note**: When you select **Free Running**, the icon appears indicating to select the **Single-Shot** option.
Traffic Duration	Duration (in seconds) of the transmission of the traffic that you want to test. Type an appropriate value in the text box.

3. 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 45) and the previously tested modules (if any).

   Figure 45 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 45: *Link capacity test with MU MIMO disabled*

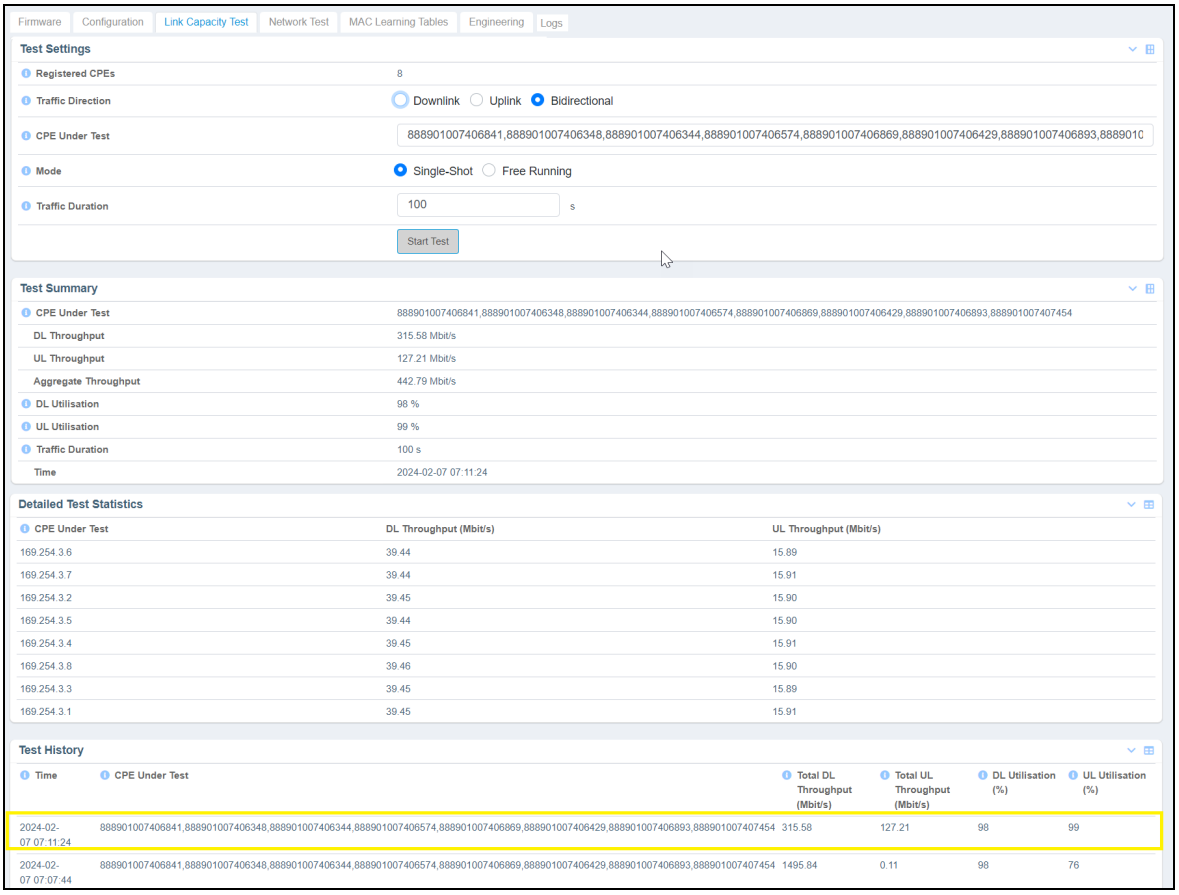


Figure 46 is an example of a link capacity test done for the same IMSIs with the following settings, where:

- **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 46: *Link capacity test with MU MIMO enabled*

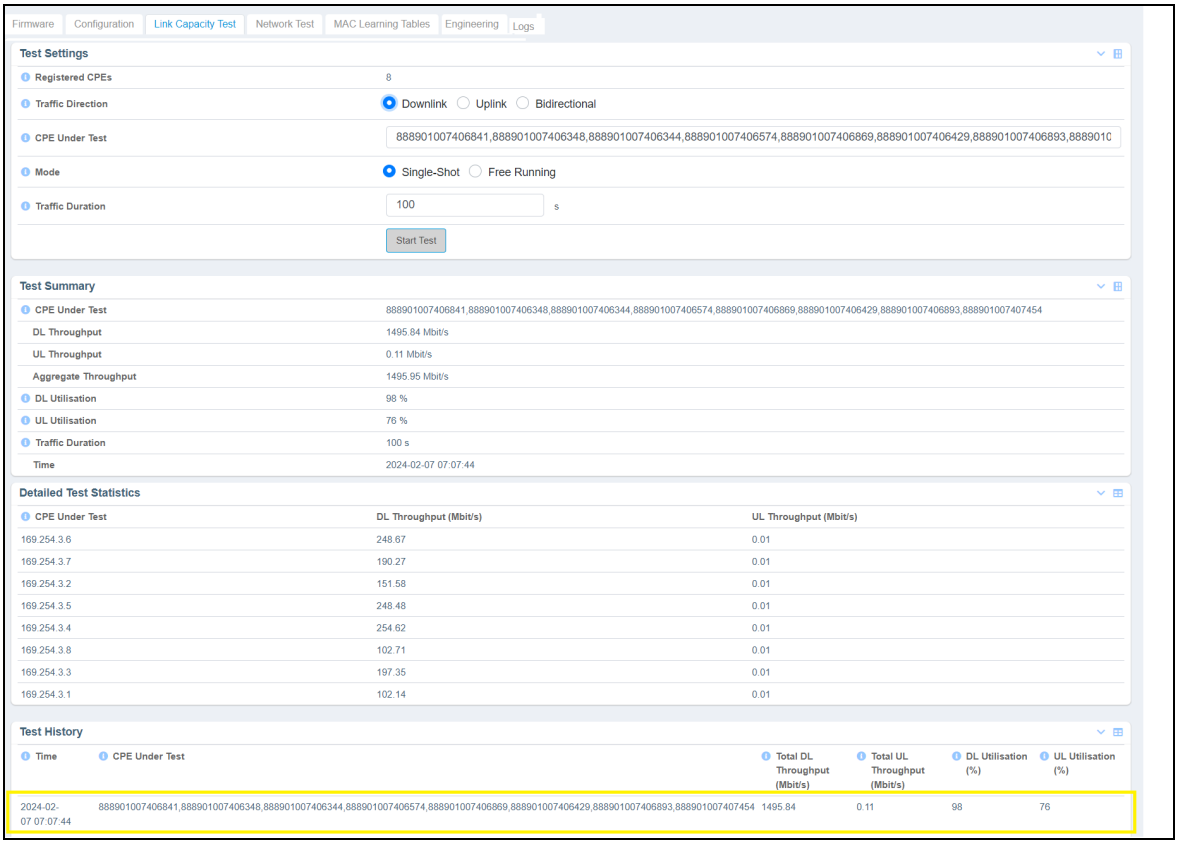


Table 28 lists and describes each parameter of the **Test Summary** and **Test History** sections in the **Link Capacity Test** page.

Table 28: 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.

Parameter	Description
Time	Date and time (YYYY-MM-DD 24-hour format format) at which the traffic 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 Throughout (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

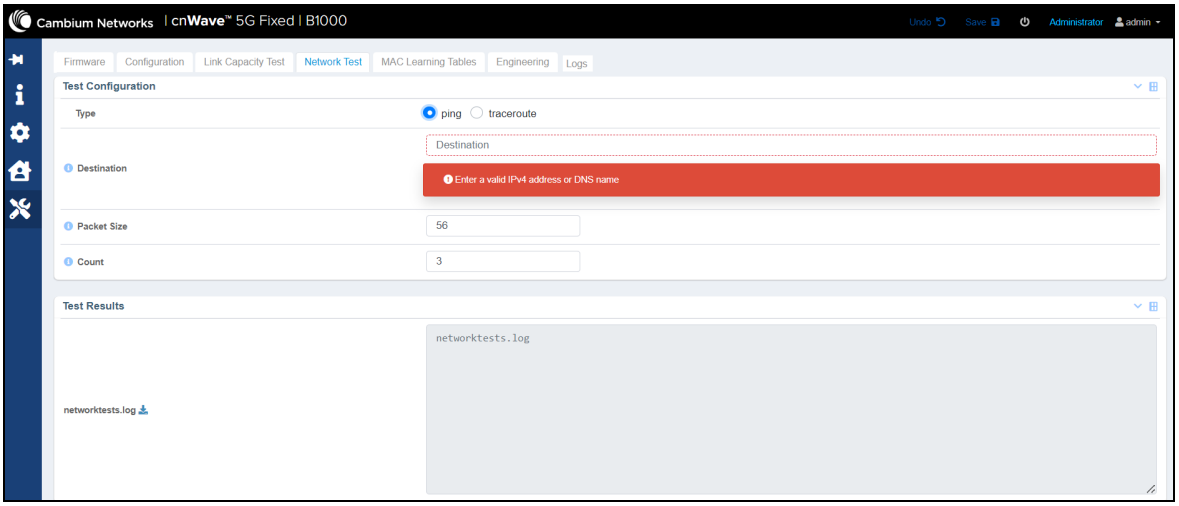
The **Network Test** is a network tool that helps you to test connectivity and accessibility of BTS to a radio network. This page allows you to ensure whether BTS is correctly connected to your network. Example: BTS connectivity with cnMaestro or a RADIUS server. This network test helps in troubleshooting 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 47.

Figure 47: *The Network Test page*



2. View and set the values for parameters, as described in Table 29.

Table 29: List of parameters in the Network Test page

Parameter	Description
Test Configuration	
Type	Determines the method used for testing a network. The following options are supported: • **ping**: BTS pings the required destination (for example, cnMaestro, RADIUS Server, DNS, or a radio network) to ensure its connectivity. If the ping is successful, this implies that BTS can reach the network or the required destination. • **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. 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. Choose the required testing type. Figure 48 and Figure 49 are examples of ping and traceroute types.
Destination	The valid IPv4 address or a DNS name of the required destination. Provide an appropriate value in the text box.
Packet Size	Number of data bytes that have to be sent to the network.

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

Figure 48 is an example of a test result for the **ping** type:

Figure 48: *Test result - ping*

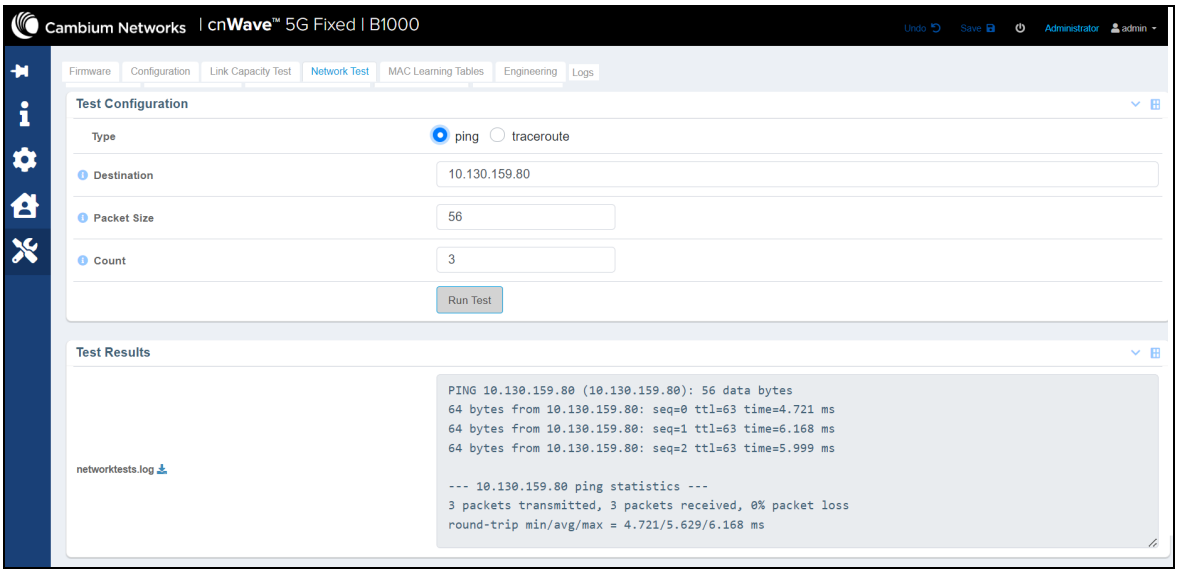
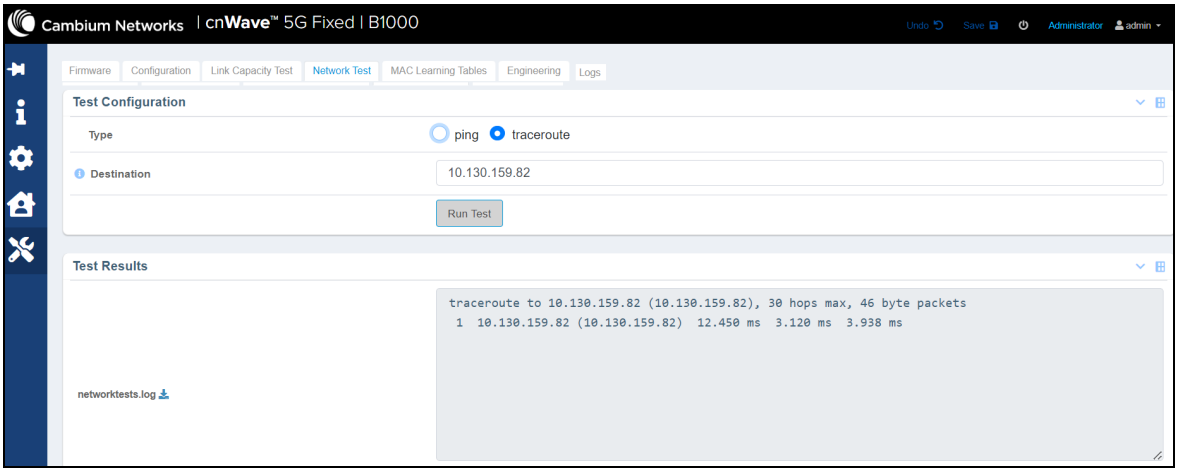


Figure 49 is an example of a test result for the **traceroute** type:

Figure 49: *Test result - traceroute*



MAC Learning Tables

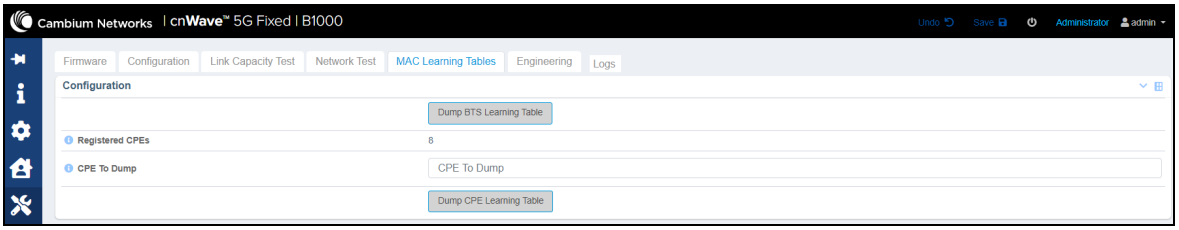
The **MAC Learning Tables** page allows you to dump the MAC addresses of equipment (or other devices) connected to the BTS and CPE radio units. You can also download the dumped MAC addresses in `.txt` file format.

To dump the MAC addresses for BTS and CPEs, perform the following steps:

1. From the main B1000 dashboard page, navigate to **Tools** > **MAC Learning Tables**.

   The **MAC Learning Tables** page appears, as shown in Figure 50.

Figure 50: *The MAC Learning Tables page*



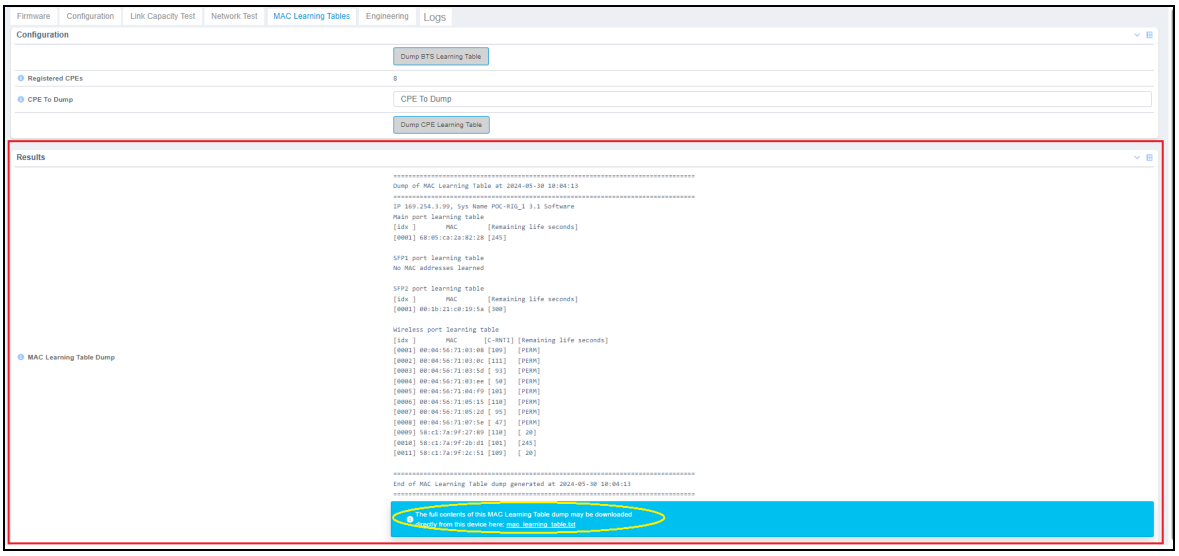
2. Set the parameters, as described in Table 30.

Table 30: Parameters on the Mac Learning Tables page

Parameter	Description
Configuration	
Dump BTS Learning Table	An option to dump the MAC addresses of equipment connected to BTS. When you click on this option, the **MAC Learning Table Dump** parameter appears with the output (which contains all the dumped MAC addresses) in the Results section (as shown in Figure 51). You can also download the output in `.txt` format.
Registered CPEs	The current number of CPEs that are connected and authenticated to this BTS. This is a read-only parameter.
CPE To Dump	The IP address, IMSI, or C-RNTI of the CPE from which you want to display the MAC learning table. You can enter only a single IP address, IMSI, or C-RNTI in this field. **Note**: Leave this field empty or blank to dump the MAC addresses for all CPEs.
Dump CPE Learning Table	An option to dump MAC addresses of equipment connected to the CPE (s). When you click on this option, the **MAC Learning Table Dump** parameter displays the output, which contains MAC addresses of equipment connected to the CPE (s).

Figure 51 is an example of using the **Dump BTS Learning Table** option.

Figure 51: *A sample MAC table dump for BTS*



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

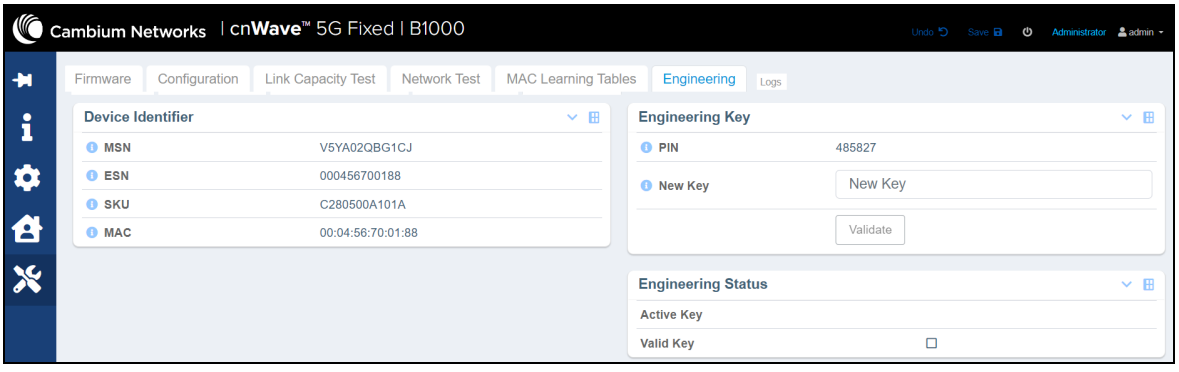
The **Engineering** page is configured and applicable only for troubleshooting and support purposes.

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

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

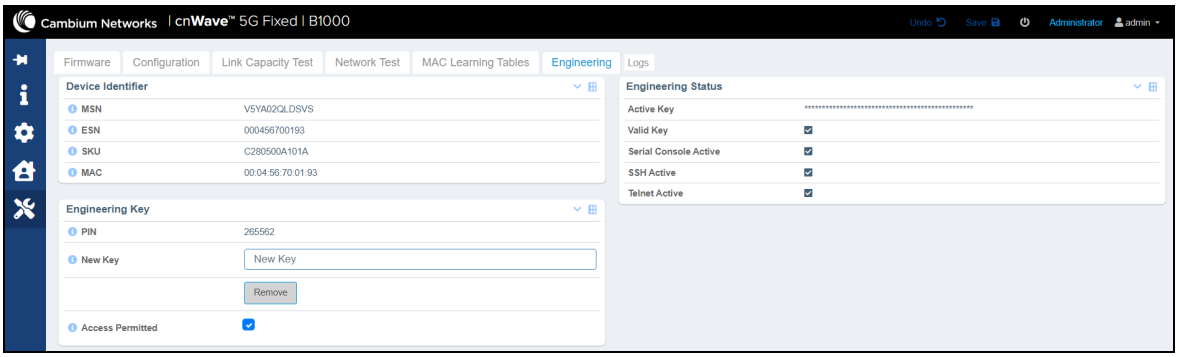
   The **Engineering** page appears, as shown in Figure 52.

   Figure 52: *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 53.

Figure 53: *The Engineering page with all the key details*



2. View and set the values for parameters, as described in Table 31.

Table 31: List of parameters in the Engineering page

Parameter	Description
Device Identifier	
MSN	MSN of the BTS device that is used for identification.
ESN	ESN of the BTS device.
SKU	SKU of the BTS device.
MAC	The MAC address that is assigned to the network interface and used for the BTS 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 checkbox to enable engineering access for the new key.

Parameter	Description
	Note: By default, the engineering access is enabled when a new key is installed.
Engineering Status - The 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.

Logs

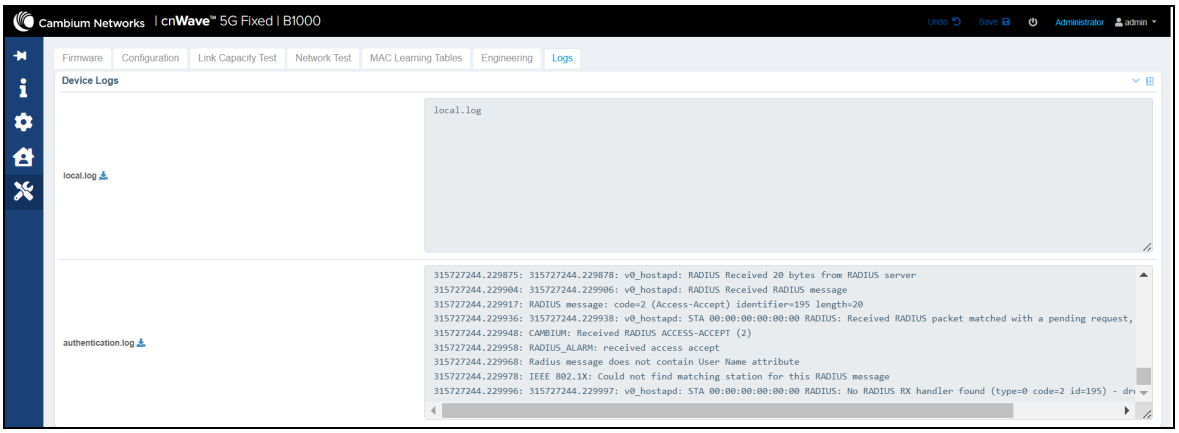
The **Logs** page allows you to view and download `local.log` and `authentication.log` files of the BTS. You can use these logs for troubleshooting.

To view and download the logs, complete the following steps:

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

   The **Logs** page appears, as shown in Figure 54. You can view the logs.

   Figure 54: *The Logs page - B1000 UI*



2. Click the icon to download the logs.

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

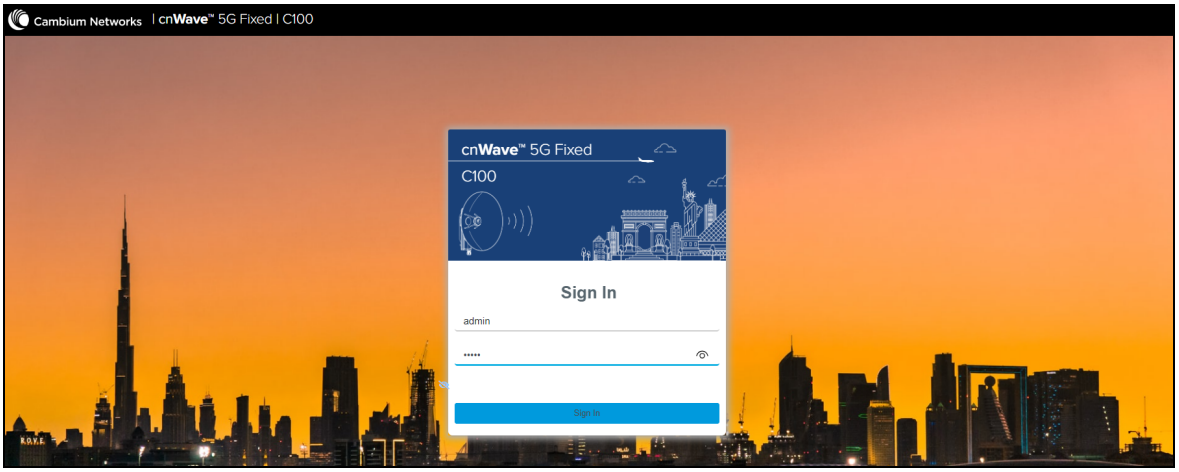
This section explains how to log on to the C100 (CPE) UI and view the C100 dashboard.

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 55.

   Figure 55: *The Sign In page for C100 UI (CPE)*



4. Type an appropriate username and password.

   Default username: admin

   Default password: admin

   You can use the show-password eye icon (👁) to view the password characters.

5. Click **Sign In**.

The **Profile** page appears, as shown in Figure 56. 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 56: *The Profile page*

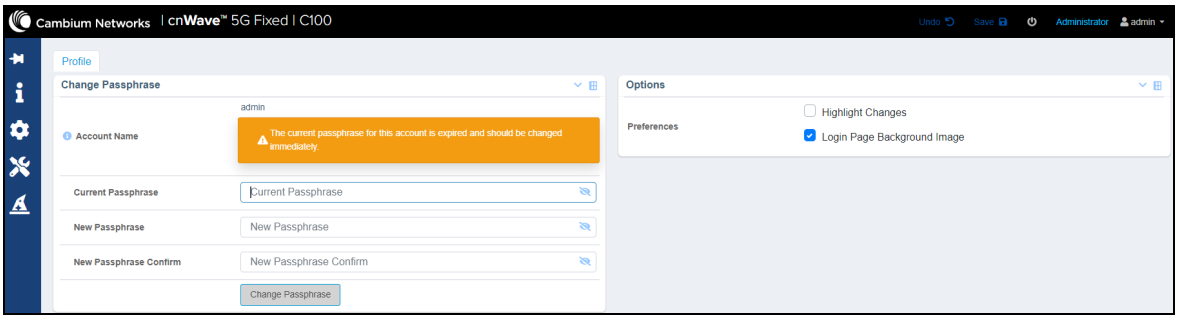


Table 32 lists and describes the parameters on the Profile page of C100 UI.

Table 32: 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
	• **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 quickly monitor 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 55). Select the required option.

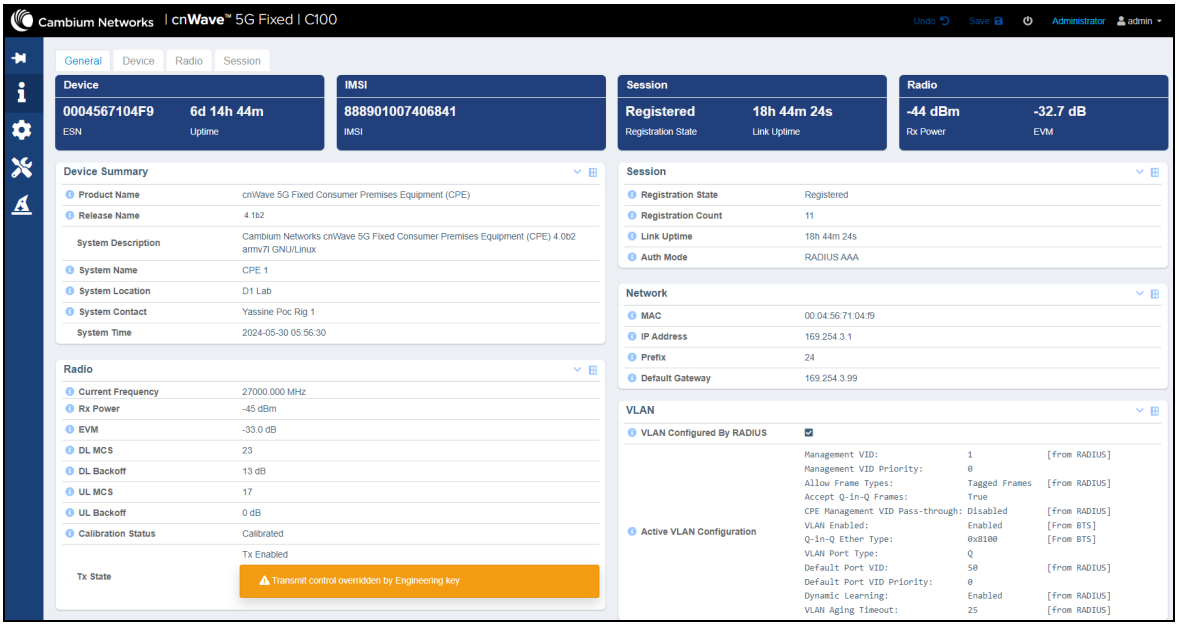
6. On changing the password, log on to the C100 UI using admin (username) and the new password (which you set on the **Profile** page).

   The **Profile** page appears, as shown in Figure 56.

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

   The main **Dashboard** page appears, as shown in Figure 57.

   Figure 57: *The C100 dashboard page*



   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 57) provides comprehensive information about the link status, radio parameters, RADIUS session settings, and other network details. Example: In Figure 57, 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 57) and registered sessions. It also displays details of IMSI, Rx Power, VLAN, and the other system related details. Table 33 lists and describes parameters available on the **General** page.

Table 33: Parameters in the General page

Parameter	Description
Device	The Electronic Serial Number (ESN) of the hardware device (CPE), which is the same as the MAC address. This parameter also indicates the uptime of the CPE device.
IMSI	IMSI that is associated with the CPE (subscriber). IMSI is a number that uniquely identifies the user of a cellular network.
Session	The registration state and the time elapsed after the last successful registration of 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 CPE device.

Parameter	Description
	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.
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	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 the power allocation maximized for the CPE, which also requires for minimizing interference.
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.
Calibration Status	Indicates the unit calibration status. The calibrated status implies that CPE has been tested and calibrated for all the frequency ranges. **Note**: A production unit showing an uncalibrated or a persistent uncalibrated state indicates a problem that requires factory repair.
Tx State	Specifies the status of transmit control (Tx). This is a read-only parameter. By default, this parameter is enabled. **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.

Parameter	Description
	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.
Session	
Registration State	Indicates the progress that a CPE (device) has made to enter the network. For more information about this parameter, refer to Table 36.
Registration Count	Number of times that the CPE has successfully registered with the BTS. For more information about this parameter, refer to Table 36.
Link Uptime	The time elapsed after the last successful registration of the link for the CPE. This parameter displays the time in days or hours, minutes, and seconds.
Auth Mode	Indicates the CPE authentication mode. For more information about this parameter, refer to Table 36.
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	Displays 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 58).

Figure 58: *The Device page - C100 UI*

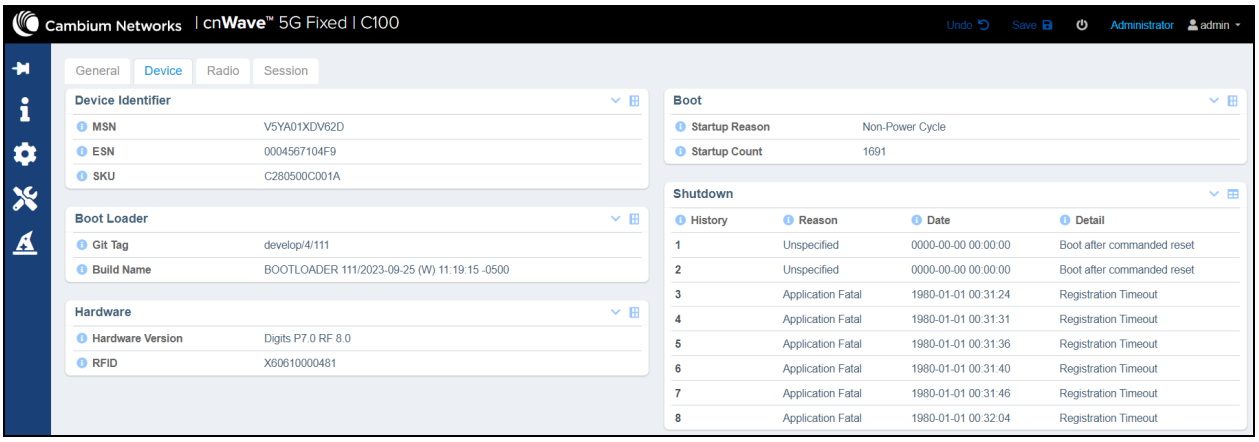


Table 34 lists and describes parameters available on the **Device** page.

Table 34: 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 software.
Hardware	
Hardware Version	Hardware version of the CPE.
RFID	The radio frequency (RF) module ID.
Boot	
Startup Reason	Indicates the reason for the previous system reboot. The following reasons are supported: • 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

Parameter	Description
	starts.
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: • 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.
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 59). You can monitor the C100 (CPE) dashboard to ensure that a connection has been authenticated and established with the desired BTS.

Figure 59: *The Radio page - C100 UI*

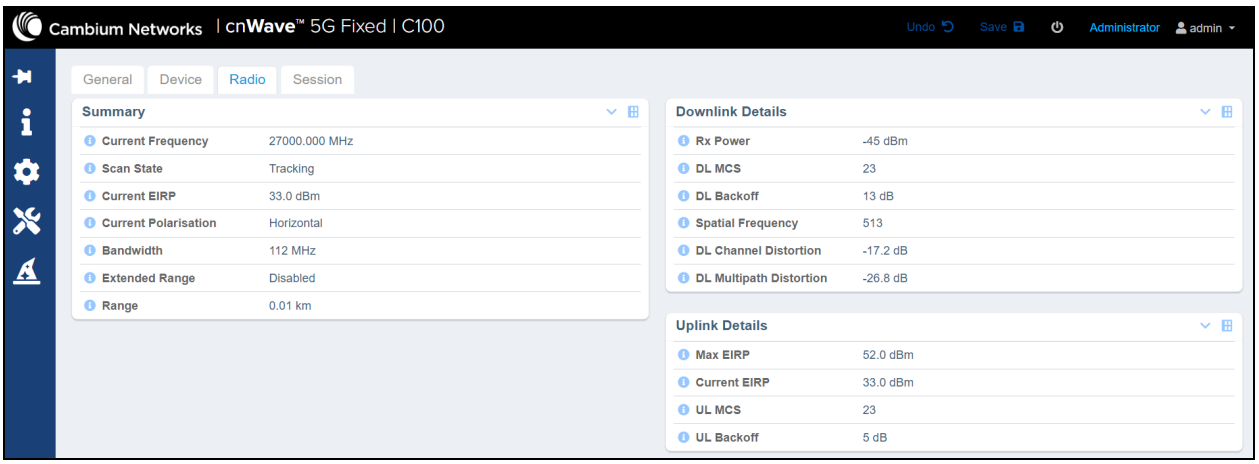


Table 35 lists and describes parameters available on the **Radio** page.

Table 35: Parameters in the Radio page

Parameter	Description
Summary	
Current Frequency	The current operating frequency (in MHz).
Scan State	The current status of the BTS signal specific acquisition state machine. The following states are supported: • Scanning • Scanning - Fine • Acquiring • Tracking **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.

Parameter	Description
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 33.
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 60).

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

Figure 60: *The Session page*

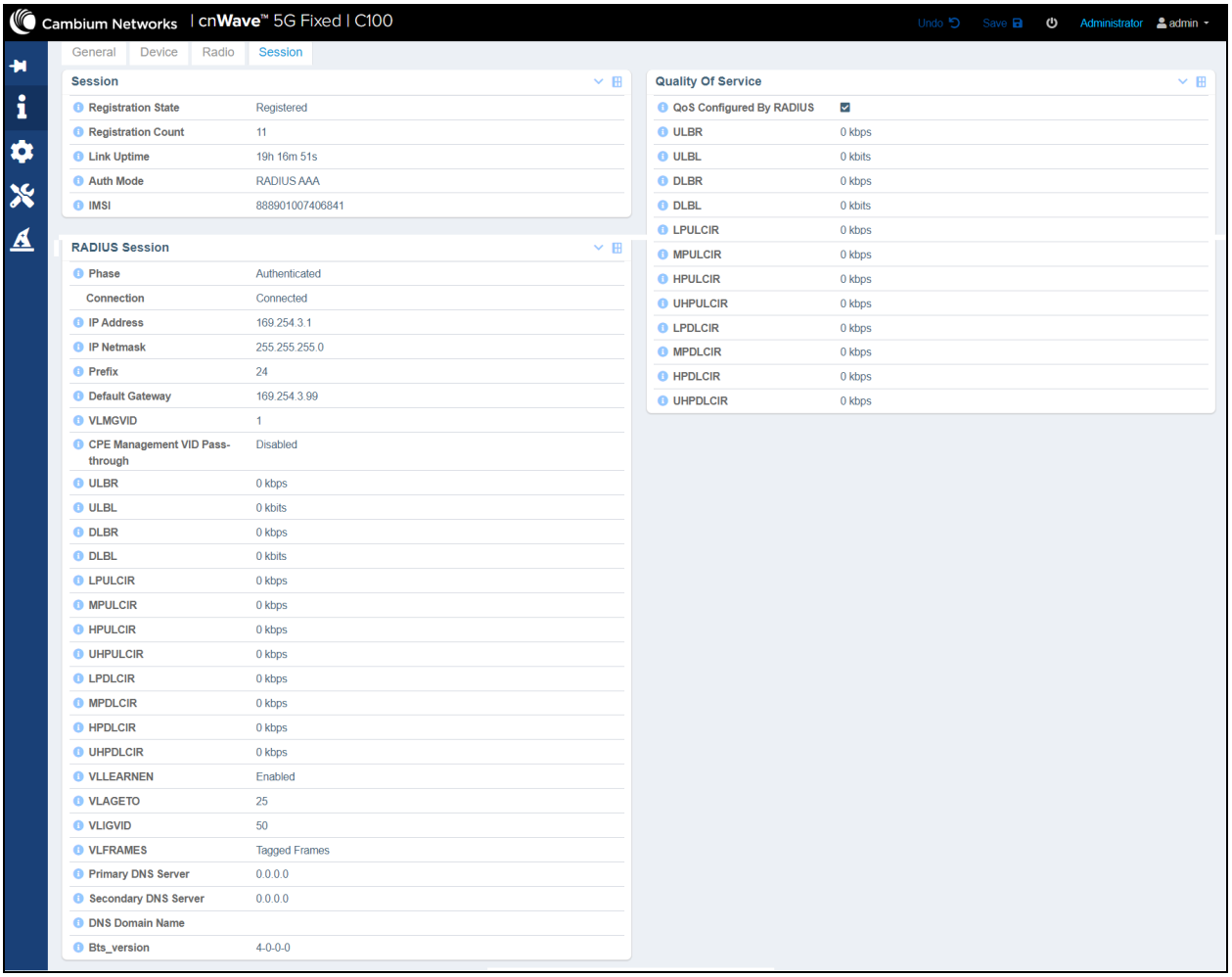


Table 36 lists and describes parameters available on the **Session** page.

Table 36: Parameters in the Session page

Parameter	Description
Session	
Registration State	Indicates the progress that a CPE (device) has made to enter the network. This parameter supports the following device transition states: • 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.

Parameter	Description
	• Configuring - Indicates that the CPE is being configured. • Registered - Indicates that the CPE is ready to pass user traffic.
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: • 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

Parameter	Description
	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 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).
VLLEARNEN	Determines whether the CPE must add the VLAN IDs (VIDs) of upstream frames to the VID table (VLAN learning).

Parameter	Description
	This parameter supports the following values: • 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.
VLAGETO	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 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
Primary DNS Server	IP address of the primary DNS server assigned by RADIUS Server (if any).
Secondary DNS Server	IP address of the secondary DNS server assigned by RADIUS Server (if any).
DNS Domain Name	Name of the DNS domain assigned by RADIUS Server (if any).
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: • Major: This release type is not frequent and implies a significant feature addition or an architectural change.

Parameter	Description
	• 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	
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
- Syslog

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:

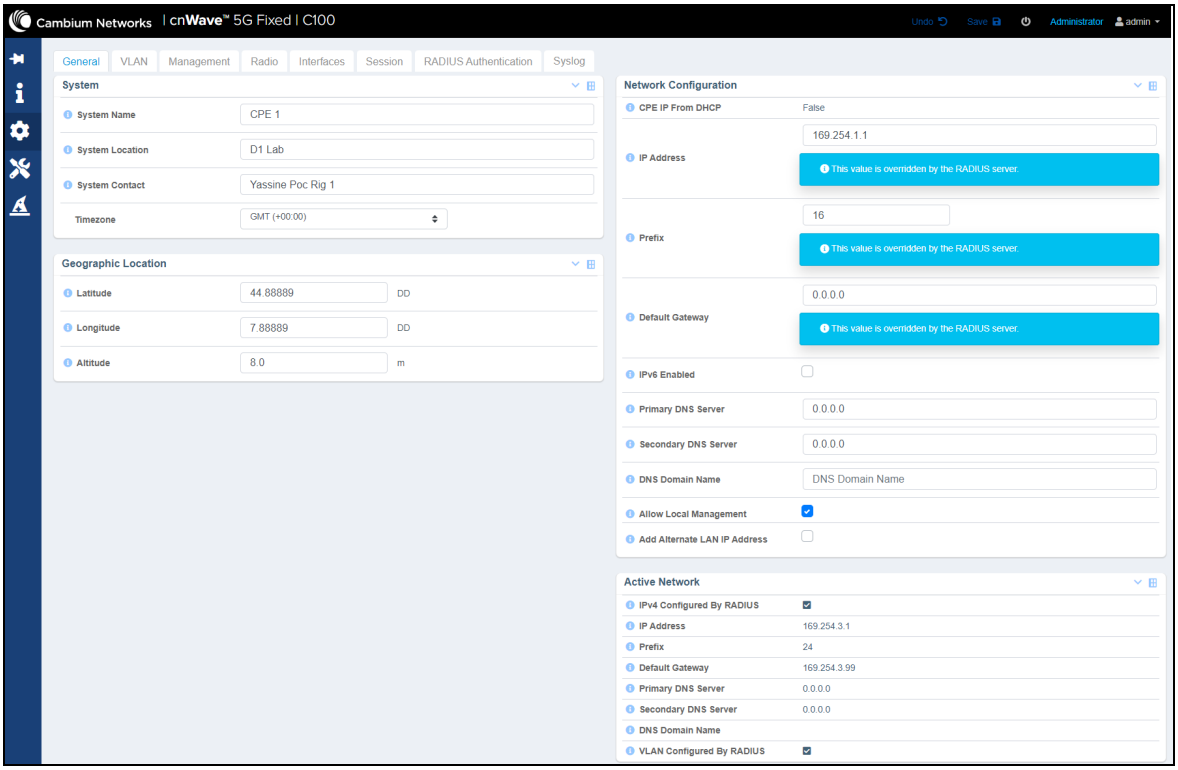
1. Log on to the C100 UI (as described in the Accessing the C100 UI section).

   The main C100 dashboard page appears (as shown in Figure 57).

2. On the left navigation column, click the **System** icon ( ).

   A system setting-specific page appears, as shown in Figure 61. By default, the **General** tab is selected.

Figure 61: *The System page - General settings*



3. Set the values for each parameter, as described in Table 37.

Table 37: 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 CPE 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)

Parameter	Description
Geographic Location	
Latitude	Latitude (in DD) of the geographical location where the CPE is located. Enter an appropriate value in the text box. **Note**: Decimal degrees (DD) indicate 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 CPE is located. Enter an appropriate value in the text box. 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). Enter an appropriate value in the text box.
Network Configuration	
CPE IP From DHCP	Determines whether the CPE's IP network configuration is supplied by a DHCP server. The following values are supported: • 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. If disabled and the Authentication Mode is **None**, the CPE's IP network configuration is set locally at each CPE. You can configure this parameter using the **CPE Provisioning** page of the B1000 UI.
IP Address	The IPv4 address that is assigned to the network interface and used for the device management. Provide appropriate value in the text box. **Note**: The value of this parameter is overridden by the RADIUS server (if connected).
Prefix	The IPv4 network prefix that is assigned to the network interface and used for the device management. Provide appropriate value in the text box.

Parameter	Description
	Note: The value of this parameter is overridden by the RADIUS server (if connected).
Default Gateway	The IPv4 address of the default gateway (if any) that is used for device management. Provide appropriate value in the text box. **Note**: The value of this parameter is overridden by the RADIUS server (if connected).
IPv6 Enabled	Determines whether IPv6 is enabled for CPE management (in addition to the always enabled IPv4 management access). By default, this parameter is disabled. Select the checkbox to enable IPv6 for device management. **Note**: When the select the **IPv6 Enabled** checkbox, the following IPv6-specific parameters appear: • IPv6 Address • IPv6 Prefix • IPv6 Default Gateway
IPv6 Address	This parameter appears when the **IPv6 Enabled** checkbox is selected. Indicates the IPv6 address assigned to the network interface that is used for the device management. Enter a valid IPv6 address.
Pv6 Prefix	This parameter appears when the **IPv6 Enabled** checkbox is selected. Indicates the IPv6 network prefix assigned to the network interface that is used for the device management. Enter an appropriate value. **Note**: Any change to this setting is applicable when the device reboots next. The active value of this setting is currently 0.
IPv6 Default Gateway	This parameter appears when the **IPv6 Enabled** checkbox is selected. Indicates the IPv6 default gateway address used for the device management. Enter an appropriate value. **Note**: Any change to this setting is applicable when the device reboots next.

Parameter	Description
Primary DNS Server	IP address assigned to the primary DNS server (if any) that is used for device management. Enter a valid value in the text box.
Secondary DNS Server	IP address assigned to the secondary DNS server (if any) that is used for device management. Enter a valid value in the text box. **Note**: This parameter can always have an IPv4 address. But it can alternatively have an IPv6 if **IPv6 Enabled** is selected.
DNS Domain Name	The domain name to use for managing DNS configuration. This domain name may be concatenated to DNS names configured for the management interface. Enter an appropriate name in the text box. **Note**: This parameter can always have an IPv4 address. But it can alternatively have an IPv6 if **IPv6 Enabled** is selected.
Allow Local Management	Determines whether you want to manage this device through the local management interface or the radio link. By default, the checkbox is selected (enabled), indicating that the local management interface is used for this device management. If you disable or uncheck the **Allow Local Management** checkbox, all local management traffic is dropped, and the device management is possible only through the radio link. **Note**: If you disable this checkbox, this setting can only be re-enabled by remote management or by resetting to factory defaults.
Add Alternate LAN IP Address	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. If you select the checkbox, the following parameters appear: • Alternate LAN IP Address • Alternate LAN Prefix
Alternate LAN IP Address	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.

Parameter	Description
	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). 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. 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.
Alternate LAN Prefix	The IP network prefix of the alternate LAN IP address. Default value: 16 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. Type an appropriate value in the text box (if required).
Activate Saved Alternate LAN IP Configuration	An option to update the alternate LAN IP configuration and use the currently saved settings. **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. The following are the read-only parameters:	
IPv4 Configured by RADIUS	Indicates whether the IPv4 network configuration is set through RADIUS AAA. The checkbox is selected if the IPv4 network configuration is set through RADIUS AAA. **Note**: On a CPE that is configured for RADIUS authentication, the IPv4 network configuration uses the locally configured settings and swaps to the Radius-supported settings when the RADIUS authentication takes place. The locally configured settings may be overridden by the Radius-supported settings during registration.
IP Address	The IPv4 address that is assigned to the network interface and used for the device management.
Prefix	The IPv4 network prefix that is assigned to the network interface and used for the device management.

Parameter	Description
Default Gateway	The IPv4 address of the default gateway (if any) that is used for the device management.
Primary DNS Server	IP address assigned to the primary DNS server (if any) that is used for the device management.
Secondary DNS Server	IP address assigned to the secondary DNS server (if any) that is used for the device management.
DNS Domain Name	The domain name to use for managing DNS configuration. This domain name may be concatenated to DNS names configured for the management interface.
VLAN Configured by RADIUS	Indicates whether the VLAN configuration is set through RADIUS AAA. At boot, locally configured settings are used for the VLAN network configuration. These settings are overridden by RADIUS-supplied settings during registration. The checkbox is selected if the network configuration is set through RADIUS AAA.

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

VLAN

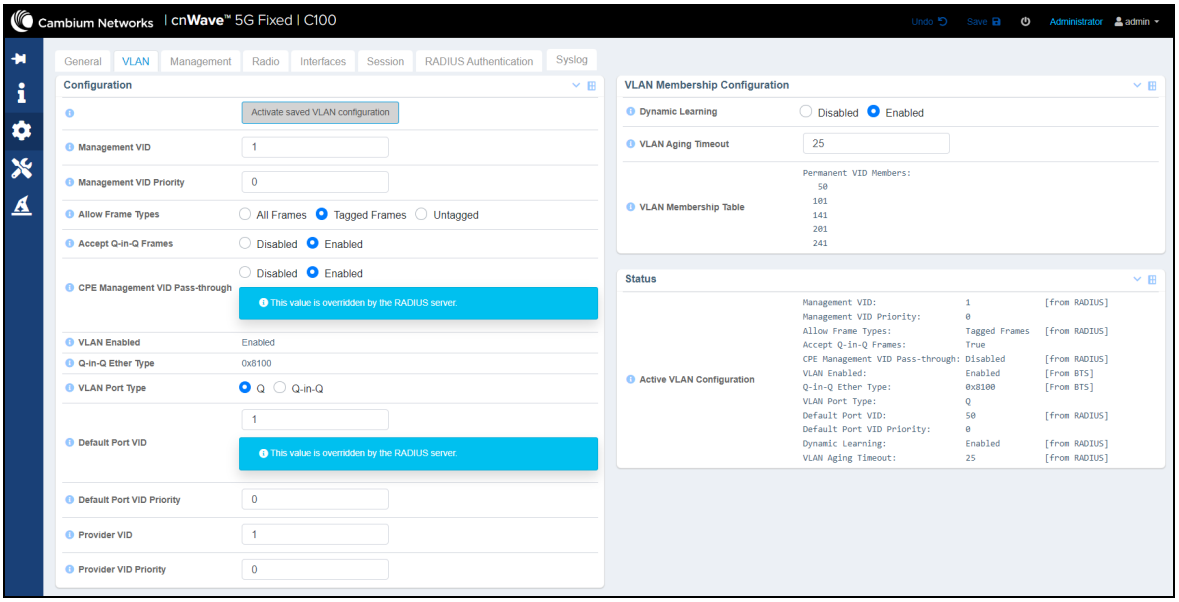
The **VLAN** page allows you to configure VLANs and related settings for the CPE device. This page also displays the active VLAN configuration.

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 62.

Figure 62: *The VLAN page*



2. Set the values for each parameter, as described in Table 37.

Table 38: Parameters on the VLAN page

Parameter	Description
Configuration	
Activate Saved VLAN Configuration	An action that updates the live VLAN configuration to use the currently saved settings unless they are overridden by RADIUS. **Note**: If you have changed **Management VID**, then you will lose contact with the device until you make the corresponding changes. 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.
Management VID	The VLAN ID used to communicate with BTS and CPE for the management purpose. Type an appropriate value in the text box. Default value: 1 - which implies that there is no VLAN in the system. You can set up an ID value between 2 and 4094.
Management VID Priority	The priority value that is set for the management VLAN ID.

Parameter	Description
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. The following options are supported: • All Frames • Tagged Frames • Untagged Select the required incoming frame type. Default value: All Frames **Note**: The value of this parameter is overridden by the RADIUS server (if connected).
Accept Q-in-Q Frames	Determines whether a Q-in-Q frames are accepted or blocked. 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. 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. This parameter supports the following options: • Disabled • Enabled Default value: Disabled Select the required option. **Note**: To apply the changes to this setting, reboot the device.
CPE Management VID Pass-through	Determines whether the Management VID traffic (VLMGVID) is allowed to or from the CPE wired interface. The following options are supported: • Disabled • Enabled Default value: Enabled Select the required option. To apply the changes to this setting, reboot the device. **Note**: The value of this parameter is overridden by the RADIUS server (if connected).

Parameter	Description
VLAN Enabled	Determines whether the VLAN functionality for the BTS and all linked CPEs is enabled. 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.
Q-in-Q Ether Type	The Ether types for Q-in-Q (802.1ad) and outer tag (S-Tag). Default value: 0x88a8 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	Indicates the VLAN tunnel technique or port type used by the Ethernet service provider for segregating the traffic. The following options are supported: • 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. **Note**: The VLAN port type configures the behaviour of the local Ethernet only and the internal management interfaces always operate as Q ports. Default value: Q Select the required port type.
Default Port VID	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). Default value: 1 **Note**: The value of this parameter is overridden by the RADIUS server (if connected).
Default Port VID Priority	The priority value that is set for the default VID VLAN. Default value: 0
Provider VID	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. If an existing 802.1Q frame arrives, the provider VID is used for adding and removing the outer S-tag. If an untagged frame arrives at a Q-om-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. Default value: 1

Parameter	Description
Provider VID Priority	The priority value that is set for the default VID VLAN. Default value: 0
VLAN Membership Configuration	
Dynamic Learning	Determines whether the CPE must add the VLAN IDs (VIDs) of upstream frames to the VID table. The following options are supported: • Disabled: The CPE does not add the VIDs. • Enabled: The CPE adds the VIDs. The CPE drops frames with VIDs, which are not stored in the VID table. Default value: Enabled Select the required option. **Note**: If you modify the values of this parameter, the value is overridden during RADIUS AAA registration.
VLAN Aging Timeout	Specifies 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) Provide an appropriate value in the text box. **Note**: VIDs that you set for the Untagged Ingress VID and Management VID parameters do not time out.
VLAN Membership Table	Lists the permanent VID members. This is a read-only parameter.
Status	
Active VLAN Configuration	Details of a summary of the active VLAN configuration.

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

Management

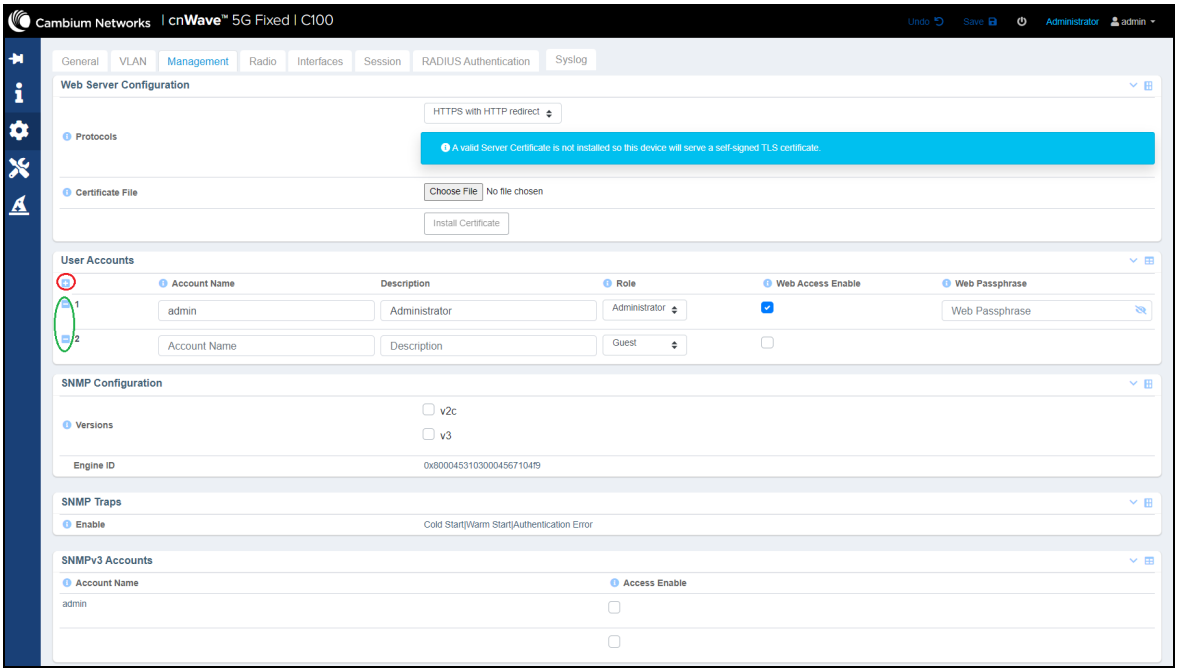
The **Management** page allows you to set up user account and SNMP configuration related information. This configuration allows the users to manage the C100 dashboard and the CPEs using SNMP.

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 63.

Figure 63: *The Management page*



2. Set the values for each parameter, as described in Table 39.

Table 39: Parameters in the Management page

Parameter	Description
Web Server Configuration	
Protocols	Type of protocol that must be configured for accessing and managing the web UI of CPE. This parameter supports the following options: • **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. Default value: HTTPS with HTTP redirect Select the required protocol from the drop-down list.

Parameter	Description
	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.
Certificate File	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. To upload a certificate file (.PEM) from the desired location locally, perform the following steps: a. Click **Choose File**. A file folder appears. b. Browse the location where you have saved the required certificate file (.PEM) on your machine. c. Click **Open**. The certificate file is selected, and the file name appears next to the **Choose File** button. d. Click **Install Certificate**. The selected certificate file is installed, which is authenticated and encrypted.
User Accounts	
Account Name	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. Provide an appropriate name in the text box. Example: admin 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. **Note**: To add a new user account row, use the ⊞ icon located beside the **Account name** parameter (as shown in Figure 63). To delete a user account, use the ⊟ icon located beside the corresponding account name.
Description	A brief description of the account. Provide a brief description for the user account that you want to add. Example: Super admin

Parameter	Description
Role	Specifies the role of the user who wants to access the CPE device. This parameter supports the following roles, which have different capabilities and serve different functions: • **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 roles 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. Select an appropriate option from the drop-down list.
Web Access Enables	Determines whether the access for web UI of the CPE device is enabled for the selected role. Select the checkbox if you want to enable web access for the required user role. **Note**: Multiple users are allowed to access the UI simultaneously.
Web Passphrase	The passphrase (password) that is assigned to the user role of this account for accessing the web UI.

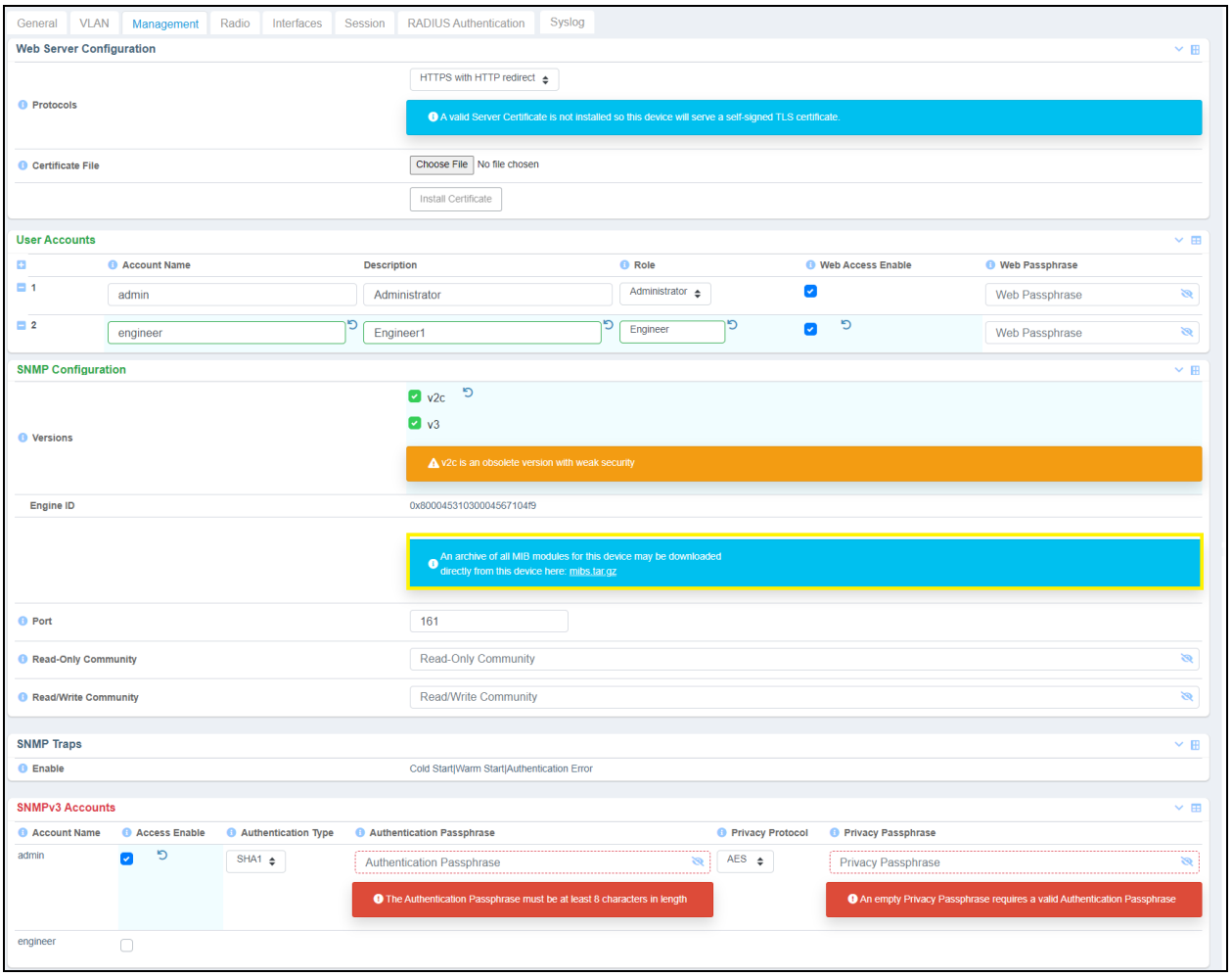
Parameter	Description
	Type an appropriate password in the text box.
SNMP Configuration	
Versions	The version of the SNMP protocol that is supported by the agent running this CPE device. The SNMP protocols are used for managing and monitoring the network devices. The following SNMP protocol versions are supported: • V2c : A standard and simpler community-based security model. It is an obsolete version with weak security. • V3: An advanced version designed to address security , access control, privacy, and authentication issues. Choose the required SNMP version.
Engine ID	Unique ID that is used by the SNMP agent.
Note: A message is visible after the **Engine ID** field, providing an option to download the SNMP MIB files directly from the device (as shown in Figure 64). Using the SNMP MIB files, you can access VLAN and QoS attributes of CPEs.	
Port	This parameter appears only when you select an SNMP version (V2c or V3). Indicates the network port number assigned to the SNMP agent, which is running on the device. Default value: 161 Provide an appropriate value in the text box.
The following parameters appear only when you set V2c in the **Versions** field:	
Read/Only Community	Name of the SNMP V2c community for read-only access to the device. Provide an appropriate value in this text box.
Read/Write Community	Name of the SNMP V2c community for read-write access to the device. Provide an appropriate value in this text box.
SNMP Traps	
Enable	Indicates the categories of SNMP traps sent by the device. This is a ready-only parameter.
SNMPv3 Account - This section allows you to set access control, authentication, and privacy-	

Parameter	Description
related properties (as shown in Figure 64) for the roles selected in the **User Accounts**.	
Account Name	The account name that is used for authentication of the CPE device. This is read-only parameter that contains account names, which you added in the **User Accounts** section.
Access Enable	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). Select the checkbox for the required account names. This setting permits the user role to access the CPE device using SNMP. **Note**: To modify this parameter, you must enable V3 using the **Versions** parameter in the **SNMP Configuration** section.
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 64):	
Authentication Type	Indicates the authentication type to use. This parameter supports the following options: • None • MD5 • SHA1 Select the required option from the drop-down list.
Authentication Passphrase	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. The value of this parameter can contain any combination of ASCII characters. The value must consist of eight characters in length. Type a valid value in the text box.
Privacy Protocol	Specifies the protocol that must be used for account privacy. This parameter supports the following options: • None • DES • AES Select the required option from the drop-down list.

Parameter	Description
Privacy Passphrase	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. The value of this parameter can contain any combination of ASCII characters. Also, the value must consist of eight characters in length. Type a valid value in the text box. 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.

Figure 64 is an example of configuring the **Management** page for the CPE.

Figure 64: *The Management page - C100 UI*



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

Radio

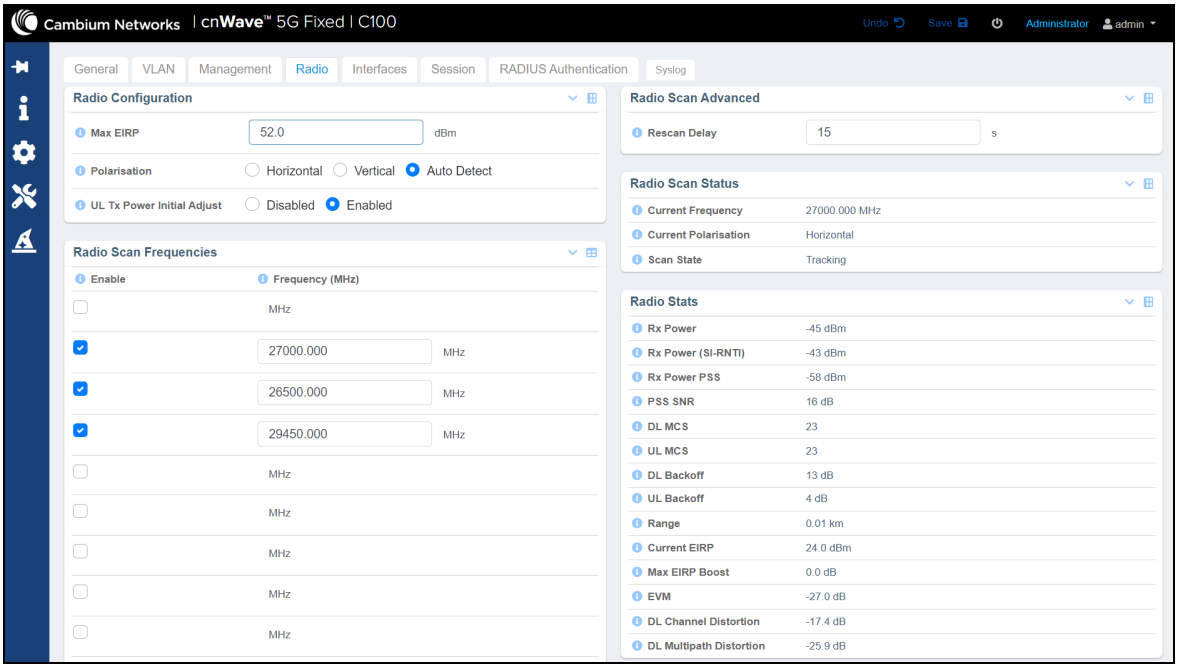
This **Radio** page allows you to configure the radio configuration parameters and radio scan frequencies. It also provides information about the radio scan status and statistics.

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 65.

   Figure 65: *The Radio page - C100 UI*



2. Set the values for each parameter, as described in Table 40.

   Table 40: Parameters on the Radio page

Parameter	Description
Radio Configuration	
Max EIRP	The maximum EIRP configured value (in dBm). Type an appropriate value in the text box. **Note**: Ensure that the value is greater than or equal to 20.0 dBm.
Polarisation	Determines the antenna polarisation settings. This parameter supports the following polarisation settings: • Horizontal • Vertical

Parameter	Description
	• Auto Detect (recommended value for the CPE) Select the required polarisation for the antenna.
UL Tx Power Initial Adjust	Indicates the uplink initial transmit power control mode for CPEs. This parameter supports the following options: • Disabled - If this parameter is disabled, CPEs use their configured maximum transmit power. • Enabled - If this parameter is enabled, CPEs adjust their transmit power to reach the BTS target receive power before starting transmission. By default, this parameter is **Enabled**. Select the required option.
Radio Scan Frequencies	List of required frequencies (in MHz) that the CPE can use. You can also enable the configured frequency, for effective use, by selecting the corresponding frequency checkbox. Type appropriate frequency values (in MHz) and select the checkbox in the corresponding row. **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.
Radio Scan Advanced	
Rescan Delay	The delay period (in seconds) before rescanning radio frequencies when the signal is lost. Type an appropriate value in the text box.
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	Indicates the radio scan state. Example: Tracking
Radio Stats	
Rx Power	The Receive power of data symbols (in dBm).
Rx Power (SI-RNTI)	Indicates the Receive power (in dBm) for the SI-RNTI on the strongest beam.

Parameter	Description
	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. **Note**: The CPE reports the SI-RNTI statistics such as bandwidth (in MHz) and DL Rx Power (SI-RNTI) in dBm.
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. 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 the power allocation maximized for the CPE, which also requires for minimizing interference.
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.
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	Value (in dB) that indicates the distortion (or degraded) length of the downlink MU-MIMO. **Note**: Values that are less than -10 are considered good values.
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.

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

Interface

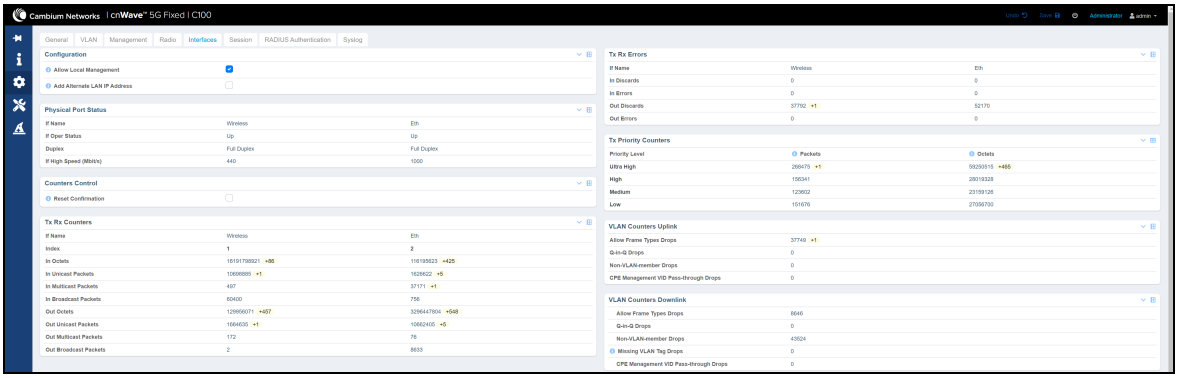
The **Interface** page allows you to configure the local management of interfaces. It also provides statistical information about all the CPE interfaces (such as Copper).

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 66.

   Figure 66: *The Interface page*



2. View or monitor the interface related parameters, as described in Table 41.

   Table 41: Parameters in the Interface page

Parameter	Description
Configuration	
Allow Local Management	Determines whether you want to manage this device through the local management interface or the radio link. By default, the checkbox is selected (enabled), indicating that the local management interface is used for this device management. If you disable or uncheck the **Allow Local Management** checkbox, all local management traffic is dropped and the device management is possible only through the radio link. **Note**: If you disable this checkbox, this setting can only be re-enabled by remote management or by resetting to factory defaults.
Add Alternate LAN IP Address	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. If you select the checkbox, the following parameters appear:

Parameter	Description
	• Alternate LAN IP Address • Alternate LAN Prefix
Alternate LAN IP Address	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. **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). 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. 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.
Alternate LAN Prefix	The IP network prefix of the alternate LAN IP address. Default value: 16 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. Type an appropriate value in the text box (if required).
Activate Saved Alternate LAN IP Configuration	An option to update the alternate LAN IP configuration and use the currently saved settings. **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.
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).

Parameter	Description
Counters	
Reset Confirmation	An option to reset the SNMP MIB-II interface counters. When you select the checkbox, the **Reset Counters** button appears. You can use this button to reset the SNMP MIB-II interface counters.
Tx Rx Counters - Applicable to data ports and wireless. The data report is listed in the following columns: • **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.
Tx Rx Errors - Applicable to data ports and wireless.	
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 labeled as discarded by the CPEs.
Out Errors	Number of outgoing data packets (from CPEs) that contain errors.
Tx Priority Counters	
Priority Level	Displays the priority level of the bearer relevant to each Transmit counter.

Parameter	Description
	This parameter displays the following priority levels: • Ultra High • High • Medium • Low You can view the number of packets and octets transmitted at each priority level.
Packets	Number of packets successfully delivered to the far end of the link based on priority.
Octets	The number of Octets successfully delivered to the far end of the link based on priority.
VLAN Counters Uplink - Displays the statistics for VLAN counters UL.	
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-thorough events that are dropped by the CPE in the uplink direction.
VLAN Counters Downlink - Displays the statistics of VLAN counters DL.	
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.

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

Session

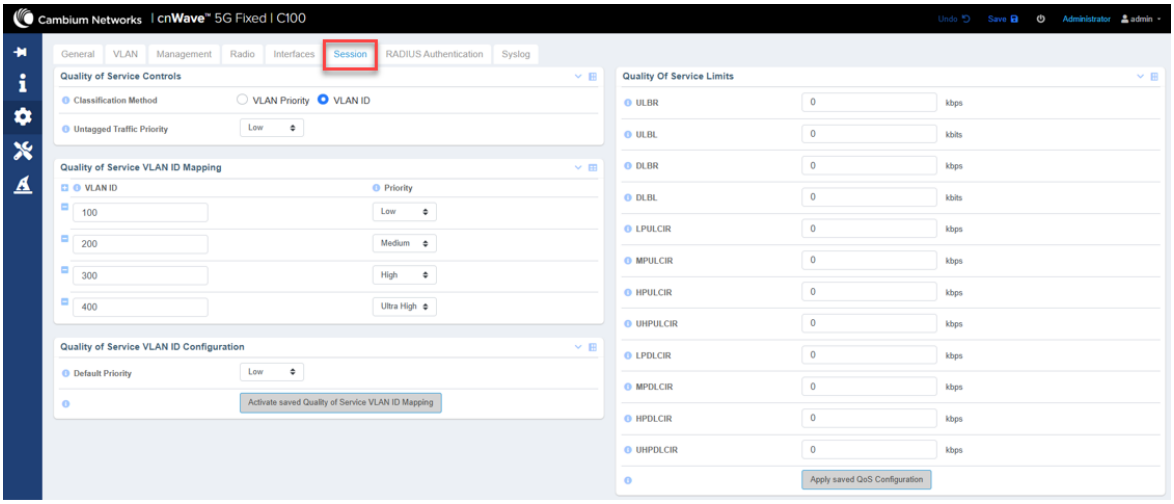
The **Session** page allows you to enable the Watchdog to monitor the registration sessions of the CPE.

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 67.

   Figure 67: *The Session page - C100 UI*



2. View the session related settings, as described in Table 42.

   Table 42: List of parameters in the Session page

Parameter	Description
Quality of Services Controls	
Classification Method	This controls which field within the VLAN header is used to perform the packet classification. The following options are supported: • VLAN Priority • VLAN ID If **VLAN Priority** is selected, the packets transmitted over-the-air by the BTS are classified using the 3-bit **Priority** field of the VLAN ID, with the mapping from the Priority bit to the priority within the B1000 being as follows: • 0 or 1 -> Low Priority • 2 or 3 -> Medium Priority

Parameter	Description
	• 4 or 5 -> High Priority • 6 or 7 -> Very High Priority If **VLAN ID** is selected, the packets transmitted over the air by the BTS are classified using the VLAN ID to the Priority level as defined below by the **Quality of Service VLAN ID Mapping**.
Untagged Traffic Priority	This controls which priority the BTS must assign to untagged traffic. The following options are supported: • Low • Medium • High • Very High
Quality of Services VLAN ID Mapping	
VLAN ID and Priority	This section is only visible and relevant if the **Classification Method** above is set to “VLAN ID”. This is a dynamic table that defines which priority to assign to a VLAN packet based on its VLAN ID. Up to 32 entries can be specified. For each entry, a VLAN ID value between 1 and 4095 must be specified and a priority level of Low, Medium, High, and Very High must be selected for that VLAN ID.
Quality of Services VLAN ID Configuration	
Default Priority	This section is only visible and relevant if the **Classification Method** above is set to **VLAN ID**. This controls what level of priority must be assigned to VLAN packets for which the VLAN ID could not be matched in the list provided in the **VLANID** and **Priority** section above. The following options are supported: • Low • Medium • High • Very High
Activate saved Quality of Service VLAN ID Mapping	This button is only visible and relevant if the **ClassificationMethod** above is set to **VLAN ID**.

Parameter	Description
	It activates the Quality of Service VLAN ID Mapping entered in the section above. Please remember to click this button once you have made changes to the **VLAN ID and Priority** or **Default Priority** above.

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

RADIUS Authentication

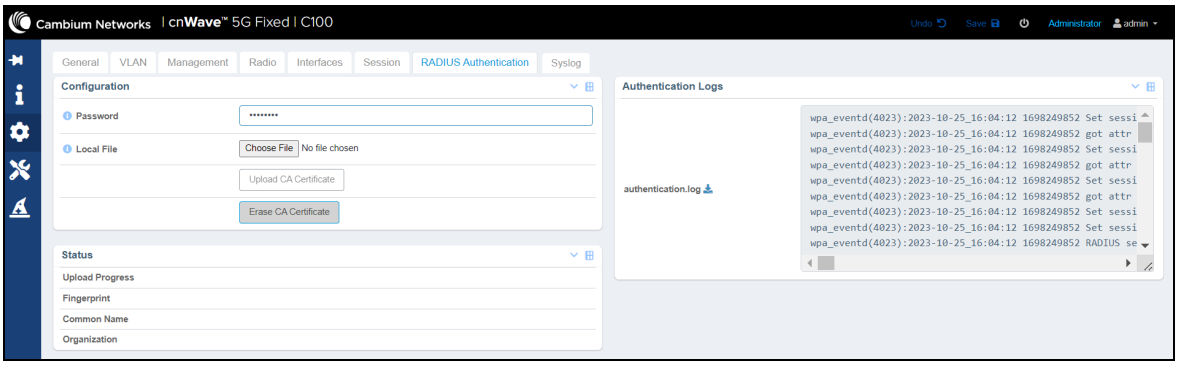
The **RADIUS Authentication** page allows you to configure the RADIUS server specific certificate authority (CA) certificate (for security purposes) required for the RADIUS authentication.

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 68.

   Figure 68: *The RADIUS Authentication page - C100 UI*



2. Set the parameters, as described in Table 43.

   Table 43: 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: a. Click **Choose File** in the Local File field. A file browser window appears.

Parameter	Description
	b. Browse the location where you have saved the CA certificate on your system locally. c. Select the certificate file and click **Open**. The local file is selected. d. To upload the selected local file, click **Upload CA Certificate**on 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.
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 binds 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.

Syslog

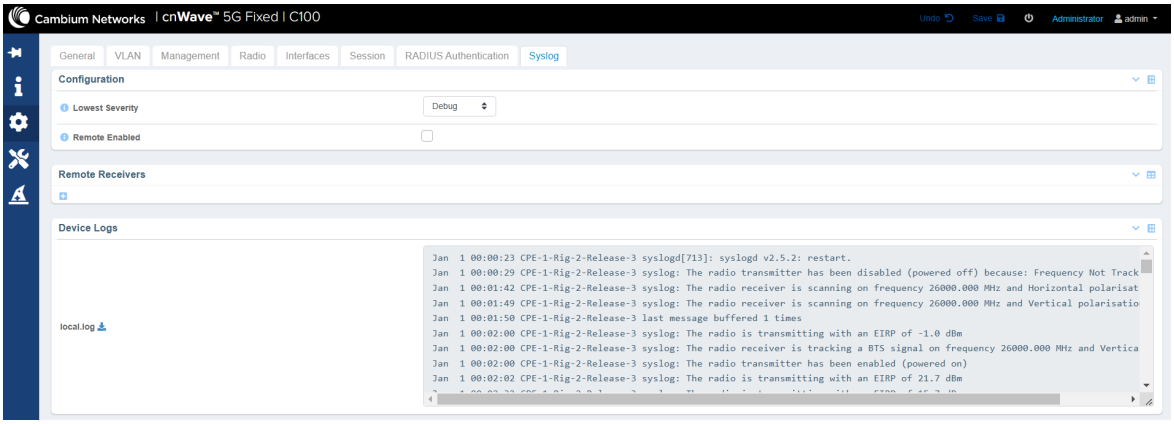
The **Syslog** page allows you to allocate the lowest syslog severity level and enable the remote syslog specific parameters for the CPE device. The syslog configuration helps you to record and view all events of the CPE device. Example: CPE connected to BTS.

To configure and view the **Syslog** page, perform the following steps:

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

   The **Syslog** page appears, as shown in .

Figure 69: *The Syslog page - C100 UI*



2. Set the value of each parameter, as described in the table below.

Table 44: List of parameters in the Syslog page - C100 UI

Parameter	Description
Configuration	
Lowest Severity	Allows you to configure the lowest syslog severity that is logged locally on the CPE device. The following syslog severity levels are supported: • Emergency - means system is unusable. • Alert - means action must be taken immediately. • Critical - means critical conditions. • Error - means error conditions. • Warning - means warning conditions. • Notice - means normal but significant conditions. • Information - means informative messages. • Debug - means debug-level messages. Select the required severity from the drop-down list.
Remote Enabled	When you enable this remote syslog parameter, important system events are sent to the configured remote syslog receivers. Syslog facilities include `syslog`, `auth`, and `local0 thro local7`.

Parameter	Description
	When you select the **Remote Enabled** checkbox, the **Remote Receivers** section appears with the following parameters: • Inet Address • Port • Standard • Lowest Severity
Remote Receivers	
Inet Address	IP address that is assigned to the remote syslog receiver. All enabled severity levels of syslog messages are sent to this address. Type an appropriate value in the text box.
Port	The network port that is assigned to the remote syslog receiver. Type a valid value in the text box. **Note**: The zero (0) value is not valid.
Standard	Indicates the syslog message format, which is determined by RFC 3164 and RFC 5424 standards. The following options are supported: • RFC 3164 • RFC 5424 Select the required option from the drop-down list.
Lowest Severity	Allows you to configure the lowest syslog severity message that is sent to the remote syslog receiver. The following syslog severity levels are supported: • Emergency - means system is unusable. • Alert - means action must be taken immediately. • Critical - means critical conditions. • Error - means error conditions. • Warning - means warning conditions. • Notice - means normal but significant conditions. • Information - means informative messages.

Parameter	Description
	• Debug - means debug-level messages. Select the required severity from the drop-down list.

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

   The **Device Logs** section displays the events of the CPE device for the selected severity level. You can view and download the logs (if required) using the icon.

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
- MAC Learning Tables
- Engineering
- Logs

Firmware

The **Firmware** page allows you to upgrade or downgrade software firmware. This page also provides 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.

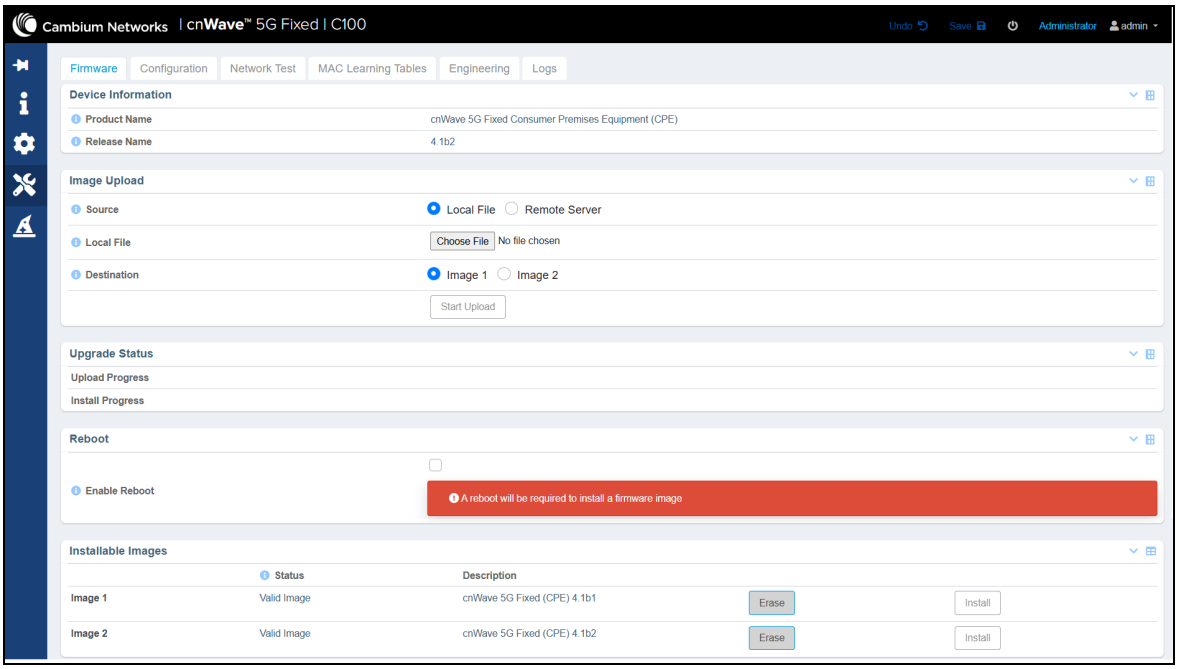
  b. Upgrade the BTS to the previous official software release version W.

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

   Figure 70: *The Tools page - C100 UI*



2. Set the required parameters, as described in Table 45.

   Table 45: 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 Customer Premise Equipment (CPE)
Release Name	Release number of the operational software.
Image Upload	

Parameter	Description
Source	An option to select the firmware image file from a location (stored). This parameter supports the following options: • 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	This parameter is applicable only if you have selected **Local File** as the upload source. 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.
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 firmware images table. 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 checkbox to enable the device to reboot. When you select the checkbox, a message appears indicating that the device will reboot to install a firmware image.
Installable Images	List of images that are recently uploaded, with details of the latest uploaded image at the top row.

Parameter	Description

	You can upload multiple image files and manage them in this section.
	
	This parameter displays the following details for the uploaded images:
	
	• **Status**: Displays one of the following supported statuses of the image:
	  ◦ 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.
	
	To install an image file that you uploaded, click **Install** in the corresponding row of the required image file.
	
	To delete an image file that you uploaded, click **Erase** in the corresponding row of the required image file.

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

Configuration

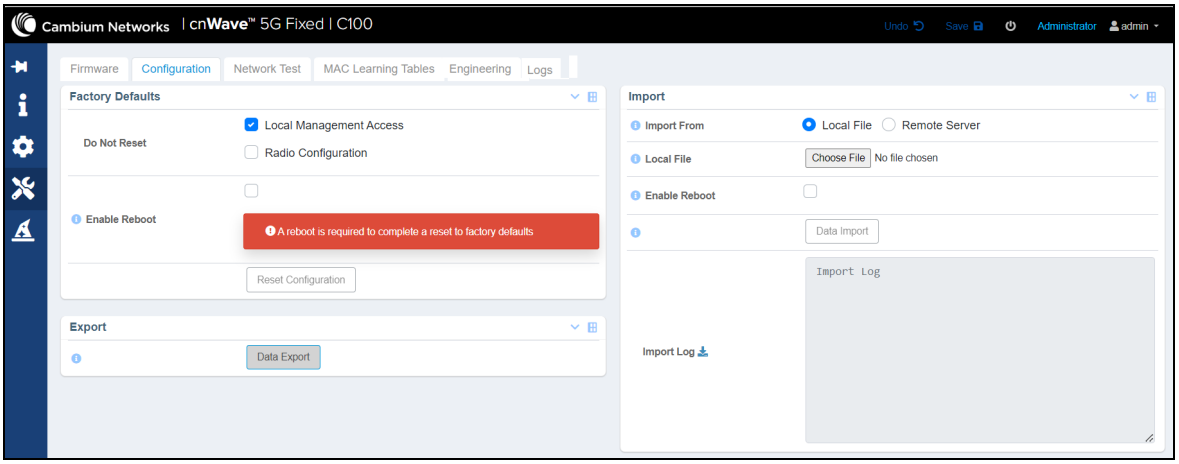
The **Configuration** page allows you to set the CPE to factory defaults. This page also allows you to import a saved configuration or export a CPE configuration for backup (restore). This Import feature exports or imports the date model configuration (and/or status) as a JSON file.

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

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

   The **Configuration** page appears, as shown in Figure 71.

Figure 71: *The Configuration page - C100 UI*



2. Set the values for parameters, as described in Table 46.

Table 46: List of parameters in the Configuration page

Parameter	Description
Factory Defaults	
Do not reset	Determines whether you want to reset the CPE to factory defaults. The following options are supported: • Local Management Access • Radio Configuration By default, the **Local Management Access** checkbox is selected. If you do not select the **Local Management Access** checkbox, then all the configuration data, including IP address, is wiped out and reset to 169.254.1.1. 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. If you select **Radio Configuration**, then all the configuration data is wiped out, except for the frequency data and local IP address.
Enable Reboot	Determines whether the device is enabled to reboot to complete the process of reset to factory defaults. Select the checkbox to enable the reboot for the device.
Reset Configuration	An option to reset the system to factory defaults.

Parameter	Description
	Click **Reset Configuration** if you want to reset the CPE to factory defaults.
Export	
Data Export	An option to export the data model configuration (and/or status) as a JSON file for backup (restore). When you click the **Data Export** button, the data model configuration is downloaded by the device.
Import	
Import From	An option to select a location (stored) from where you want to import the required data configuration. This parameter supports the following options: • **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. Select the required option. **Note**: When you select **Remote Server**, the  icon appears indicating to select the **Local File** option (if required).
Local File	To upload a local import file (internally), perform the following steps: a. Click **Choose File** in the Local File field. A file browser window appears. b. Browse the location where you have saved the import file (for example, a JSON file) on your machine locally. c. Select the file and click **Open**. The local import file is selected. d. To upload the import file, click **Data Import** in the **Configuration** page.
Server URL	This parameter is applicable only if you have selected **Remote Server** in the **Import From** field. To select the import file from a remote server, provide the server URL in the text box. Then, click the **Data import** button.
Enable Reboot	Determines whether the device is enabled to reboot to complete the import configuration process. Select the checkbox to enable the reboot for the device.

Parameter	Description
	Note: Reboot is applicable only to some configuration changes.
Data Import	An option to import the required data model configuration from a JSON file.
Import Log	An option to view and download the import logs from the C100 UI. Click the icon to download the import logs.

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

Network Test

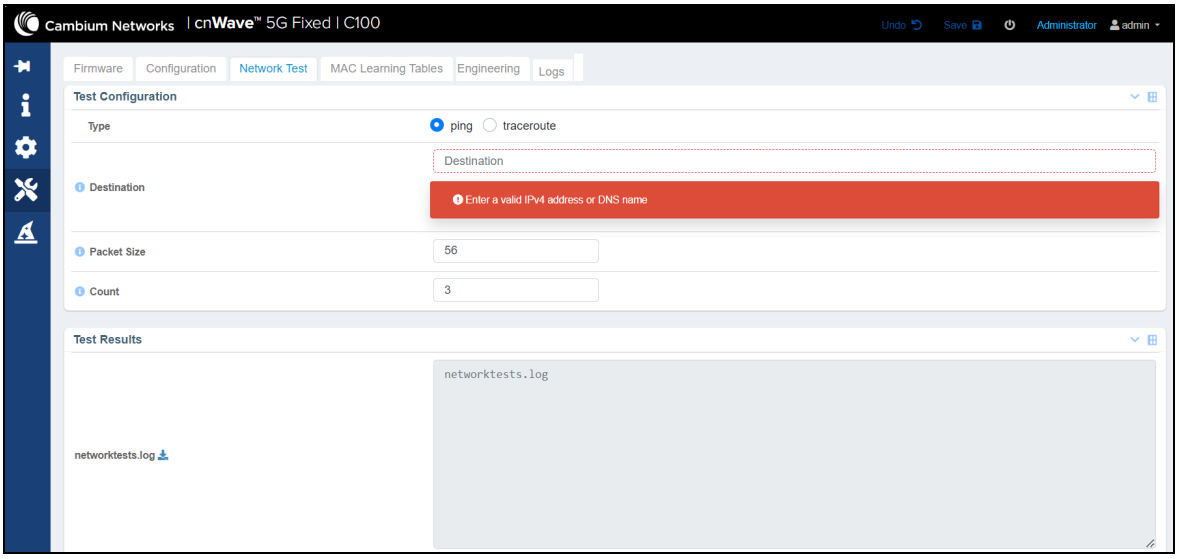
The **Network Test** is a network tool that helps you to test connectivity and accessibility of CPE to a radio network. This page allows you to ensure whether the CPE is correctly connected to your network. Example: CPE's connectivity to BTS or RADIUS Server. This network test helps in troubleshooting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

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

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

   The Network Test page appears, as shown in Figure 72.

   Figure 72: *The Network Test page - C100 UI*



2. View and set the values for parameters, as described in Table 47.

Table 47: Parameters in the Network Test page - C100 UI

Parameter	Description
Test Configuration	
Type	Determines the method used for testing a network. Following options are supported: • **ping**: The CPE pings the required destination (for example, BTS, cnMaestro, RADIUS Server, DNS, or a radio network) to ensure its connectivity. If the ping is successful, this implies that the CPE can access the BTS or the required network. • **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. 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. Choose the required test type. Figure 73 and Figure 74 are examples of ping and traceroute types.
Destination	The valid IPv4 address or a DNS name of the required destination. Provide an appropriate value in the text box.
Packet Size	Number of data bytes that has to be sent to the network. Default value: 56 data bytes, which are translated into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data. Provide the required value in the text box. **Note**: This parameter is not applicable if you select `traceroute` in the **Type** field.
Count	Number of ping packets that have to be sent to the network. Default value: 3 Provide the required value in the text box. **Note**: This parameter is not applicable if you select `Traceroute` in the **Type** field.
Run Test	An option to run the test.

Parameter	Description
	This option appears only when you provide a value in the **Destination** text box.
Stop Test	An option to stop the test that has begun. This option appears only when you run the test.
Test Results	
networktests.log	Displays the test results for the required destination. By default, this field is disabled. When you run the test, this field displays the test results. You can use the icon to download the log file.

Figure 73 is an example of a test result for the **ping** type:

Figure 73: *Test result - ping*

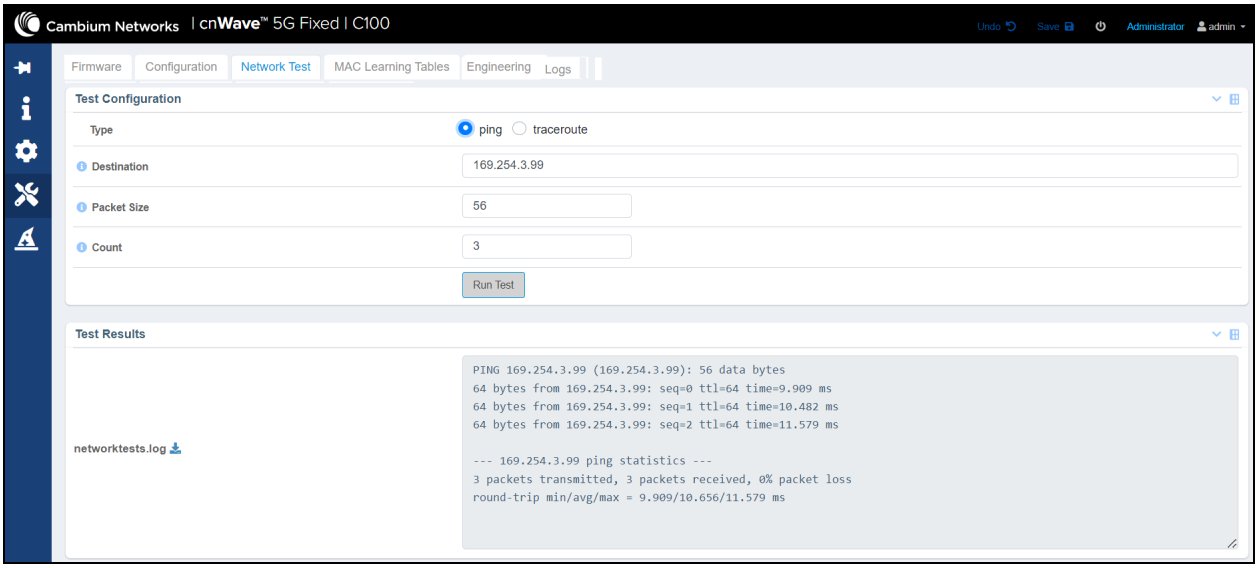
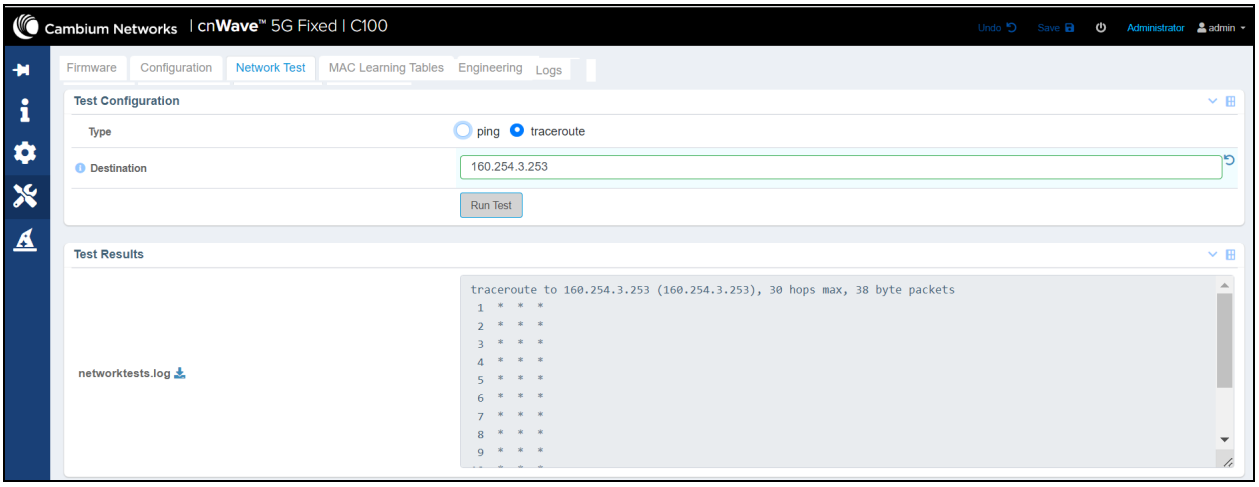


Figure 74 is an example of a test result for the **traceroute** type:

Figure 74: *Test result - traceroute*



MAC Learning Tables

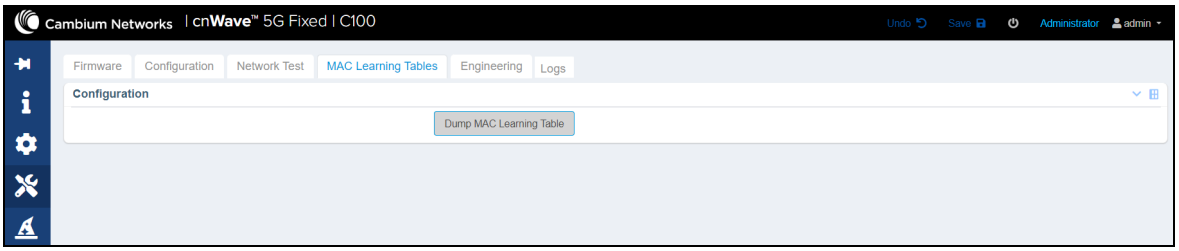
The **MAC Learning Tables** page allows you to dump the MAC addresses of equipment (or other devices) connected to the CPE radio units. You can also download the dumped MAC addresses in `.txt` file format.

To dump the MAC learning tables for CPEs, perform the following steps:

1. From the main C100 dashboard page, navigate to **Tools** > **MAC Learning Tables**.

   The **MAC Learning Tables** page appears, as shown in Figure 75.

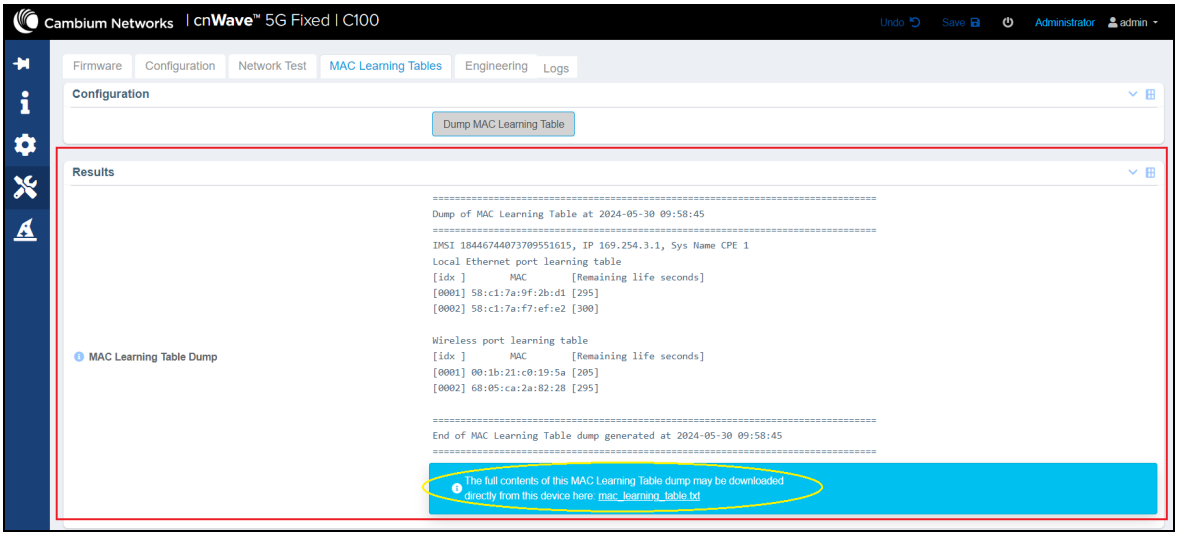
   Figure 75: *The MAC Learning Tables page - C100 UI*

2. In the **Configuration** section, click on the **Dump MAC Learning Table** button.

   The **MAC Learning Table Dump** parameter appears with the output in the **Results** section (as shown in Figure 76).

Figure 76: *A sample MAC table dump for CPE*



3. Download the `mac_learning_table.txt` file from the UI (if required).

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:

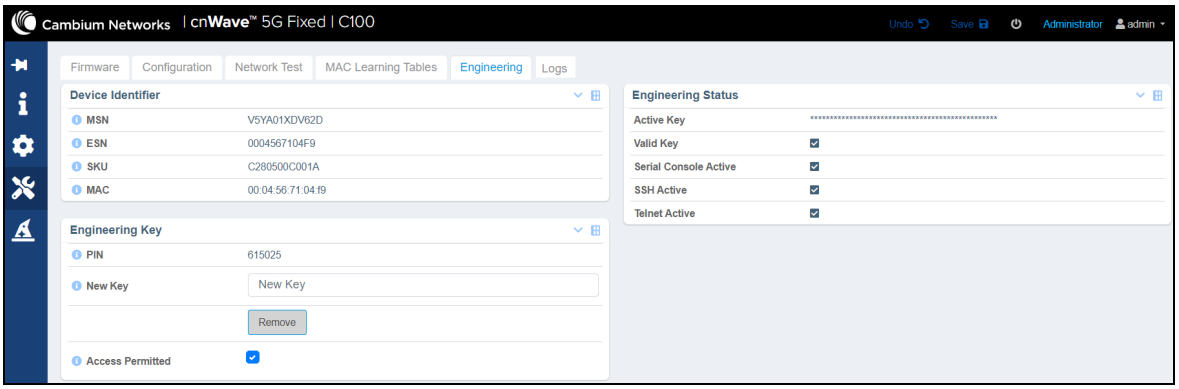
1. From the main C100 dashboard page, navigate to **Tools** > **Engineering**.

   The **Engineering** page appears, as shown in Figure 77..

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 77.

Figure 77: *The Engineering page - C100 UI*



2. View and set the values for parameters, as described in Table 48.

Table 48: 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.

Parameter	Description
	Select the checkbox 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.

Logs

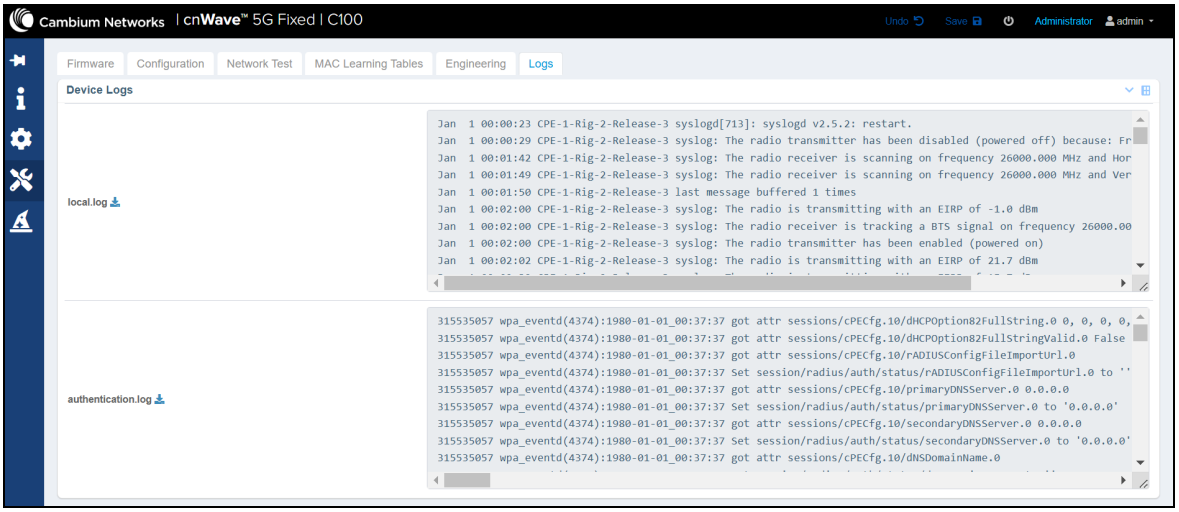
The **Logs** page allows you to view and download `local.log` and `authentication.log` files of CPEs. You can use these logs for troubleshooting.

To view and download the logs, complete the following steps:

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

   The **Logs** page appears, as shown in Figure 78. You can view the logs.

   Figure 78: *The Logs page - C100 UI*



2. Click the icon to download the logs.

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.

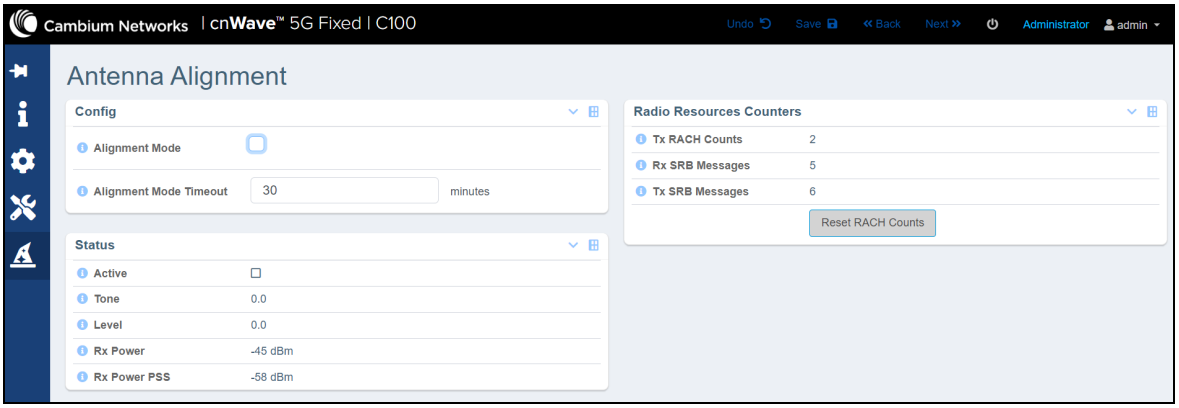
You can also use the **Set-up Wizard** icon ( ) to configure, view, and manage the setup wizard for CPEs.

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 79.

   Figure 79: *The Set-up Wizard page - C100 UI*



2. Set and view the details of parameters, as described in Table 49.

   Table 49: 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	

Parameter	Description
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). 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

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:

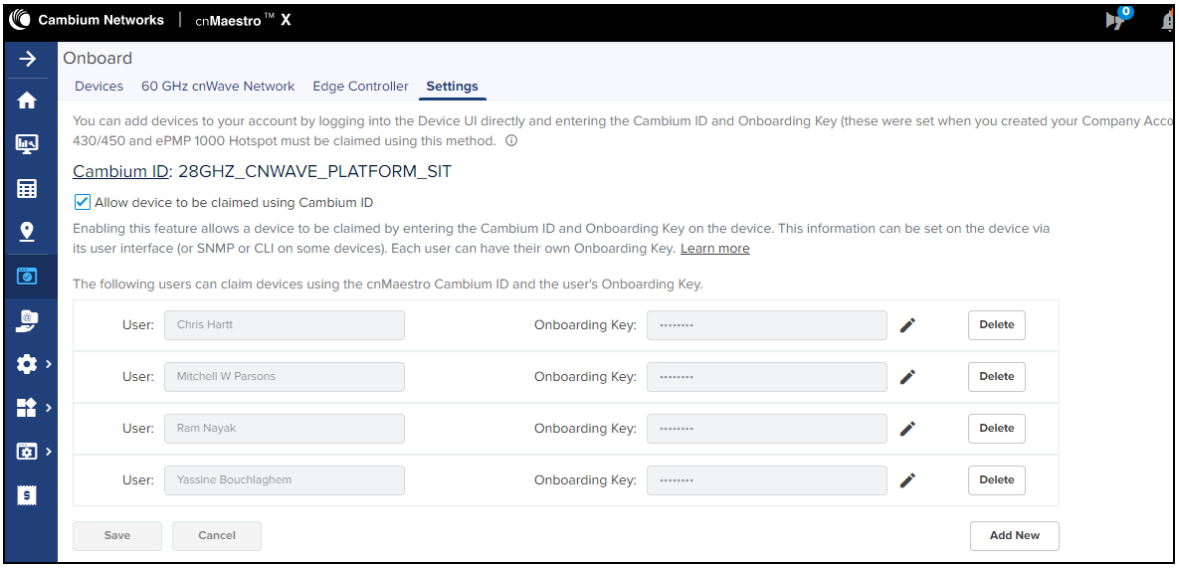
1. Log on to the cnMaestro X UI (cloud or on-premises) using appropriate username and password.

   The **cnMaestro X** home page appears.

2. From the home page, navigate to **Onboard** > **Settings**.

   The **Onboard** > **Settings** page appears, as shown in Figure 80.

   Figure 80: *The **Settings** page*



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

   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:

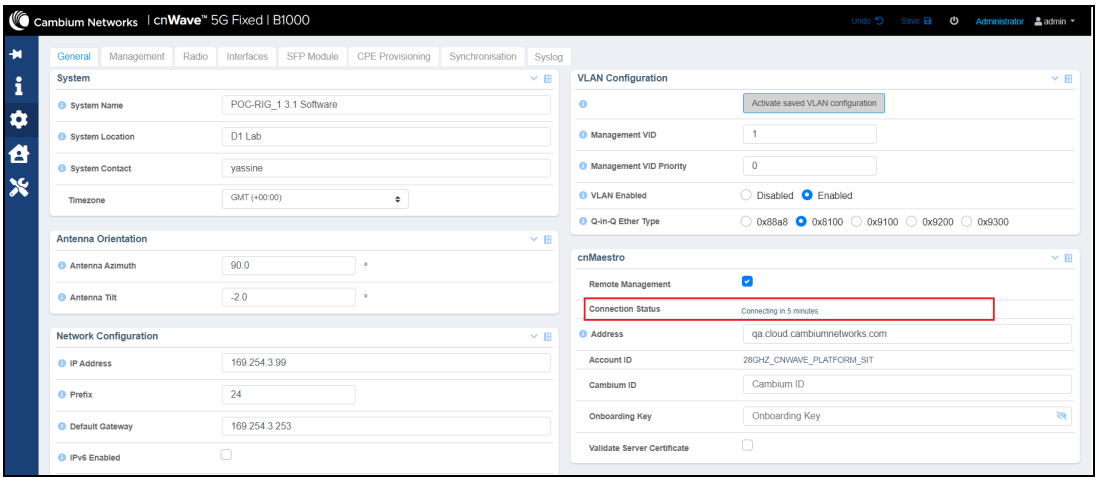
a. From the main B1000 dashboard page, navigate to **System** > **General**.

The **General** page appears, as shown in Figure 10.

b. In the **cnMaestro** section, Select the **Remote Management** checkbox.

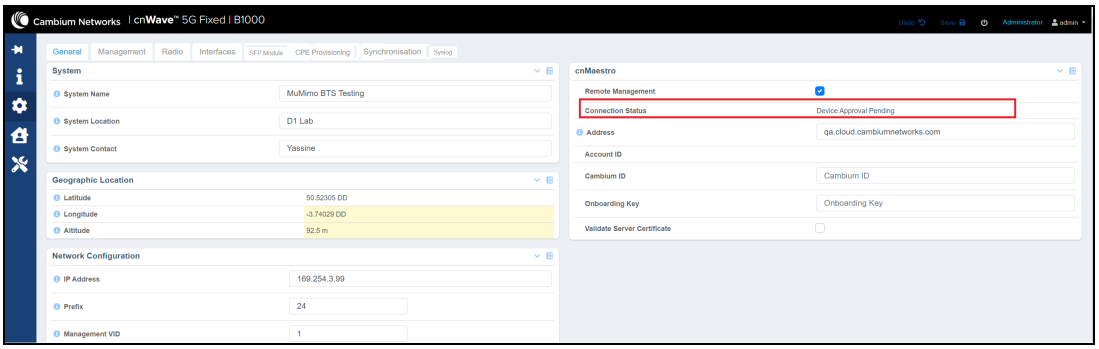
If everything works correctly at the background, the **cnMaestro** section displays the connection status (Connecting in 5 minutes) of the BTS system and cnMaestro-specific parameters (as shown in Figure 81).

Figure 81: *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 82).

Figure 82: *The Device Approval Pending status*

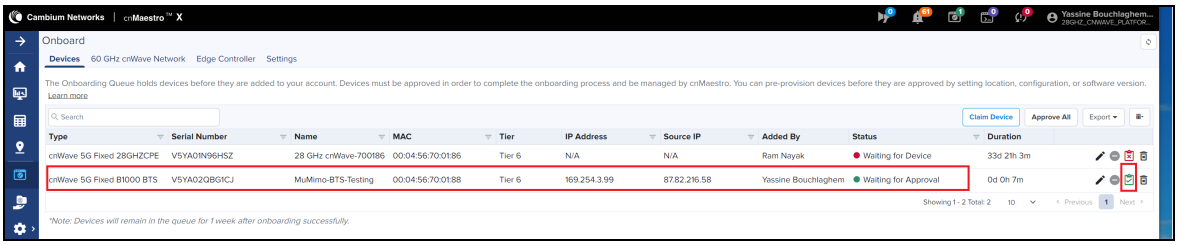


The BTS device needs approval for onboarding.

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 83).

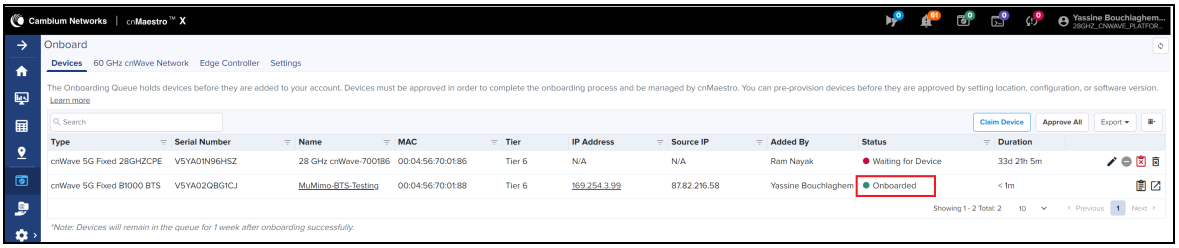
Figure 83: *The Waiting for approval status of the BTS device*



6. Select the tick box ( ) on the required corresponding row, as shown in Figure 83.

   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 84.

   Figure 84: *The Onboarded status of the BTS device*



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

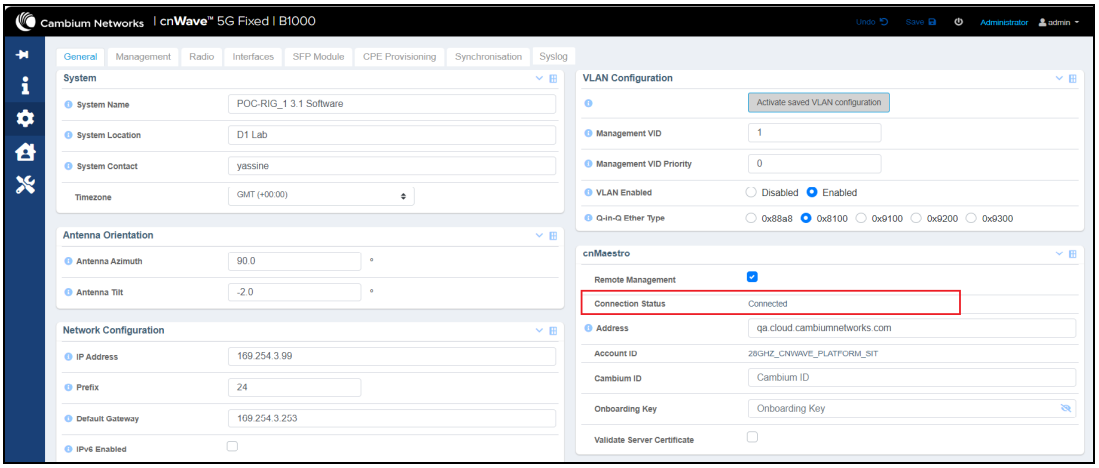
   a. In the **cnMaestro** section, enter the Cambium ID and the onboarding key that you set on the **Settings** page of cnMaestro UI.

      For more information about cnMaestro-specific parameters in the B1000 UI, refer to Table 8.

   b. Click **Save**.

      The **Connection Status** parameter in the **cnMaestro** section displays Connected, as shown in Figure 85.

Figure 85: *The connected status of the BTS device*

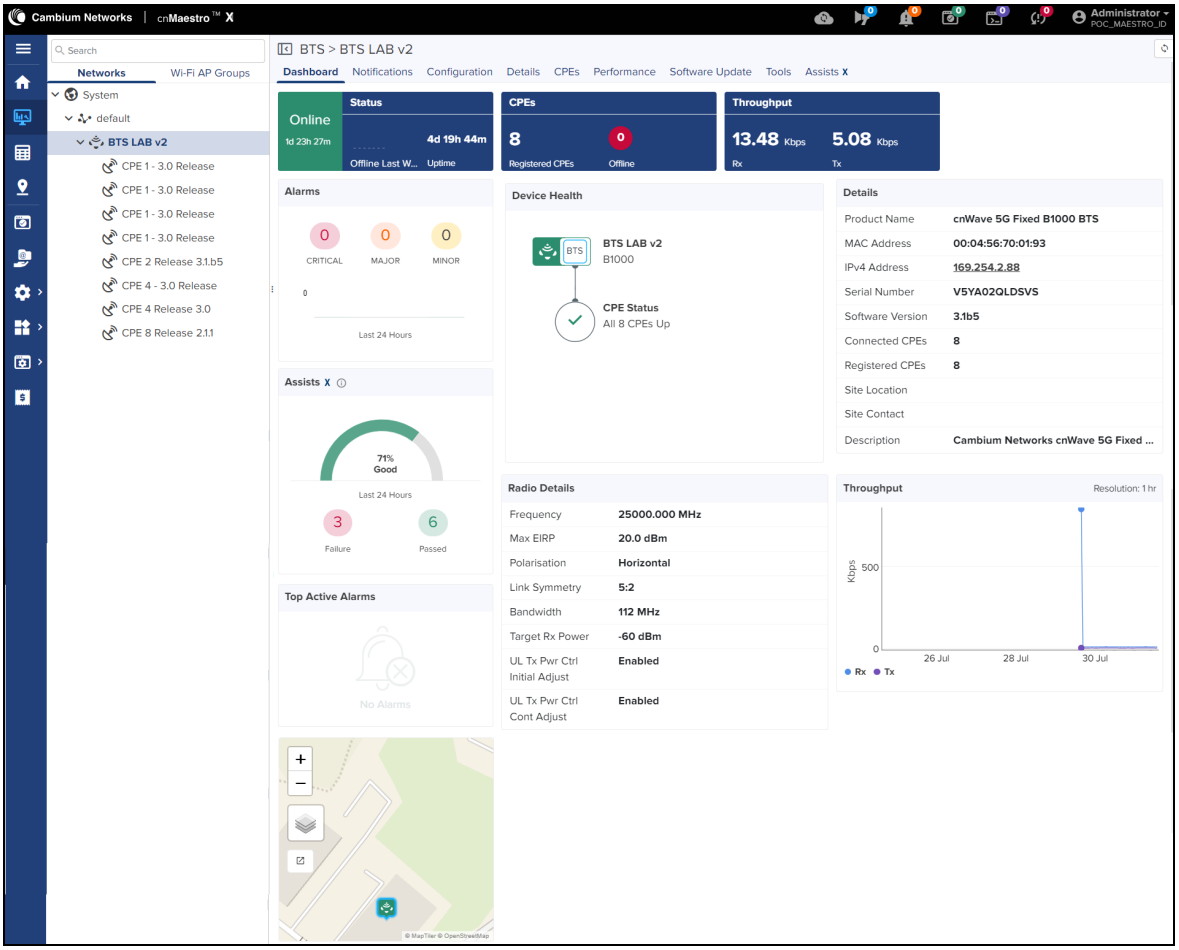


The BTS device has connected to cnMaestro, successfully.

8. 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 86), 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 86: *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 86.

Table 50 lists and describes the widgets available on the **Dashboard** page for the BTS and a CPE.

Table 50: 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

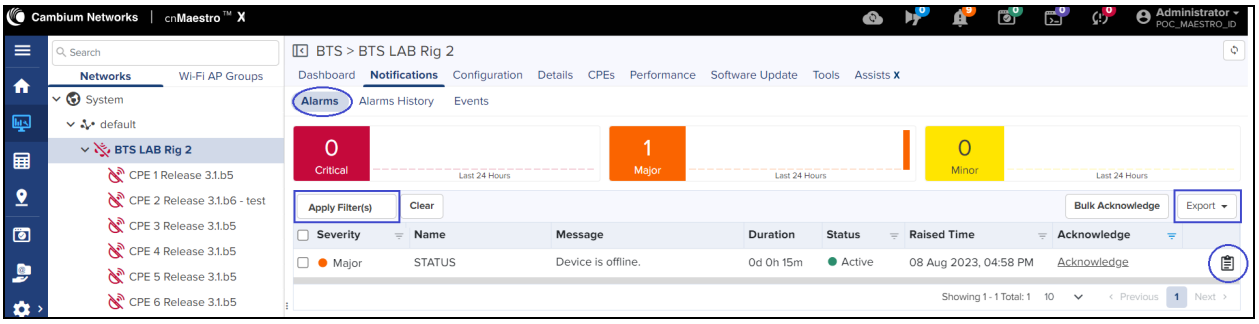
The **Notifications** page provides detailed information of alarms raised for the BTS or the CPE device. This page contains the following tabs:

- Alarms
- Alarm History
- Events

Alarms

The **Alarms** page displays the count of critical, major, and minor alarms in different colors (as shown in Figure 87). 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 87: *The Notifications > Alarms page*



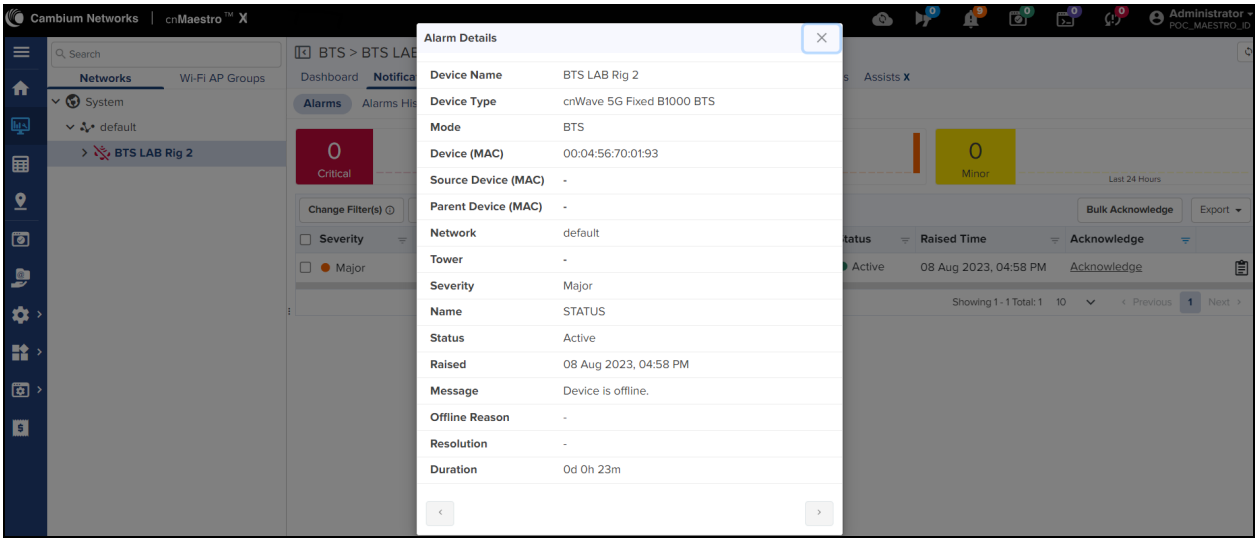
Using the **Apply Filter(s)** button, you can set and apply the following filters for viewing the alarm data in a table:

- 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 87).

When you click on the **View Details** icon (), the **Alarm Details** page appears (as shown in Figure 88). You can use this page to view the detailed information of an alarm.

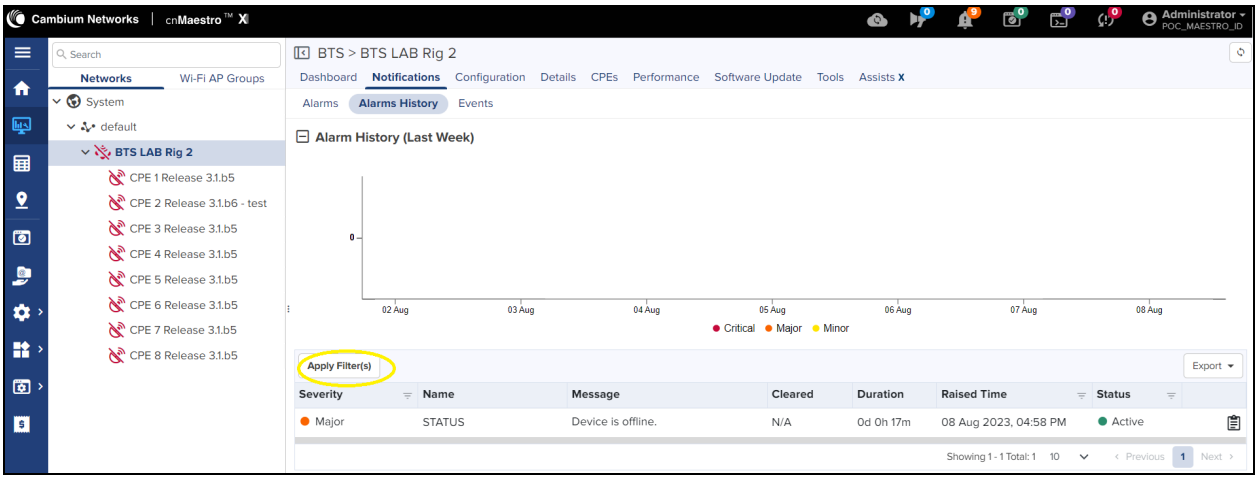
Figure 88: *The Alarm Details page*



Alarm History

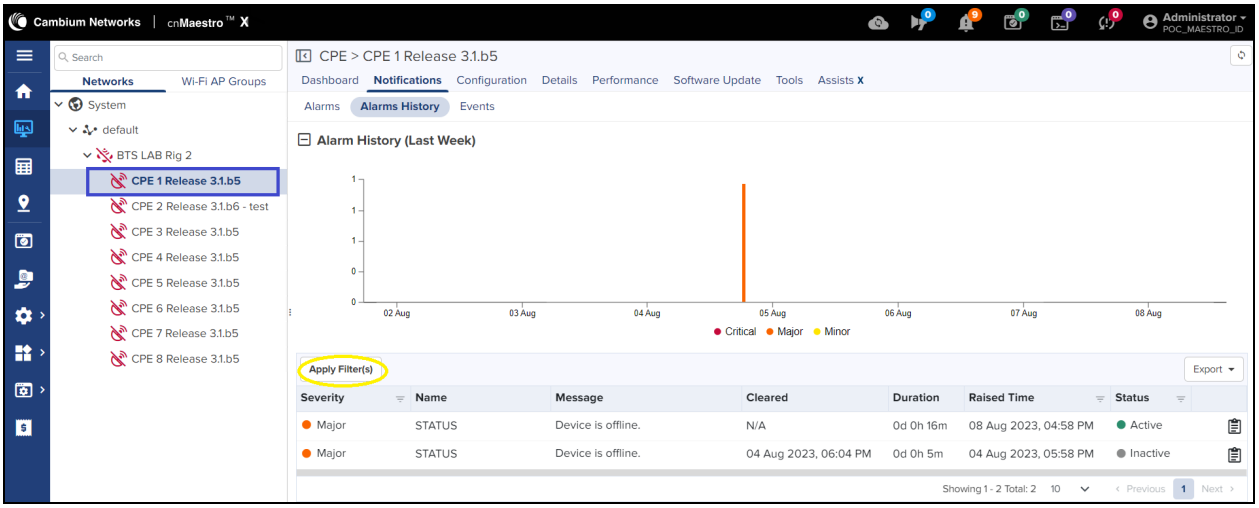
The Alarm History page displays the alarm data for the previous week in graph and table format (as shown in Figure 89).

Figure 89: *The Notifications > Alarms History page*



When you select a CPE , the **Alarms History** page displays data as shown in Figure 90.

Figure 90: *The alarm history for a CPE (offline)*

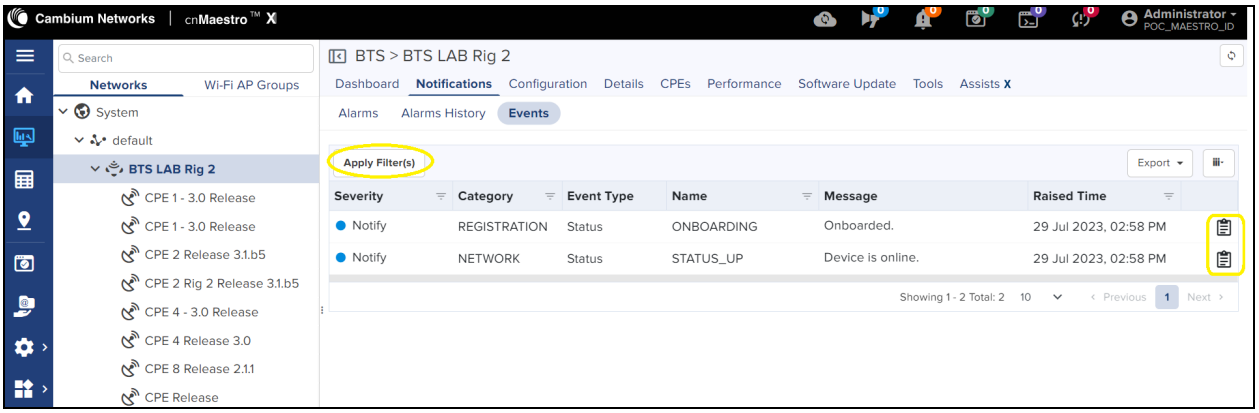


Use the **Apply Filter(s)** button to set and apply filters for viewing alarm data in the table.

Events

The **Events** page displays detailed information of alarms in a table format, as shown in Figure 91.

Figure 91: *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 detailed information about an event.

Configuration

The **Configuration** page allows you to configure the device settings, as shown in Figure 92.

Figure 92: *The Configuration page*

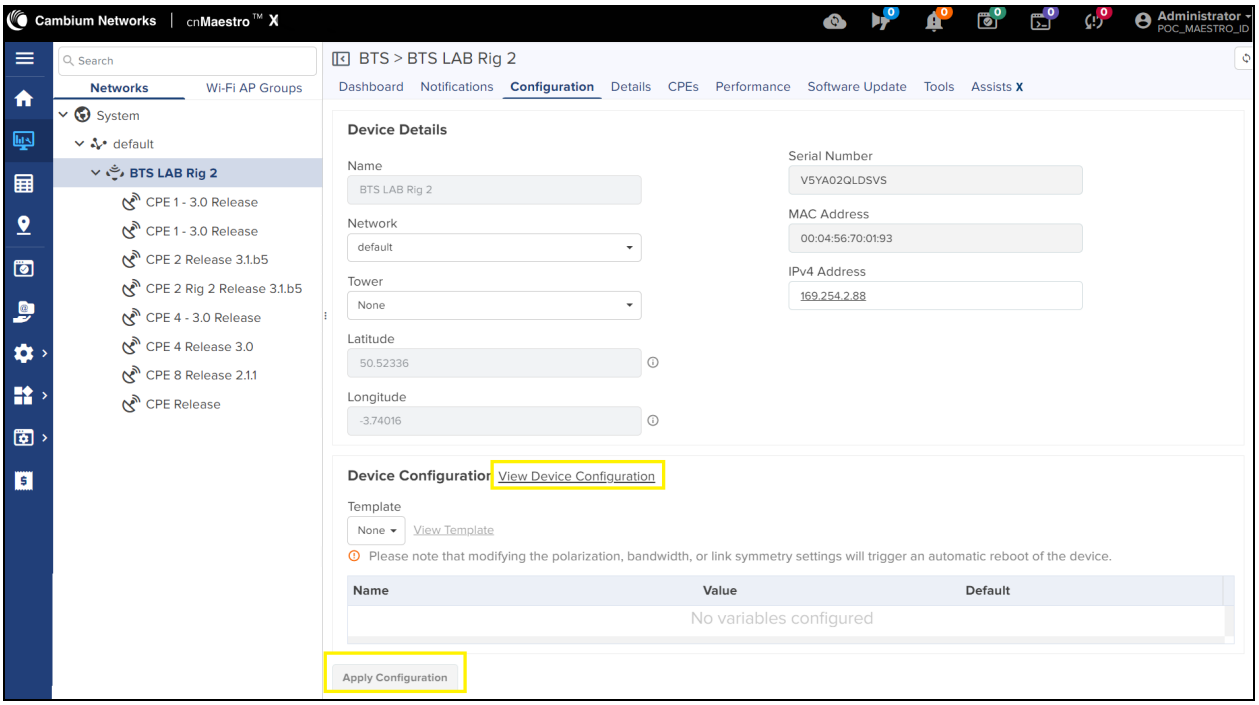


Table 51 lists and describes the parameters available on the **Configuration** page.

Table 51: 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.

Parameter	Description
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.
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

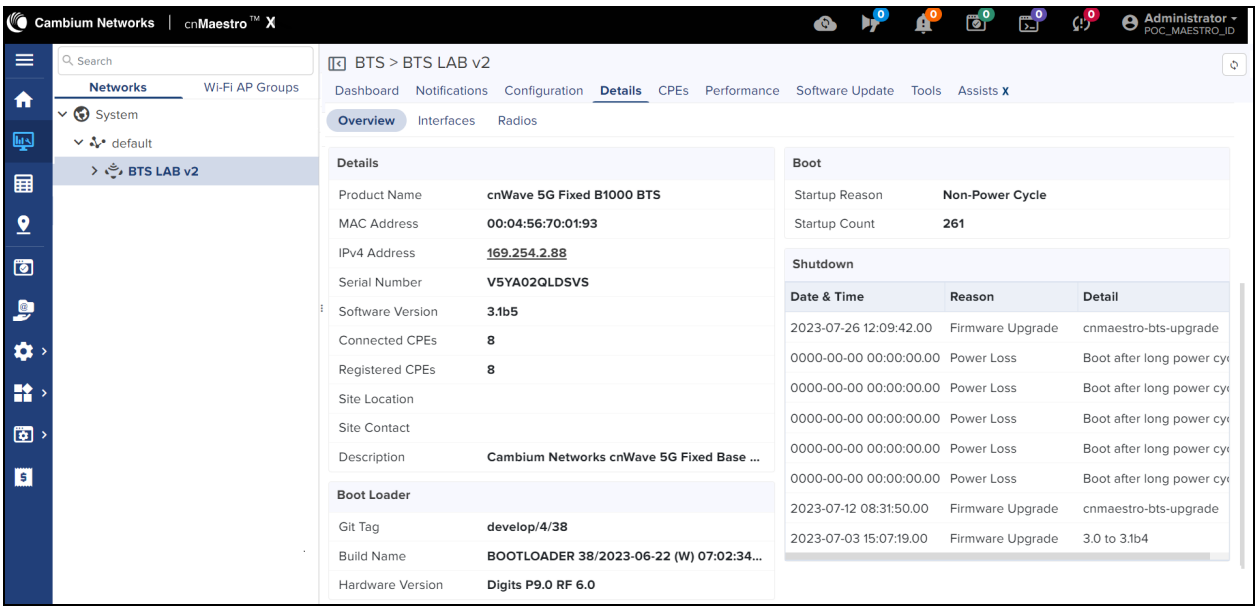
The **Details** page provides an overview, interface, and the radio details of the BTS or CPE device. This page contains the following tabs:

- 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 93).

Figure 93: *The Details > Overview page for the BTS*

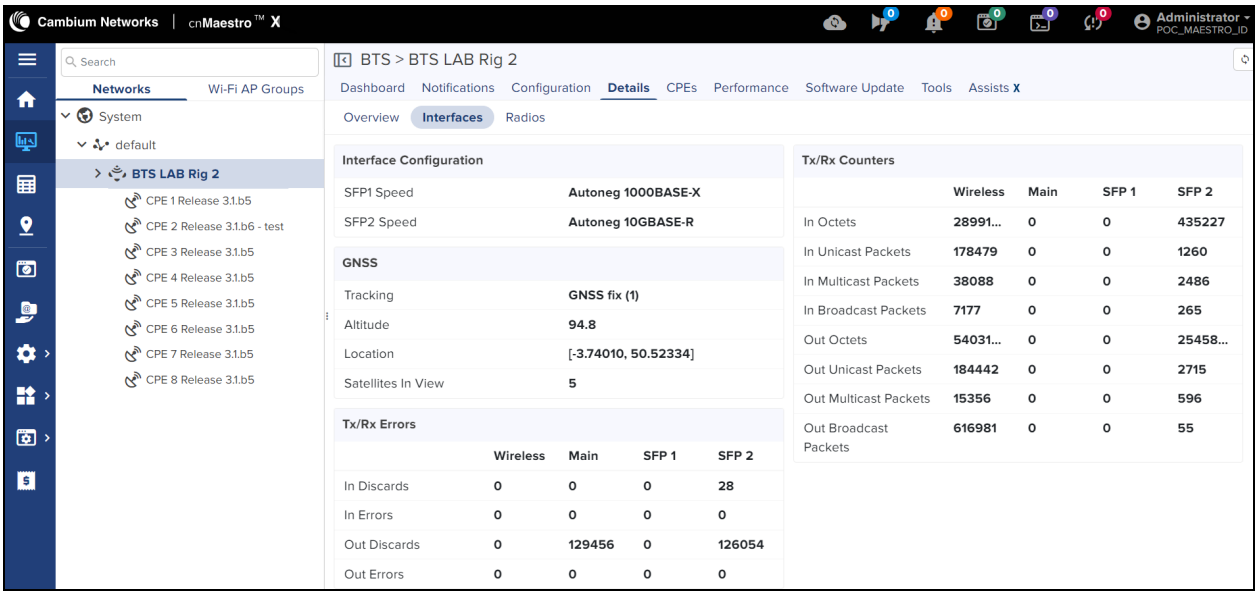


For each CPE, the **Overview** page displays device, radio, and session details. For information on parameters available of the **Overview** page, refer to Table 5 in the Device section.

Interface

The Interface page displays the radio interface configuration details of the BTS or the CPE device (as shown in Figure 94).

Figure 94: *The Details > Interface page for the BTS*

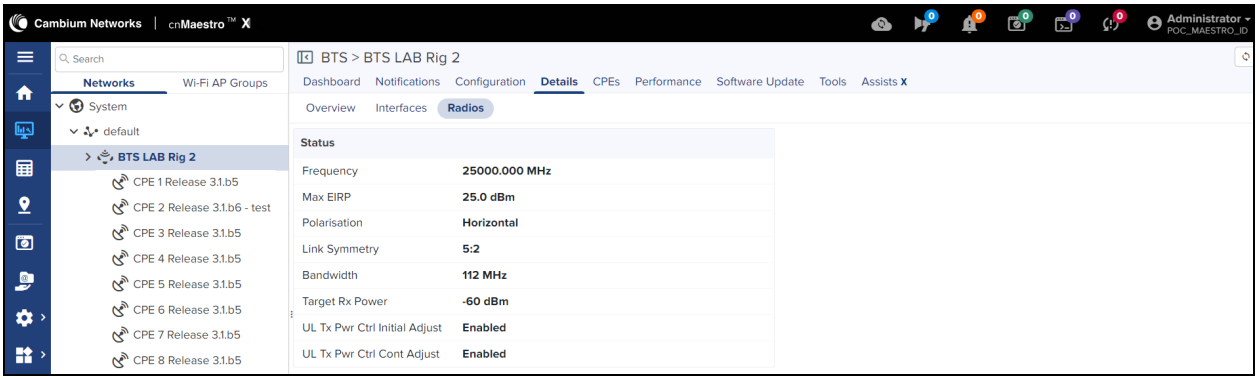


For each CPE, the **Interface** page displays Ethernet and wireless interface related details.

Radio

The **Radio** page displays the radio status of the BTS or the CPE device (as shown in Figure 95). Example: Frequency, Polarisation, link symmetry, and bandwidth details of the BTS.

Figure 95: *The Details > Radio page for the BTS*

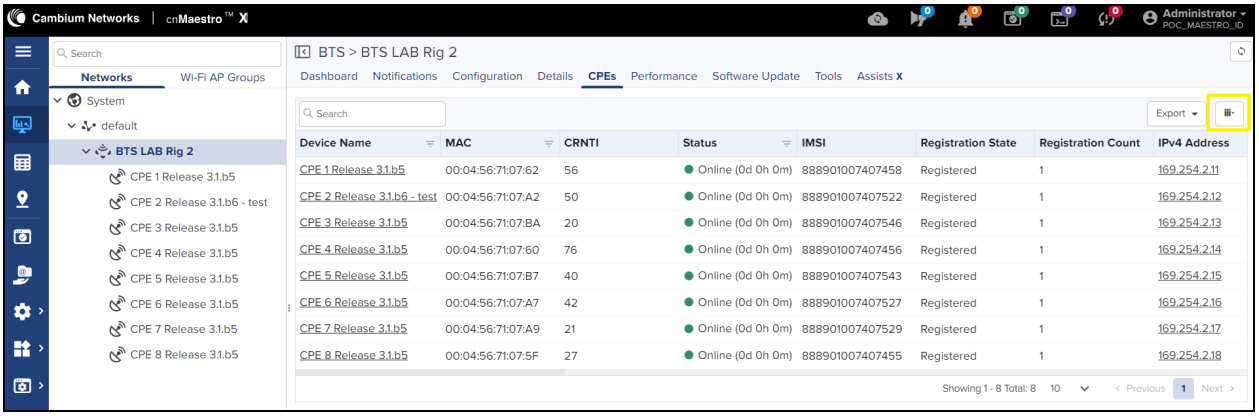


For each CPE, the **Radio** page displays radio interface related details such as alignment active, range, current EIRP, UL sounding state and DL sounding state.

CPEs

The **CPEs** page provides information on all the connected and registered CPEs with the BTS (as shown in Figure 96). The **CPEs** page is applicable only to the BTS.

Figure 96: *The CPEs page*

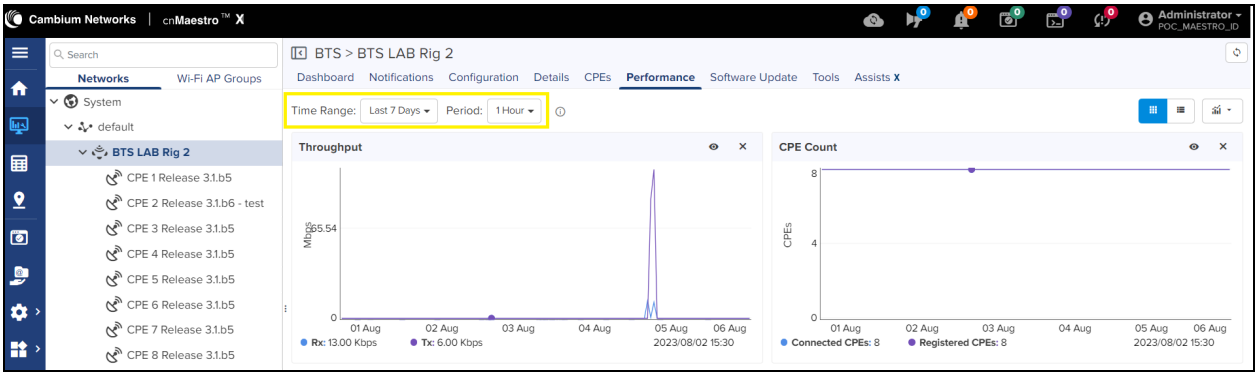


Use the **column Selector** icon (⫼) to choose the required parameters and view the CPE data. For information on parameters available on the **CPEs** page, refer to the Viewing Subscriber (CPE) Data section.

Performance

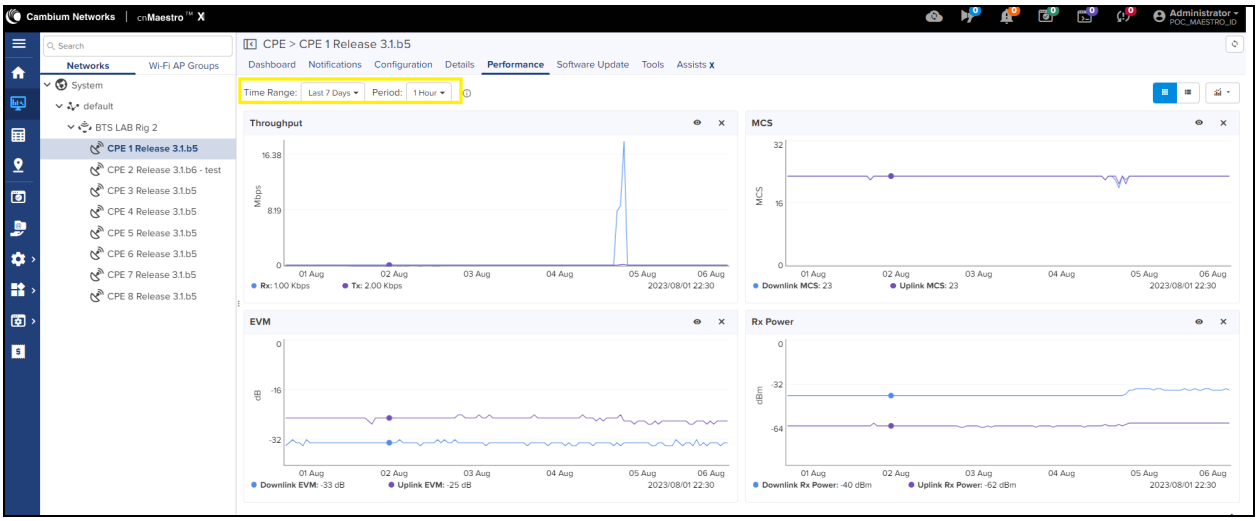
The **Performance** page displays the BTS throughput and count of CPEs for the selected time range and period in a g graph format (as shown in Figure 97). Use T**ime Range** and **Period** filters to view the performance data for the required period (for example, last 7 days and 1 hour).

Figure 97: *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 98).

Figure 98: *The Performance page for each CPE*



Software Upgrade

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

Note

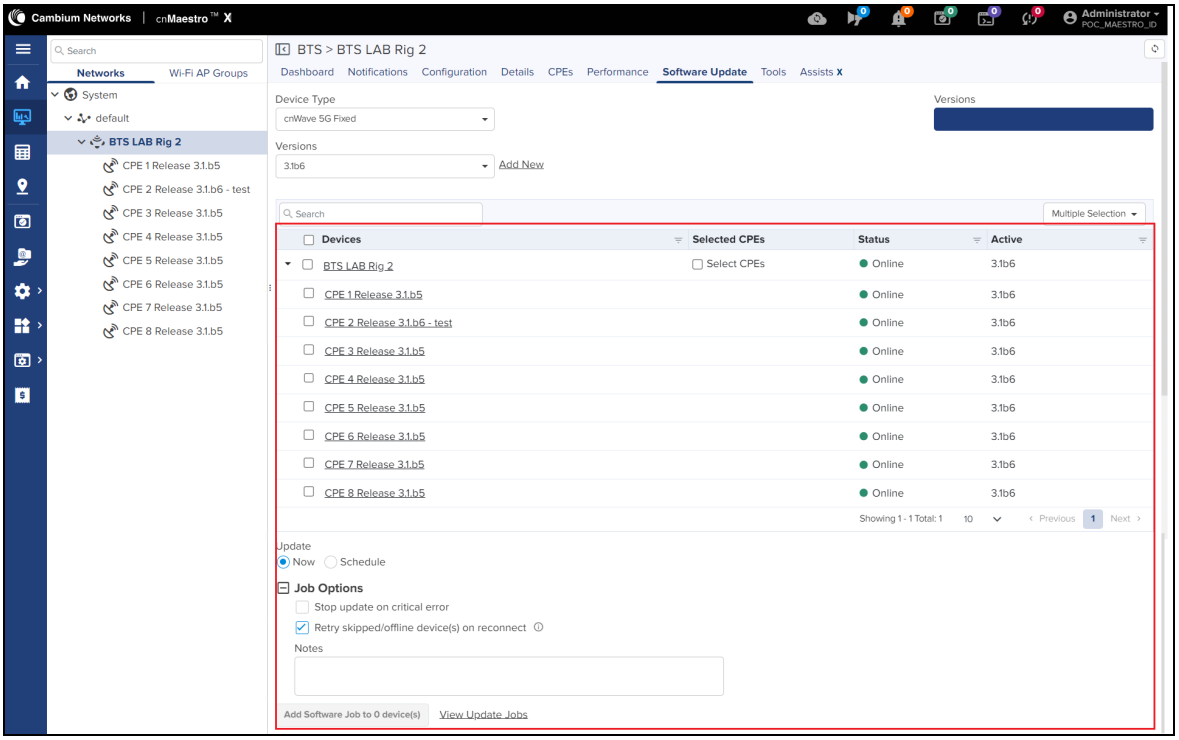
Software upgrade or downgrade using cnMaestro X is applicable only to cnWave™ 5G Fixed release 2.1 version and later versions.

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 99.

Figure 99: *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 checkbox against the required device names, for which you want to schedule this activity, in the **Devices** section (as shown in Figure 99).

    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** checkbox.

    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:

a. From the home page of cnMaestro UI, navigate to **Administration** > **Jobs** > **Software Update** page.

b. On the **Software Update** page, select either **Manual** or **Auto** option.

c. Select the checkbox against the required device name and details.

d. 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

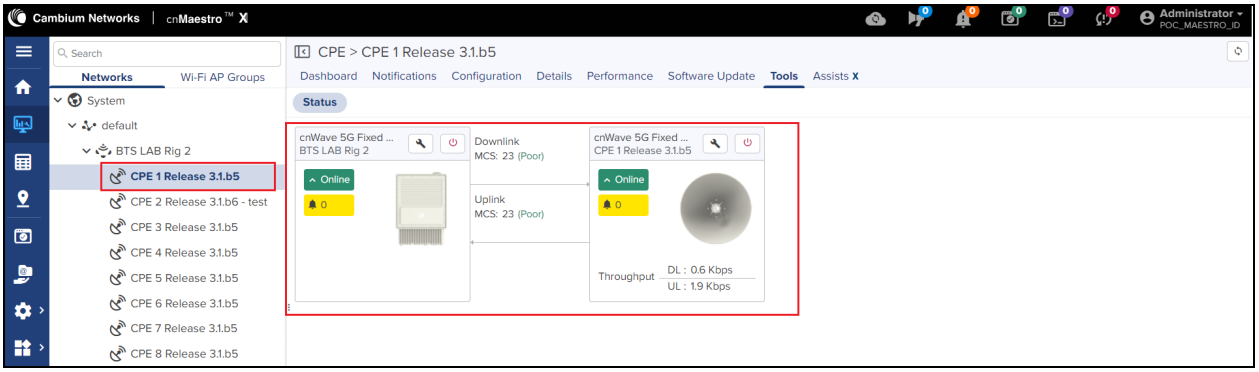
The **Tools** page contains the following tabs:

- 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 100 is an example of the CPE connection state

Figure 100: *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 101.

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

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

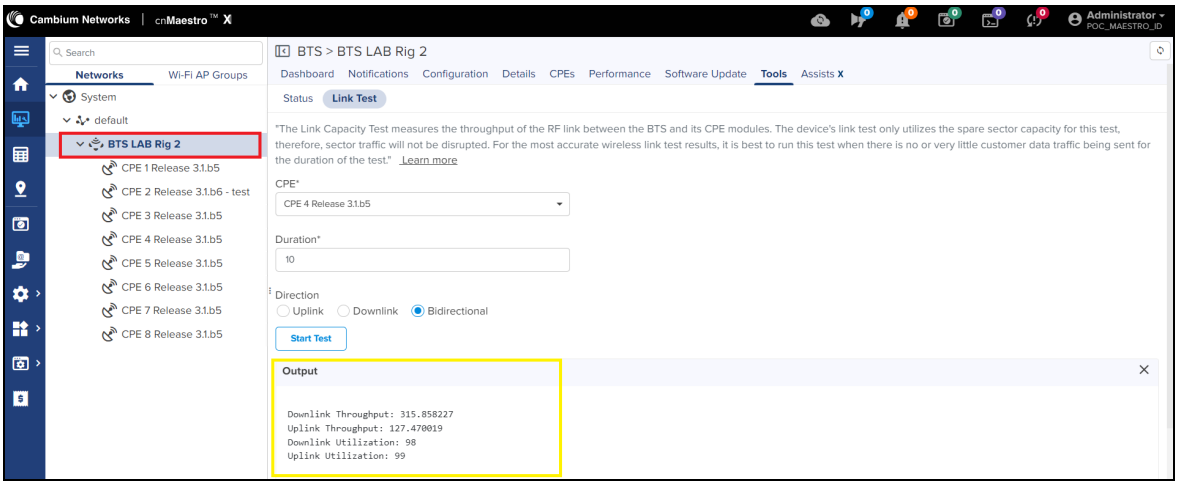
   The **Duration** parameter supports values from 0 to 60 (in seconds).
3. From the **Direction** parameter options, select the direction of transmission of the traffic that you want to test.

   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 101.

   Figure 101: *The Links Test page - cnMaestro X UI*

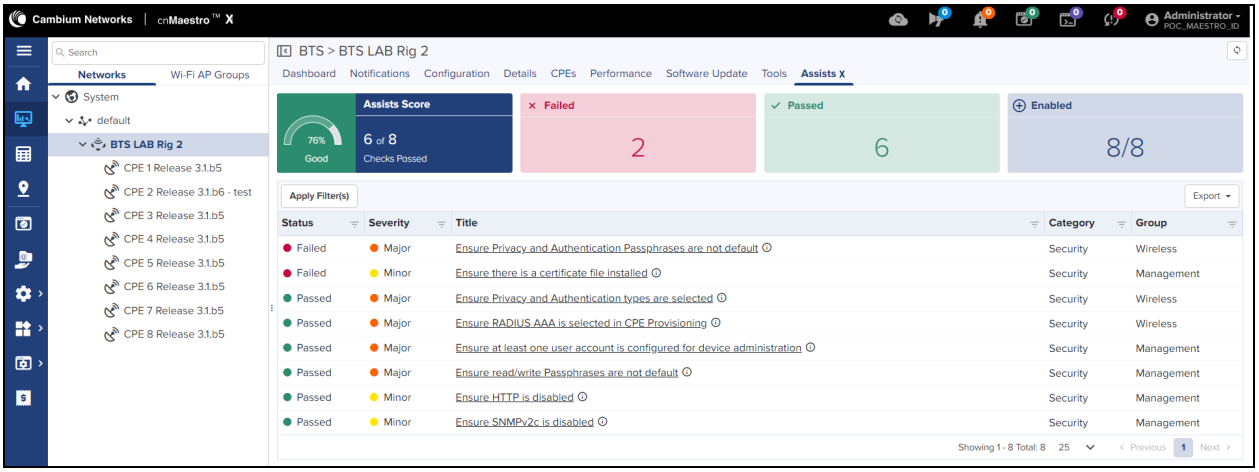


You can also test the link capacity of a CPE using the B1000 UI (BTS). For more information, refer to the Link Capacity Test section.

Assists X

The Assists X page displays statistics of failed and passed events for the BTS and CPEs. Figure 102 is an example of failed and passed event statistics for BTS.

Figure 102: *The Assists X page*



Generating data reports

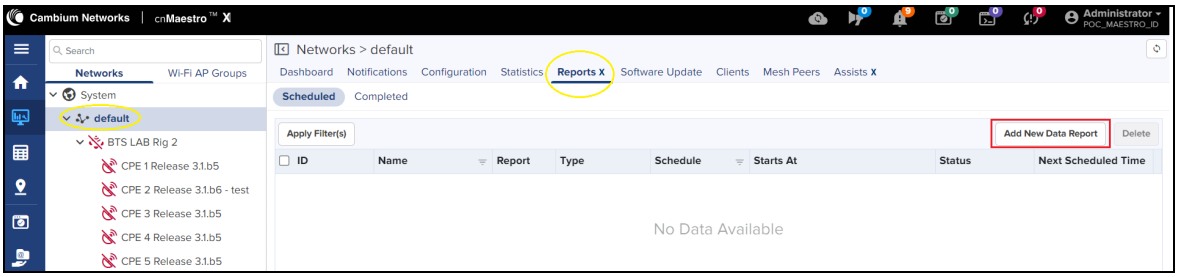
You can generate time-based data reports for cnWave 5G Fixed devices using the **Reports X** page in cnMaestro X UI. These reports help in administering and managing BTS and CPE devices.

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 103.

   Figure 103: *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 104.

Figure 104: *Parameters on the Add Report page*

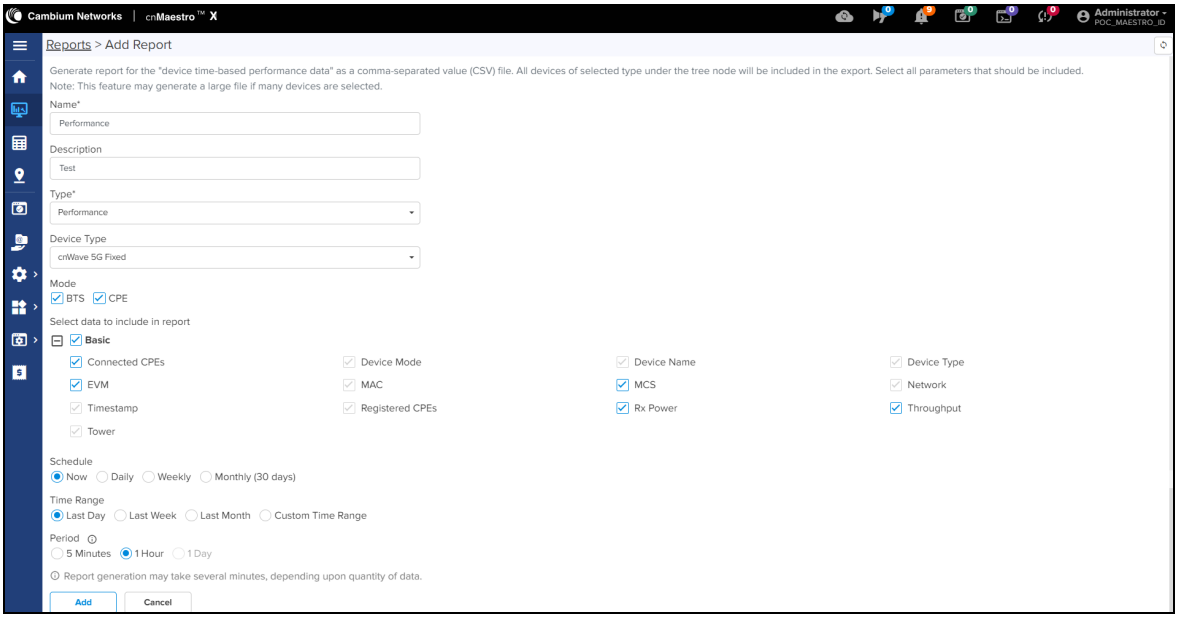


Table 52 lists and describes the parameters on the **Add Report** page.

Table 52: Parameters for generating a report

Parameter	Description
Name	Name of the report that you want to generate. This is a mandatory field. Provide an appropriate name in the text box. Example: Performance
Description	A brief description of the report.
Type	The report type that you want to generate. The following options are supported: • Devices • Performance • Active Alarms • Alarm History • Events • Clients • Mesh Peers Select the required report type from the drop-down list. This is a mandatory field.

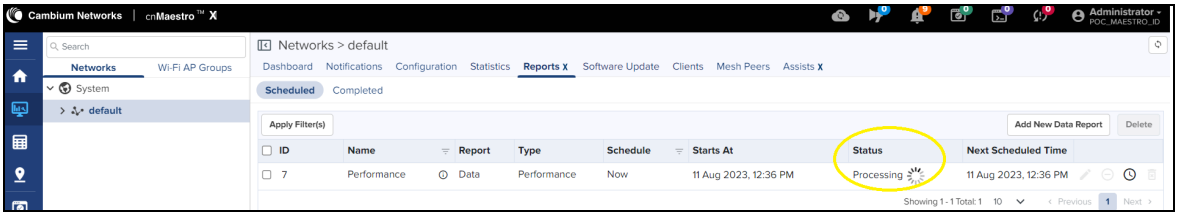
Parameter	Description
Device Type	The device for which you want to generate the report. The value of this parameter must always be **cnWave 5G Fixed**. Select the device name from the drop-down list.
Mode	The device mode for which you want to generate the report. Select BTS, CPE or both (if required).
Select data to include in report	Check the device-specific parameters that you want to include in the report. Example: Connected CPEs, EVM. The report, when generated, displays these parameters in CSV format.
Schedule	Time at when you want to generate the report. The following options are supported: • Now • Daily • Weekly • Monthly Choose the option. **Note**: When you select Daily, Weekly, or Monthly, ensure to specify the 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. The following options are supported: • 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. The following options are support: • 5 Minutes • 1 Hour

Parameter	Description
	• 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 105.

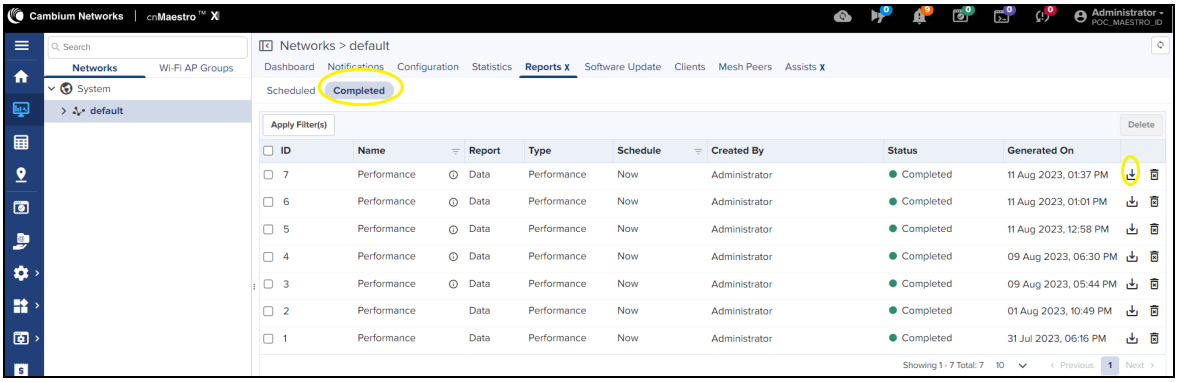
   Figure 105: *The report scheduled status*



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 106.

   Figure 106: *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 53 lists acronyms and abbreviations used in this guide.

Table 53: 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

Term	Definition
PC	Personal computer
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™ www.cambiumnetworks.com