





# USER GUIDE

cnPilot Enterprise Wi-Fi Access Points

System Release 4.2



#### Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. 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 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 3<sup>rd</sup> Party software products described in this document may include or describe copyrighted Cambium and other 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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"). 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.

© 2021 Cambium Networks Limited. All Rights Reserved.

## Contents

| Contents                                | n  |
|---|----|
| Contents                                |    |
| List of Figures                         |    |
| List of Tables                          |    |
| Upgrade/Downgrade Guidelines            |    |
| Section-1                               | 15 |
| Section-2                               | 15 |
| Chapter 1: About This User Guide        | 17 |
| Overview of cnPilot products            | 17 |
| Intended audience                       | 17 |
| Purpose                                 | 17 |
| Related documents                       | 17 |
| Features and Enhancements               |    |
| System Release 3.11.4                   |    |
| System Release 4.0                      |    |
| Supported hardware platforms            |    |
| New hardware platforms                  |    |
| Chapter 2: Quick Start - Device Access  |    |
| Powering up the device                  |    |
| PoE switches (802.3af/802.3at)          |    |
| PoE adapter                             | 21 |
| Accessing the device                    | 22 |
| Device access using default/fallback IP | 22 |
| Device access using zeroconf IP         | 23 |
| Device access using DHCP IP address     |    |
| LED status                              |    |
| Chapter 3: Device Modes                 | 27 |
| cnMaestro managed mode                  | 27 |
| Autopilot mode                          | 27 |
| Standalone mode                         | 27 |
| Chapter 4: cnMaestro Onboarding         |    |
| Overview                                |    |
| Device Onboarding and Provisioning      |    |
| Onboarding to cnMaestro cloud using MSN |    |
| Onboarding to cnMaestro On-Premises     |    |

| Auto-Provisioning  |    |
|--|----|
| Other options  |    |
| Directing devices to the cnMaestro On-Premises server using DHCP |    |
| Claim using Cambium ID   |    |
| Claim through static URL without Cambium ID and onboarding key   |    |
| Claim through static URL with Cambium ID and onboarding key      |    |
| Chapter 5: UI Navigation   |    |
| Login screen   |    |
| Home page (Dashboard)  |    |
| Monitor  |    |
| Configure  |    |
| Operations   | 40 |
| Troubleshoot   |    |
| Chapter 6: Configuration - System                                |    |
| System   | 41 |
| Management   |    |
| Time settings  |    |
| Event Logging  |    |
| Chapter 7: Configuration - Radio                                 |    |
| Overview   |    |
| Configuring Radio parameters                                     |    |
| Chapter 8: Configuration - Wireless LAN                          | 55 |
| Overview   | 55 |
| Configuring WLAN parameters                                      | 55 |
| Chapter 9: Configuration - Network                               |    |
| Overview   |    |
| Configuring Network parameters                                   |    |
| IPv4 network parameters  |    |
| IPv6 network parameters  |    |
| General network parameters                                       |    |
| Ethernet Ports   |    |
| Security   |    |
| DHCP   |    |
| Tunnel   |    |
| PPPoE  |    |
| VLAN Pool  |    |
| WWAN   |    |

| Chapter 10: Configuration - Services |  |
|--------------------------------------|--|
| Overview                             |  |
| Configuring Services                 |  |
| LDAP                                 |  |
| APIs                                 |  |
| NAT Logging                          |  |
| Location API                         |  |
| BT Location API                      |  |
| Speed Test                           |  |
| DHCP Option 82                       |  |
| Chapter 11: Operations               |  |
| Overview                             |  |
| Firmware update                      |  |
| System                               |  |
| Configuration                        |  |
| Chapter 12: Troubleshoot             |  |
| Logging                              |  |
| Events                               |  |
| Debug Logs                           |  |
| Radio Frequency                      |  |
| Wi-Fi Analyzer                       |  |
| Spectrum analyzer                    |  |
| Unconnected clients                  |  |
| Packet capture                       |  |
| Performance                          |  |
| Wi-Fi Perf speed test                |  |
| Speedtest on Access Point            |  |
| Connectivity                         |  |
| Chapter 13: Management Access        |  |
| Local authentication                 |  |
| Device configuration                 |  |
| SSH-Key authentication               |  |
| Device configuration                 |  |
| SSH Key Generation                   |  |
| RADIUS authentication                |  |
| Device configuration                 |  |
| Chapter 14: Mesh                     |  |

| Mesh configurable parameters                      |  |
|---|--|
| Mesh link   |  |
| Order of Mesh profile configuration               |  |
| VLAN 1 as management interface                    |  |
| Non-VLAN 1 as management interface                |  |
| Chapter 15: Autopilot                             |  |
| Configuration and Onboarding                      |  |
| Configure member AP to Autopilot master           |  |
| Configuring WLAN in default WLAN Group            |  |
| Configuring WLANs with user created WLAN Group    |  |
| WLAN group override                               |  |
| Configuring WPA2-Enterprise WLAN                  |  |
| Onboard member APs to Autopilot master            |  |
| Connect clients to the WLANs and check statistics |  |
| Manage Autopilot                                  |  |
| Firmware  |  |
| System  |  |
| Access Point Management                           |  |
| Tools   |  |
| Dashboard   |  |
| Overview  |  |
| Access Points                                     |  |
| Wireless clients                                  |  |
| Wireless LANs                                     |  |
| Insight   |  |
| Pulse   |  |
| Timeview  |  |
| Events  |  |
| Chapter 16: Guest Access Portal- INTERNAL         |  |
| Introduction                                      |  |
| Configurable Parameters                           |  |
| Access policy                                     |  |
| Splash page                                       |  |
| Redirect Parameters                               |  |
| Success Message                                   |  |
| Timeout   |  |
| MAC Authentication fallback                       |  |
| Extended interface                                |  |

| Whitelist                                      |     |
|--|-----|
| Captive portal bypass user agent               |     |
| Configuration examples                         |     |
| Access Policy - Clickthrough                   |     |
| Access Policy - Radius                         |     |
| Access Policy - LDAP                           |     |
| Access Policy - Local Guest Account            |     |
| Chapter 17: Guest Access Portal- EXTERNAL      |     |
| Introduction                                   |     |
| Configurable Parameters                        |     |
| Access policy                                  |     |
| WISPr  |     |
| External Portal Post Through cnMaestro         |     |
| External Portal Type                           |     |
| Redirect Parameters                            |     |
| Success Message                                |     |
| Timeout  |     |
| MAC Authentication fallback                    |     |
| Extended interface                             |     |
| Whitelist                                      |     |
| Captive portal bypass user agent               |     |
| Configuration examples                         |     |
| Access Policy - Clickthrough                   |     |
| Chapter 18: Guest Access – cnMaestro           |     |
| Configurable Parameters                        |     |
| cnPilot  |     |
| cnMaestro                                      |     |
| Configuration examples                         | 246 |
| Free   | 247 |
| Free – Custom fields                           | 250 |
| Free – Social Login                            |     |
| Free - SMS Authentication                      |     |
| Paid - Payment Gateway                         |     |
| Vouchers                                       |     |
| WiFi4EU  |     |
| Chapter 19: Policy Based VLAN Assignment (PBA) |     |
| Introduction                                   |     |
| Chapter 20: Device Recovery Methods            |     |
|  |     |

# Upgrade/Downgrade Guidelines

### Section-1

Mandatory image extension verification to follow while upgrade/downgrade from **4.x to 4.x, 3.11.x to 4.x and vice versa**. This procedure is applicable on cnMaestro (On-Premise recommended version is 2.2.1-r36 and above) and standalone AP UI/CLI. This procedure will **not be applicable on cnMaestro-Cloud**, since image upgrade/downgrade is automatic for APs.



#### Note

This recommendation is applicable for all models of cnPilot APs.

Refer the below table and validate the **image extension** w.r.t the version before proceeding to upgrade/downgrade.

| Versio | 'n     | Image extension |
|--------|--------|-----------------|
| From   | То     |                 |
| 4.x    | 4.x    | CIMG            |
| 4.x    | 3.11.x | IMG             |
| 3.11.x | 4.x    | **IMG           |



#### \*\*Note

For **cnPilot e410/e430/e510/e600 and e700** APs, refer additional instructions mentioned in before proceeding to upgrade/downgrade.

### Section-2



#### Attention

To upgrade/downgrade from 3.11.x (3.11.4-r9/3.11.3.1-r4/3.11.3-r7 etc.) to 4.x (4.0/4.1/4.2 and later subsequent images) and vice versa, mandatorily use 3.11.4.1-r3 and 4.1-r3 and above image versions. Ignoring this suggestion can lead to failure in loading the image and resulting in flashed partition (backup partition) getting corrupted. To recover the corrupted partition, user may have to contact Cambium Support team.

Perform the below steps to upgrade image from 3.11.4-r9 to 4.1.1-r3 and above:

- 1. First upgrade the AP from **3.11.4-r9** to **3.11.4.1-r3**
- 2. Then upgrade the AP from **3.11.4.1-r3** to **4.1.1-r3** and above

Perform the below steps to upgrade image from 4.1.1-r3 and above to 3.11.4-r9:

- 1. First downgrade the AP from 4.1.1-r3 and above to 3.11.4.1-r3
- 2. Then downgrade the AP from 3.11.4.1-r3 to 3.11.4-r9



### Note

This recommendation is only applicable for cnPilot e410/e430/e510/e600 and e700.

# Chapter 1: About This User Guide

This chapter describes the following topics:

- Overview of cnPilot products
- Intended audience
- Purpose
- Related documents
- Features and Enhancements
- New platforms

### Overview of cnPilot products

Thank you for choosing Cambium cnPilot Access Point (AP)!

This User Guide describes the features supported by cnPilot Enterprise AP and provides detailed instructions for setting Up and configuring cnPilot Enterprise AP.

cnPilot's are the industry's upcoming feature-rich Wi-Fi APs designed for Indoor/Outdoor which are easy to deploy and configure.

### Intended audience

This guide is intended for use by the system designer, system installer and system administrator.

### Purpose

Cambium Network's cnPilot Enterprise AP documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium's equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or expressed, 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.

### Related documents

Table 1 provides details on cnPilot's support information.

#### Table 2 Related documents

| cnPilot Enterprise product details                  | https://www.cambiumnetworks.com/products/wifi-cnpilot/ |
|---|--|
| cnPilot Enterprise AP User Guide<br>(This document) | https://support.cambiumnetworks.com/files              |
| cnPilot Enterprise AP Release Notes                 | https://support.cambiumnetworks.com/files              |
| Software Resources                                  | https://support.cambiumnetworks.com/files              |

| Knowledge Base (KB) Articles | http://community.cambiumnetworks.com/t5/cnPilot-E-<br>Series-Enterprise-APs/bd-p/cnPilot_E_Series/ |
|------------------------------|--|
| Community                    | http://community.cambiumnetworks.com/  |
| Support                      | https://www.cambiumnetworks.com/support/contact-<br>support/                                       |
| Warranty                     | https://www.cambiumnetworks.com/support/warranty/  |
| Feedback                     | For feedback, e-mail to support@cambiumnetworks.com/   |

### Features and Enhancements

### System Release 3.11.4

System release 3.11.4 includes the following enhancements:

#### Table 3 New features

| Features    | Platform Support | Summary   |
|-------------|------------------|---|
| VAN support | e600             | ZTE 4G dongle is supported as a WAN link in cnPilot e600.           |
| Auto-RF     | All              | Auto-RF enhancements.   |
| System      | All              | Provision to disable factory reset due to continuous power outages. |
| System      | All              | Provision to honor MTU learnt from DHCP option 26.                  |

### System Release 4.0

System release 4.0 includes the following new features:

#### Table 4 New features

| Features         | Platform Support       | Summary  |
|------------------|------------------------|--|
| GRE over UDP     | All                    | Layer 3 GRE tunnel support with any standard vendor.                                       |
| Cambium GRE      | All                    | Layer 3 GRE tunnel support with Cambium cnMaestro c4000 Controller and c4000 Concentrator. |
| IPv6             | All                    | Support for IPv6 protocol.   |
| LACP             | e600                   | Link aggregation support.  |
| BLE Location API | e600, e430 and<br>e700 | Discover neighbor Bluetooth device.  |

System release 4.0 includes the following enhancements:

#### Table 5 Enhancements

| Features          | Platform Support | Summary   |
|-------------------|------------------|---|
| RADIUS attributes | All              | Added multiple parameters as per RFC to meet customer requirements. |
| ACL               | All              | Improved the efficiency of throughput when ACL is enabled.          |
| Syslog            | All              | Added multilevel debugging capability.                              |

### Supported hardware platforms

#### Table 6 Supported platforms

| Hardware | Description   |
|----------|---|
| E400     | 2x2:2, 802.11a/b/g/n/ac wave 1 indoor Access Point                                    |
| E500     | 2x2:2, 802.11a/b/g/n/ac wave 1 outdoor Access Point                                   |
| E501S    | 2x2:2, 802.11a/b/g/n/ac wave 1 90°/120° outdoor Access Point                          |
| e502S    | 2x2:2, 802.11a/b/g/n/ac wave 1 30° outdoor Access Point                               |
| e410     | 2x2:2, 802.11a/b/g/n/ac wave 2 indoor Access Point                                    |
| e510     | 2x2:2, 802.11a/b/g/n/ac wave 2 outdoor Access Point                                   |
| e600     | 2x2:2 for 2.4 GHz and 4x4:4 for 5 GHz, 802.11a/b/g/n/ac wave 2 indoor<br>Access Point |
| e430     | 2x2:2, 802.11a/b/g/n/ac wave 2 indoor Access Point                                    |
| e700     | 2x2:2 for 2.4 GHz and 4x4:4 for 5 GHz, 802.11a/b/g/n/ac wave 2 indoor<br>Access Point |

### New hardware platforms

System release 4.2 includes the following new Platforms:

#### Table 7 New platforms

| Hardware | Description   |
|----------|---|
| e410b    | 2x2:2, 802.11a/b/g/n/ac wave 2 Indoor Access Point. |

# Chapter 2: Quick Start - Device Access

This chapter describes the following topics:

- Powering up the device
- Accessing the device
- LED status

### Powering up the device

This section includes the following topics:

- PoE switches (802.3af/802.3at)
- PoE adapter

cnPilot product family can be powered either using PoE adapter provided in the package or it can be powered using 802.3af or 802.3at capable switches.

For cnPilot e600 and e430, there is additional provision to power ON device using DC power adapter.

### PoE switches (802.3af/802.3at)

All devices can be powered by PoE switches supplying standard 802.3af or 802.3at power. The following restrictions apply if 802.3af power is used:

- On cnPilot E501S and e502S along with E500, e430 and e425H the PoE out feature will not be operational.
- On cnPIlot e600, radio transmit power will be limited to 17dBm and the USB port will not be operational.
- On cnPilot e700, the radio transmit power will be limited to 17dBm and PoE out feature will not be operational.

To avoid these restrictions, power the device using 802.3at capable switches. In addition, 802.3af / 802.3at switches do not supply sufficient power to use the PoE out feature on cnPilot e700. Use a power injector such as the 60W Cambium N000065L001C Gigabit power injector when operating with this feature enabled.

To power ON the cnPilot device, connect Eth1 of device to PoE switch port. **Figure 1** displays how cnPilot e430 connects to a PoE capable switch.



Figure 1 Installation of cnPilot to PoE capable switch

### PoE adapter

Follow the below procedure to power up the device using PoE adapter (Figure 2):

- 1. Connect the Ethernet cable from Eth1/PoE-IN of the device to the PoE port of Gigabit Data + Power.
- 2. Connect an Ethernet cable from your LAN or Computer to the Gigabit Data port of the PoE adapter.

Figure 2 Installation of cnPilot to PoE adapter





### Note

- 1. If Auxiliary port is used to power a secondary device, the maximum cable length between AP and the secondary device is 5 meters.
- 2. Secondary device is allowed to install 0.6 meters below the highest point on the metal mounting pole.
- 3. If Auxiliary port is used for only LAN connection between AP and secondary device. If cable length exceeds 5 meters or if the secondary device is installed on a different pole, then additional gigabit surge suppressor is recommended between AP and Secondary device.
- **3.** Connect the power cord to the adapter, and then plug the power cord into a power outlet as shown in Figure 3. Once powered **ON**, the Power LED should illuminate continuously on the PoE Adapter.



Figure 3 Installation of adapter to power outlet

### Accessing the device

This section includes the following topics:

- Device access using default/fallback IP
- Device access using zeroconf IP
- Device access using DHCP IP address

Once the device is powered up ensure the device is up and running before you try to access it based on LED status. Power LED on the cnPilot device should turn Green which indicates that the device is ready for access.

#### Device access using default/fallback IP

- 1. Select **Properties** for the Ethernet port:
  - a) For Windows 7: Control Panel > Network and Internet > Network Connections > Local Area Connection
  - b) For Windows 10: Control Panel > Network and Internet > Network and Sharing Center > Local Area Connection

| Local Area Connection Properties   | X |
|--|---|
| Networking Authentication Sharing  |   |
| Connect using:   |   |
| Intel(R) Ethemet Connection I217-LM  |   |
| Configure  | ] |
| This connection uses the following items:  | _ |
| Client for Microsoft Networks     Juniper Network Service     QoS Packet Scheduler     File and Printer Sharing for Microsoft Networks |   |
|  |   |
| <ul> <li>Link-Layer Topology Discovery Mapper I/O Driver</li> <li>Link-Layer Topology Discovery Responder</li> </ul>                   |   |
| Install Uninstall Properties   |   |
| Description<br>Allows your computer to access resources on a Microsoft<br>network.   |   |

2. IP Address Configuration:

The cnPilot AP obtains its IP address from a DHCP server. A default IP address of **192.168.0.1/24** will be used if an IP address is not obtained from the DHCP server.

| Internet Protocol Version 4 (TCP/IPv4)  | Properties          | × |
|---|---------------------|---|
| General   |                     |   |
| You can get IP settings assigned auton<br>this capability. Otherwise, you need to<br>for the appropriate IP settings. |                     |   |
| O Obtain an IP address automatical  | у                   |   |
| • Use the following IP address:   |                     |   |
| IP address:   | 192.168.0.100       |   |
| Subnet mask:  | 255 . 255 . 255 . 0 |   |
| Default gateway:  |                     |   |
| Obtain DNS server address autom   | natically           |   |
| • Use the following DNS server add  | resses:             |   |
| Preferred DNS server:   |                     |   |
| Alternate DNS server:   |                     |   |
| Validate settings upon exit   | Ad <u>v</u> anced   |   |
|   | OK Cance            |   |

Open any browser on the PC and browse http://192.168.0.1 with default credentials as below:

- Username: admin
- Password: admin

#### Device access using zeroconf IP

To access the device using zeroconf IP, follow the below steps:

For example:

- a) Convert the last two bytes of ESN of the device to decimal. If ESN is **58:C1:CC:DD:AA:BB**, last two bytes of this ESN is **AA:BB**. Decimal equivalent of AA:BB is **170:187**.
- b) Zeroconf IP of device with ESN 58:C1:CC:DD:AA:BB is 169.254.170.187
- c) Configure Management PC with **169.254.100.100/16** as below:

| Internet Protocol Version 4 (TCP/IPv4)  | Properties            | × |
|---|-----------------------|---|
| General   |                       |   |
| You can get IP settings assigned autom<br>this capability. Otherwise, you need to<br>for the appropriate IP settings. |                       |   |
| O Obtain an IP address automatical  | у                     |   |
| • Use the following IP address:   |                       |   |
| IP address:   | 169 . 254 . 100 . 100 |   |
| Subnet mask:  | 255.255.0.0           |   |
| Default gateway:  |                       |   |
| Obtain DNS server address autom   | atically              |   |
| • Use the following DNS server addr   | resses:               |   |
| Preferred DNS server:   |                       |   |
| <u>A</u> lternate DNS server:   |                       |   |
| Uaļidate settings upon exit   | Ad <u>v</u> anced     |   |
|   | OK Cancel             | I |

- d) Access the device UI using http://169.254.170.187 with default credentials as below:
  - Username: admin
  - Password: admin

#### Device access using DHCP IP address

- 1. Plug in the device to the network.
- 2. Get the IP address of the device from the System administrator.
- 3. Access device UI using http://<IP address> with default credentials as below:
  - Username: admin
  - Password: admin

### LED status

The **e410/e410b/e430/e425H/e600/e505** AP has single color LED. The power LED will glow Amber as the AP boots up and turn Green once it has booted up successfully. The network/status LED will glow Amber if the connection to cnMaestro controller/manager is down and turns Blue once the AP is connected successfully to cnMaestro.

#### Table 8 e410/e410b/e430/e425H/e600/e505 LED status

| LED Color | Status Indication  |  |  |  |  |  |
|-----------|--|--|--|--|--|--|
|           | Device is booting up.     Note If these LEDs remain 'Amber' for more than 5 minutes, indicates that the device failed to boot. |  |  |  |  |  |
|           | <ul><li>Device is successfully up and accessible.</li><li>Wi-Fi services are up if configured.</li></ul>                       |  |  |  |  |  |
|           | cnMaestro connection is successful.  |  |  |  |  |  |

The **e700/e510** AP has two multi-colored LEDs. The power LED will glow Amber as the AP boots up and turns Green once it has booted up successfully. The network/status LED will glow Amber if the connection to cnMaestro controller/manager is down and turns Blue once the AP is connected successfully to cnMaestro.

#### Table 9 e700/e510 LED status

| LED Color |                           | Status Indication  |
|-----------|---------------------------|--|
| ወ         | <del>ठ<sup>8</sup>ठ</del> |  |
|           |                           | Device is booting up.     Note If these LEDs remain 'Amber' for more than 5 minutes, indicates that the device failed to boot.                           |
|           |                           | <ul><li>Device is successfully up and accessible.</li><li>Wi-Fi services are up if configured.</li></ul>   |
|           |                           | <ul> <li>Device is successfully up and accessible.</li> <li>Wi-Fi services are up if configured.</li> <li>cnMaestro connection is successful.</li> </ul> |

The **E400/E500/E501S/e502S** AP has two multi-colored LEDs. The power LED will glow Amber as the AP boots up and turns Green once it has booted up successfully. The network/status LED will glow Amber if the connection to cnMaestro controller/manager is down and turns Green once the AP is connected successfully to cnMaestro.

#### Table 10 E400/E500/E501S/e502S LED status

| LED Color |                | Status Indication  |
|-----------|----------------|--|
|           | <del>8</del> 8 |  |
|           |                | <ul> <li>Device is booting up.</li> <li>Note If these LEDs remain 'Amber' for more than 5 minutes, indicates that the device failed to boot.</li> </ul>  |
|           |                | <ul><li>Device is successfully up and accessible.</li><li>Wi-Fi services are up if configured.</li></ul>   |
|           |                | <ul> <li>Device is successfully up and accessible.</li> <li>Wi-Fi services are up if configured.</li> <li>cnMaestro connection is successful.</li> </ul> |

# Chapter 3: Device Modes

cnPilot product family supports three modes of operation based on deployment size. Details of mode of operation supported by cnMaestro are given below:

- cnMaestro managed mode
- Autopilot mode
- Standalone mode

### cnMaestro managed mode

This mode is also known as controller mode, in which all management traffic is tunneled to cnMaestro and data traffic is offloaded from AP to the network. There are provisions to tunnel data traffic to cnMaestro but has its own limitations w.r.t size of deployment. Device onboarding methods and procedures are explained in further chapters. By default, devices onboard to cnMaestro cloud ( https://cloud.cambiumnetworks.com), however we can also onboard the devices to cnMaestro On-Premises by mapping the cnMaestro IP address on the device.



Note cnMaestro managed mode is the recommended mode for any cnPilot devices.

### Autopilot mode

This is a proprietary mode supported by cnPilot devices. This mode allows one of the cnPilot devices to act as controller, which allows to configure other devices in the network. This mode has its own limitations, which will be explained in detail in the following chapters.

### Standalone mode

This is the default mode a cnPilot device operates. In this mode, it is expected that each device has to be configured and managed independently, which is cumbersome if deployment size exceeds 10 devices.

## Chapter 4: cnMaestro Onboarding

This chapter describes the following topics:

- Overview
- Device Onboarding and Provisioning
- Directing devices to the cnMaestro On-Premises server
- Claim using Cambium ID

### Overview

cnMaestro is Cambium's next generation network management platform based on cloud technologies. In addition to the cloud-based cnMaestro solution, it can also be installed as a standalone On-Premises server. By default, all devices contact https://cloud.cambiumnetworks.com, no user action is required to direct devices to contact cnMaestro cloud. You can onboard and provision devices without any additional setup.

If you are using cnMaestro On-Premises you must direct devices to correct cnMaestro server using DHCP or static URL configuration.

### Device Onboarding and Provisioning

This section includes the following topics:

- Onboarding to cnMaestro cloud using MSN
- Onboarding to cnMaestro On-Premises
- Auto-Provisioning
- Other options

### Onboarding to cnMaestro cloud using MSN

This mode is preferable for cnMaestro cloud. Inorder to claim through MSN Address, follow the below steps:

- 1. Login to On-Premises server using default username and password (admin/admin) or the username and password set by the Administrator.
- 2. Navigate to Home > Onboard Devices > Claim from cnMaestro.
- 3. Select the **Device type** that needs to be onboarded and provide the MSN in the combo box and click the **Claim Devices button**. Multiple MSN Addresses of same device type can be claimed using (, ) separator between MSN or by entering them in the new line.

|     | Cambium Networks                        |                                 |                |  |                   |                           | Ĺ         |                | ()<br>()<br>() | C ShashankT -       |
|-----|---|---------------------------------|----------------|--|-------------------|---------------------------|-----------|----------------|----------------|---------------------|
| -14 | Onboard                                 |                                 |                | Claim Devices with Serial Number   |                   |                           |           |                |                | 0                   |
| 俞   | Onboard Claim from Device               |                                 |                | Enter the Serial Numbers (MSNs) of the devices you want to add to your account<br>(comma-separated or one per line). Once a device is claimed, it is placed in the |                   |                           |           |                |                |                     |
| Eg. | Claim Device                            |                                 |                | Cnboarding Queue when it comes online.  Note: All devices with 12 digit strong Serial Numbers can be claimed here. Other   |                   |                           |           |                |                |                     |
|     | The Onboarding Queue holds devices be   |                                 |                | devices can be claimed using <u>Cambium ID</u>   | vision devices be | fore they are approved by |           |                |                |                     |
|     | C Search                                |                                 |                | Enter / Place a cursor in the box and use a barcode scanner to quickly claim<br>devices.   |                   |                           |           |                | Export         | Approve All         |
| S.  | Type 🕆 Seria                            | l Number 🛛 🕆                    | Device T       | MAC  | τ                 | Duration                  | Configure |                |                |                     |
| ¢   | cnPilot W8T                             | K03TLDJW6                       | cnPilot-0604EF | exC:   | ing for Device    | 108d 17h 1m               | 🖹 🚱 🛓     | <u>a</u>       | Unapp          | rove Delete         |
| 留   |   |                                 |                |  |                   |                           | Sh        | wing 1 - 1 Tot | d: 1 10 1      | < Previous 1 Next > |
| ٨٩  | "Note: Devices will remain in the queue | e for 1 week after onboarding : |                |  |                   |                           |           |                |                |                     |
|     |   |                                 |                | Claim Devices Clear  |                   |                           |           |                |                |                     |
|     |   |                                 |                |  |                   |                           |           |                |                |                     |

#### Figure 4 Onboarding to cnMaestro cloud using MSN

#### Onboarding to cnMaestro On-Premises

This mode is preferable for cnMaestro On-Premises. Inorder to claim through MAC Address (ESN), please follow the below steps:

- 1. Login to On-Premises server using default username and password (admin/admin) or the username and password set by the Administrator at the time of On-Premises server installation.
- 2. Navigate to Home > Onboard Devices > Claim from cnMaestro.
- 3. Select the **Device type** for which onboarding is to be done and provide the MAC Address in the combo box and click the **Claim Devices button**. Multiple MAC Addresses of same device type can be claimed using (, ) separator between MAC Addresses or by entering them in the new line.

|    | cn <b>Maestro</b>  |  |                 | Claim Devices with                             | MAC Address                   |                               | ×              | <u>(</u> )           | Ċ     | )    |             | i či            | Administrat  | tor- |
|----|--------------------|--|-----------------|--|-------------------------------|-------------------------------|----------------|----------------------|-------|------|-------------|-----------------|--------------|------|
| -  | Onboard            |  |                 |  |                               |                               |                |                      |       |      |             |                 |              | 2    |
| ណ៌ | Onboard Claim from | n Device   |                 | Enter the ESN (Etherne<br>comma-separated or o |                               | vould like to add to your acc | ount           |                      |       |      |             |                 |              |      |
| a. | Claim Device       |  |                 | Note: Devices can                              | be claimed using ESN (Ethe    | met MAC) or Cambium ID        |                |                      |       |      |             |                 |              |      |
| Ş  |                    | olds devices before they are a<br>r software version. Learn more |                 | Device Type:                                   | cnPilot Enterprise (E-Series) | •                             | d by           | cnMaestro. You can p |       |      | ices before | they are approv | red by setti |      |
|    | Q Search           |  |                 | Enter / Place a cursor<br>devices.             | in the box and use a barcod   | le scanner to quickly claim   |                |                      |       |      | Export      | + Approve All   |              | •    |
| S. | Туре 🕆             | Serial Number 🔫  | Device T        |  |                               |                               |                | Duration             | Confi | gure |             |                 |              |      |
| Ħ  | cnPilot e600       | W8TL074Z2VLL   | E600-0CDB3C     |  |                               |                               | Devi           | ice 30d 14h 8m       |       | 0 ±  | Cart        | Unapprove       | Delete       |      |
| ÷  | cnPilot e600       | W8TL023K3WGG   | E600-0A1B1C     |  |                               |                               | Devi           | ice 30d 14h 8m       |       | 0 ±  | ø           | Unapprove       | Delete       |      |
| 먾  | cnPilot e430W      | W5UC02SHHXW3   | E430-36CD4F     | Claim Devices                                  | Clear                         |                               | Devi           | ice 30d 14h 8m       |       | 0 ¥  | (a)         | Unapprove       | Delete       |      |
| ۸۶ | cnPilot e430W      | W5UC02G3J91W   | E430-36C737     | 58:C1:7A:36:C7:37                              | 10.110.214.152                | - • Wa                        | iting for Devi | ice 30d 14h 8m       |       | 0 ±  | ø           | Unapprove       | Delete       |      |
|    | cnPilot e700       | W8UC0CG44CVM   | E700-260A3A     | 58:C1:7A:26:0A:3A                              | 10.110.214.144                | - • Wa<br>Unsolicited         | iting for Devi | ice 30d 14h 8m       |       | 0 ¥  | Cart .      | Unapprove       | Delete       |      |
|    | cnPilot e600       | W8TJ03Q8WHBM   | E600-GA-MESHBAE | 00:04:56:A6:AF:BC                              | 10.110.32.32                  | - • Wa<br>Unsolicited         | iting for Devi | ice 30d 14h 8m       |       | 0 ±  | Carl        | Unapprove       | Delete       |      |
|    | cnPilot e430W      | W5TM00C12QFV   | E430-369172     | 58:C1:7A:36:91:72                              | 10.110.211.241                | - • Wa<br>Unsolicited         | iting for Devi | ice 30d 14h 8m       |       | 0 ±  | (M)         | Unapprove       | Delete       |      |
|    | cnPilot e700       | W8UCoCH8KoM9   | E700-260A80     | 58:C1:7A:26:0A:80                              | 10.110.219.124                | - • Wa<br>Unsolicited         | iting for Devi | ice 30d 14h 8m       |       | 9 ¥  | di s        | Unapprove       | Delete       |      |

#### Figure 5 Onboarding to cnMaestro On-Premises

### Auto-Provisioning

cnMaestro On-Premises supports Auto-Provisioning for cnPilot devices. This feature not only enables auto onboarding but also configures synchronization and positioning of device in the network architecture. It is triggered only at first instance of device onboarding. It can be configured on cnMaestro as below:

#### Configuration

It is enabled at **Shared Settings > Auto-Provisioning**, and it allows one to automatically configure and approve devices based upon IP address. To create rules for cnPilot devices:

- 1. Navigate to **Shared Settings** > **Auto-Provisioning** page.
- 2. To create a new rule, click Add. The following window appears:

|     | cn <b>Maestro</b> |                       |  |                    |   |   | 227<br>Ĵ                       | Jan Sta          | 90              |
|-----|-------------------|-----------------------|--|--------------------|---|---|--------------------------------|------------------|-----------------|
| -   | Shared Setti      | ngs > Auto-Pro∖       | visioning <sup>pp</sup>  | Add Auto-Provision | ning Rules                                    |   |                                |                  |                 |
| ŵ   |                   |                       | upon its source subnet. (For de<br>ue and must be manually app | Subnet (CIDR)      | 192.168.100.0/24                              | 0 | all.) Approved devices will au | tomatically be c | onfigured and o |
| ES. | Subnet (CIDR)     | Device Type           | Managed Account  | Device Type        | cnPilot Enterprise (E-Series, ePMP Hotspot) - |   |                                | Approve          |                 |
| 67  | 10.110.205.0/24   | cnPilot Enterprise (E | -  | Network            | Anand_SA_LDAP -                               |   |                                | true             |                 |
|     | 10.110.235.0/24   | cnPilot Enterprise (E | Base Infrastructure  | Site               | Anand_SA_LDAP_site -                          |   |                                | true             |                 |
| S.  | 10.110.200.64/26  | cnPilot Enterprise (E |  | AP Group           | 1-L2TP-                                       |   |                                | true             |                 |
| Ĥ   | 10.110.214.16/32  | cnPilot Enterprise (E | Base Infrastructure  |                    |   |   | eature_MESH_Profiles           | true             | -               |
| Ð   |                   |                       |  | Approve            | Add Cancel                                    |   |                                |                  |                 |
| ŝŝ  | Add               |                       |  |                    | Curtor  |   |                                |                  |                 |
| 母   | Add               |                       |  |                    |   |   |                                |                  |                 |
| ٨٩  |                   |                       |  |                    |   |   |                                |                  |                 |
| 291 |                   |                       |  |                    |   |   |                                |                  |                 |
|     |                   |                       |  |                    |   |   |                                |                  |                 |
|     |                   |                       |  |                    |   |   |                                |                  |                 |

#### Figure 6 Auto-Provisioning

3. Enter the following details given in Table 8:

 Table 11 Auto-Provisioning parameter details

| Parameter     | Description  |
|---------------|--|
| Subnet (CIDR) | The subnet with CIDR of the devices to which the rule has to be applied. For example, Subnet/CIDR (192.168.100.100/25) maps the devices with the IP addresses ranging from 192.168.100.1 to 192.168.100.126. |
| Device Type   | Select the type of the device from the drop-down list.   |
| Network       | Select the network to which the device should be onboarded, once the device contacts the server.   |
| Site          | Select the site under which the device should be onboarded, once the device contacts the server.   |
| AP Group      | Select the AP Group which needs to be applied on the device, once the device contacts the server while onboarding.   |

| Parameter | Description                                     |
|-----------|---|
| Approve   | Enables this option to auto-approve onboarding. |

#### 4. Click Add.



Note Auto-Provisioning is supported only for cnMaestro On-Premises and not for cnMaestro cloud.

### Other options

This section includes the following topics:

- AP Group
- Site dashboard

The device onboarding screen can also be accessed from other locations in the UI. Below options can be used in both cloud cnMaestro and cnMaestro On-Premises. For cnMaestro On-Premises, ESN/MAC Address is required for onboarding/claiming device in an account whereas for cloud cnMaestro MSN is required to claim/onboard device in an account.

#### AP Group

Inorder to claim multiple devices from the AP Group in cloud, navigate to the Wi-Fi AP Groups tree view and click the drop-down menu for the selected AP Group.

- 1. Click the **Claim Devices** option.
- 2. In the pop-up dialog, select the **Network and Site** under which these devices needs to be placed and by default the devices claimed under this group will have the configuration settings from this AP Group.
- 3. Specify the MSNs/ESNs (Manufacturing Serial Number) of the devices line-by-line or commaseparated or click **Import .csv** option to **import the MSNs/ESNs** of the devices from a file.
- 4. Click **Claim Devices** to add to the selected AP Group with the configuration applied.



Note In cnMaestro On-Premises the procedure to claim the device using Serial Number is same as cloud, but instead of MSN, the user should use the device MAC Addresses.

| (          | cnMaestro                |   | _  |  |        | <u>i</u>        | 🧖 🖑 🥵 🗗 â        | Administrator + |
|------------|--------------------------|---|--|--|--------|-----------------|------------------|-----------------|
| -11        | Search                   | System  | Claim Enterprise Wi-                                 | Fi Devices   | *      |                 |                  | 0               |
| ~          | Networks Wi-Fi AP Groups | Dashboard Notifications Configuration Statist | Enter the ESN (Ethernet I<br>(comma-separated or one | MAC) of the devices you would like to add to your account<br>over line). |        |                 |                  |                 |
| ណ          | - 🕀 System 1             | Devices                                       | Device Type:   | cnPliot Enterprise (E-Series)  | Hrs)   |                 | Resi             | olution : 1 hr  |
| H          | 1-12TP                   | 239 224 235                                   | Network:   |  |        |                 |                  |                 |
|            | > 1 Ims_62               | TOTAL ORFLINE ONBOARDING                      | Network.   | default •  |        |                 |                  |                 |
| T AND IN T | 188                      | Alarms  | Site:  | None •   |        |                 |                  |                 |
| S.         | ACL123                   |   | Enterprise AP Group:                                 | ACL-Group  | 18 30  | 00.30           | 00.30            | _               |
| 串          | ACL-Group                | 0 227 86<br>ORTICAL HAUGH HAUGH               |  | the box and use a barcode scanner to quicidy claim                       | 1.0000 |                 | w.w              |                 |
|            | act_cm                   | TOTAL ALAMAS                                  | devices.   |  | ices   |                 |                  |                 |
| 8          | > AP-1-MativeTagged      |   |  |  |        |                 |                  | Last 5 mins     |
| 영          | AP-2-NativeTagged        | 159   |  |  |        | DEVICES BY TYPE | ALARMS           |                 |
| 28         | AP-Flapp-AP-1            | C LAST 34 HOURS                               |  |  |        |                 | 123              |                 |
| 25/1       | AP-Gp-1-ZndHop           | Metrics                                       |  |  |        | _               | 30               |                 |
|            | AP-Gp-1-MB               | ACCOUNT CAPACITY                              |  |  |        |                 | 18               |                 |
|            | AP-Gp-1-MC               |   |  | E Import.csv   |        | -               | 22               |                 |
|            | MP-0p-3-MB               | Managed      Onboarding                       | Claim Devices Ca                                     | incel Ciear  |        |                 | 17               |                 |
|            | MP-Gp-2-MC               | RECOMMENDED SOFTWARE                          |  |  |        |                 | Critical      Ma | jor 🐠 Minor     |
|            | AP-Group-1               |   | 2  |  |        |                 |                  |                 |
|            | AP-Group-2               | Details                                       | +  | - 16 B   | 700    | and a           | a second         |                 |

Figure 7 Claiming the device using MAC address (ESN)

Figure 8 Claiming the device using Serial Number (MSN)

|     | Cambium Networks                 |  |  |                  |
|-----|----------------------------------|--|--|------------------|
| -14 | Search                           | System   | Claim Enterprise WI-Fi Devices ×   | Ø                |
|     | Networks Wi-Fi AP Groups         | Dashboard Notifications Configuration Statisti | Enter the Serial Numbers (MSNs) of the cnPilot Enterprise (E-Series) devices you<br>want to add to your account(comma-separated or one per line). Once a device is |                  |
| ŵ   | System i                         | Devices  | claimed it will be placed in the Ophersting Queue when it comes online   | olution : 1 hr   |
| B   | > Begumpet_WiFI_Hotspot_Services |  | Note: ePMP Hotspot devices cannot be claimed from this page. Please use  |                  |
|     | > 🛅 Begumpet_WiFI_Hotspot_Servic | 13 1 1   | Cambium ID onboarding. 13  | _                |
|     | > Begumpet_WiFI_Hotspot_Servic   | TOTAL OFFLINE ONBOARDING                       | Network: default • a   |                  |
| S.  | BNG-Home                         | Alarms   | Site: None a   |                  |
| 8   | Default Enterprise               | 0 4 2  |  | -                |
| 43  | Default Home                     | CRITICAL MAJOR MINOR                           | Enterprise AP Group: Begumpet_WIFI_Hotspot_Services_MC 1230 1830 0030 0830   |                  |
|     | FB_Shaildhar                     | TOTAL ALARMS                                   | Enter / Place a cursor in the box and use a barcode scanner to quickly claim  Offline Total Devices  |                  |
| 岛   | FB-Shillong                      |  | devices.   |                  |
| 28  | > THYD-AP-GRP                    |  |  | Last 5 mins      |
| ēΛ  | Immu-E500-GA                     |  | DEVICES BY TYPE ALARMS   |                  |
|     | > 🖿 Lingesh_Babal_AP_GRP         | LAST 24 HOURS                                  |  |                  |
|     | > 🖿 Shashank-Home-Network-BLR    | Metrics  | 2 -  |                  |
|     | test-e430-sysmon                 | RECOMMENDED SOFTWARE                           | 0  |                  |
|     |                                  |  |  |                  |
|     |                                  |  | Critical @ Maj   | jor 🕘 Minor      |
|     |                                  | Details  | Claim Devices Cancel   |                  |
|     |                                  | NETWORKS 4                                     | Varanasi Patna   | Baoshan K<br>保山市 |

#### Site dashboard

Inorder to claim multiple devices from the Site dashboard in cloud, navigate to the **Manage** section and select a site under a network and click the drop-down menu for the selected site:

- 1. Click the **Claim Devices** option.
- 2. In the pop-up dialog, select the **Network and Site** under which these devices needs to be placed and by default the devices claimed under this group will have the configuration settings from this AP Group.
- Specify the MSNs (Manufacturing Serial Number) /ESNs (Equipment Serial Number) of the devices line-by-line or comma-separated or click Import .csv option to import the MSNs/ESNs of the devices from a file.
- 4. Click **Claim Devices** to add to the selected AP Group with the configuration applied.



Note Claim using MAC address is supported by cnMaestro On-Premises only.



#### Figure 9 Claim the device using MAC address

#### Figure 10 Claim the device using MSN

| 0       | Cambium Networks  |   |                                       |  |           |                                       | P 🔊 👘          |                          |
|---------|---|---|---------------------------------------|--|-----------|---------------------------------------|----------------|--------------------------|
| -14     | Search  | System  | Claim Wi-Fi Devices                   | ×  |           |                                       |                | 0                        |
|         | Networks WI-FI AP Groups                                  | Dashboard Notifications Configuration Statist |                                       | (MSNs) of the Wi-Fi devices you want to add to your<br>d or one per line). Once a device is claimed, it will be placed |           |                                       |                |                          |
| ណ៍      | ∽⊕ System I   | - Devices                                     | in the Onboarding Queue               | when it comes online.  | Total: 13 | Connection Health (Last 24 Hrs)       |                | Resolution : 1 hr        |
| P       | <ul> <li>✓ defaoit</li> <li>✓ Å* Begumpet.</li> </ul>     | 13 1 1<br>TOTAL OFFICINE ONEOARDING           | Cambium ID onboarding                 | ces cannot be claimed from this page. Please use   | rise)     | - u                                   |                |                          |
|         | > 🗘 First_Floor   | TOTAL DEPLINE UNBOARDING                      | Site:                                 | First_Floor  |           |                                       |                |                          |
| ٩٢<br>ا | > 🗘 Home  | Alarms  | Enterprise AP Group                   | None +   |           | 3                                     |                |                          |
| @       | Office     Second Floor                                   | 0 4 2<br>CRITICAL MAJOR MINOR                 | Home AP Group:                        | None 👻   |           | 0<br>12.30 18.30                      | 00.30 0        | 6.30                     |
|         | > 🗘 Terrace   | TOTAL ALARMS                                  | Enter / Place a cursor in<br>devices. | the box and use a barcode scanner to quickly claim   |           | Offline     Offline     Total Devices |                |                          |
|         | <ul> <li>→ ↓* Labs</li> <li>→ ↓* Shashank-Home</li> </ul> | human   | LEVICES.                              |  |           |                                       |                | Last 5 mins              |
| en.     |   | 0 LASTS4HOURS                                 |                                       |  |           | DEVICES BY TYPE                       | ALARMS         |                          |
|         |   | # Metrics                                     |                                       |  |           |                                       | 2              |                          |
|         |   | RECOMMENDED SOFTWARE                          |                                       |  |           |                                       | 0              |                          |
|         |   |   |                                       | 🛎 Import.csv   |           |                                       | •              | Critical 🖲 Major 👼 Minor |
|         |   | Details                                       | Claim Devices Ca                      | ancel Clear  | wangsar   |                                       | 7 Storouwariau |                          |
|         |   | Ar NETWORKS 4                                 |                                       |  | Kota      | Varanasi Patna                        |                | Baoshan K                |

# Directing devices to the cnMaestro On-Premises server using DHCP

From cnPilot system release 4.0, cnPilot device can be onboarded either using IPv4/IPv6 DHCP options. Following are the options that are used in IPv4 and IPv6 respectively:

- IPv4
  - o DHCP Option 43/52
  - o DHCP Option 15/24
- IPv6
  - o DHCP Option 43/52
  - o DHCP Option 15/24

#### DHCP Option 43/52

This mode of onboarding is preferred to use when cnMaestro On-Premises is deployed at customer end. cnPilot reads Option 43/52 during DHCP transaction and then it connects to respective cnMaestro. This option is given high priority during cnMaestro discovery process. All these devices which have read the Option 43/52 from DHCP transaction are available in Queue on cnMaestro, which needs to be further approved by end user.

| Ô  | cnMaestro     |  |             |                             |                          |                    |                                      | Û               | 2 🔊               | N=0<br>N=0        | Administra                   |
|----|---------------|--|-------------|-----------------------------|--------------------------|--------------------|--------------------------------------|-----------------|-------------------|-------------------|------------------------------|
| Ħ  | Onboard       |  |             |                             |                          |                    |                                      |                 |                   |                   |                              |
| ົດ | Onboard Claim | from Device  |             |                             |                          |                    |                                      |                 |                   |                   |                              |
|    | Claim Device  |  |             |                             |                          |                    |                                      |                 |                   |                   |                              |
| z  |               | eue holds devices before they ar<br>on, or software version. Learn n |             | it. Devices must be approve | d in order to complete t | he onboarding proc | ess and be managed by cn             | Maestro. You ca | n pre-provision d | evices bef        | ore they are approved by set |
|    | Q. Search     |  |             |                             |                          |                    |                                      |                 |                   | Exp               | ort 👻 Approve All            |
| Y  | Туре т        | Serial Number 🔻  | Device T    | MAC T                       | IP Address 🝸             | Added By           | Status T                             | Duration        | Configure         |                   |                              |
| Ð  |               |  |             |                             |                          | Unsolicited        |                                      |                 |                   |                   |                              |
| 2  | cnPilot e400  | W8SA01760R4L   | E400-AFCAC6 | 00:04:56:AF:CA:C6           | 10.110.219.70            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 3h 50m       | 1                 | . (M <sup>1</sup> | Approve Delete               |
| 苕  | cnPilot e430W | W5TM001KSKFN   | E430-369519 | 58:C1:7A:36:95:19           | 10.110.219.73            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 5h 27m       | 🖹 🔇 🛓             | . (M <sup>1</sup> | Approve Delete               |
| ጸ  | cnPilot e700  | W8UC0CCXTGHF   | E700-2609B0 | 58:C1:7A:26:09:B0           | 10.110.219.69            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 7h 5m        | 1                 | <b>1</b>          | Approve Delete               |
|    | cnPilot e510  | W8UJ04N2KH10   | E510-C18B33 | 58:C1:7A:C1:8B:33           | 10.110.219.78            | -<br>Unsolicited   | <ul> <li>Waiting for Appr</li> </ul> | 0d 8h 44m       | 1                 | <b>1</b>          | Approve Delete               |
|    | cnPilot e410  | W8TC008M4MF4   | E410-93F17E | 00:04:56:93:F1:7E           | 10.110.219.76            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 10h 22m      | 1                 | e del             | Approve Delete               |
|    | cnPilot e500  | W8SG18792132   | E500-B99DDC | 00:04:56:B9:9D:DC           | 10.110.219.71            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 14h 20m      | 1                 | e en              | Approve Delete               |
|    | cnPilot e510  | W8VA0118Z40D   | E510-C84429 | 58:C1:7A:C8:44:29           | 10.110.214.91            | -<br>Unsolicited   | <ul> <li>Waiting for Appr</li> </ul> | 1d 16h 36m      | 🖹 🔇 🛓             | <b>A</b>          | Approve Delete               |

Figure 11 DHCP option 43/52

#### DHCP Option 15/24

This mode of onboarding is preferred to use when cnMaestro On-Premises is deployed at customer end. cnPilot reads Option 15/24 during DHCP transaction and then it connects to respective cnMaestro. All these devices which have read the Option 15/24 from DHCP transaction are available in Queue on cnMaestro, which needs to be further approved by end user.

|            | cn <b>Maestro</b> |   |             |                            |                          |                    |                                      | ů.               |                           | Administrato                       |
|------------|-------------------|---|-------------|----------------------------|--------------------------|--------------------|--------------------------------------|------------------|---------------------------|------------------------------------|
| ÷          | Onboard           |   |             |                            |                          |                    |                                      |                  |                           |                                    |
| ŝ          | Onboard Claim     | from Device   |             |                            |                          |                    |                                      |                  |                           |                                    |
|            | Claim Device      |   |             |                            |                          |                    |                                      |                  |                           |                                    |
| 89         |                   | ue holds devices before they ar<br>on, or software version. Learn n |             | t. Devices must be approve | d in order to complete t | he onboarding proc | ess and be managed by cn             | Maestro. You cai | n pre-provision devices l | pefore they are approved by settin |
|            | Q Search          |   | line a      |                            |                          |                    |                                      |                  |                           | Export • Approve All               |
| S .        | Туре т            | Serial Number 🝸   | Device T    | MAC T                      | IP Address 🝸             | Added By           | Status 🕆                             | Duration         | Configure                 |                                    |
| ŧ          |                   |   |             |                            |                          | Unsolicited        |                                      |                  |                           |                                    |
| ¢3         | cnPilot e400      | W8SA01760R4L  | E400-AFCAC6 | 00:04:56:AF:CA:C6          | 10.110.219.70            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 3h 50m        | 🖹 🛛 🕹 🥖                   | Approve Delete                     |
| 留          | cnPilot e430W     | W5TM001KSKFN  | E430-369519 | 58:C1:7A:36:95:19          | 10.110.219.73            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 5h 27m        | 🖹 🛛 🕹 🥖                   | Approve Delete                     |
| <b>λ</b> Я | cnPilot e700      | W8UC0CCXTGHF  | E700-2609B0 | 58:C1:7A:26:09:B0          | 10.110.219.69            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 7h 5m         | 🖹 🥝 🛓 🌶                   | Approve Delete                     |
|            | cnPilot e510      | W8UJ04N2KH10  | E510-C18B33 | 58:C1:7A:C1:8B:33          | 10.110.219.78            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 8h 44m        | 🖹 🛛 🕹 🥖                   | Approve Delete                     |
|            | cnPilot e410      | W8TC008M4MF4  | E410-93F17E | 00:04:56:93:F1:7E          | 10.110.219.76            | -<br>Unsolicited   | • Waiting for Appr                   | 0d 10h 22m       | 🖹 🥝 🛓 🌶                   | Approve Delete                     |
|            | cnPilot e500      | W8SG18792132  | E500-B99DDC | 00:04:56:B9:9D:DC          | 10.110.219.71            | -<br>Unsolicited   | <ul> <li>Waiting for Appr</li> </ul> | 0d 14h 20m       | 🖹 🛛 🕹 🌶                   | Approve Delete                     |
|            | cnPilot e510      | W8VA0118Z40D  | E510-C84429 | 58:C1:7A:C8:44:29          | 10.110.214.91            |                    | • Waiting for Appr                   | 1d 16h 36m       | 🖹 🧿 🛓 🥖                   | Approve Delete                     |

DHCP server configuration

More details on various DHCP server configuration for Option 43/52 is available in Cambium Knowledge Base (KB) section.

#### Windows server configuration

For Windows server configuration for onboarding devices to cnMaestro On-Premises server, please click the below URL.

http://community.cambiumnetworks.com/t5/cnMaestro/Device-Onboarding-and-Windows-DHCP-Options-for-cnMaestro-On/m-p/55199

#### Linux server configuration

A DHCP Server can be used to configure the IP Address, Gateway, and DNS servers for Cambium devices. If you administer the DHCP Server, you can also configure DHCP Options that will tell the devices how to access the cnMaestro (so the URL doesn't need to be set on each device).

http://community.cambiumnetworks.com/t5/cnMaestro/Device-Onboarding-and-Linux-DHCP-Options-for-cnMaestro-On/m-p/55187

#### Microtik server configuration

For Microtik Routerboard DHCP configuration for onboarding devices to cnMaestro On-Premises server, please click the below link.

http://community.cambiumnetworks.com/t5/cnMaestro/Microtik-Routerboard-DHCP-configuration-for-Onboarding-devices/m-p/56012

### Claim using Cambium ID

This section includes the following topics:

- Claim through static URL without Cambium ID and onboarding key
- Claim through static URL with Cambium ID and onboarding key

# Claim through static URL without Cambium ID and onboarding key

Inorder to claim the devices using the static URL without Cambium ID and onboarding key please follow the below steps:

- 1. Login to device UI and navigate to **Configure > System > Management > cnMaestro**.
- Provide static URL of On-Premises https://ON-PREMISESIPADDRESSORHOSTNAME and click Save.
- 3. Device will come to the onboarding queue in the cnMaestro Home > Onboard Devices > Onboard page and the user can approve the device.

| )nboard            |                            |                            |                      |                       |                           |                                   |                               |                    |                          |                          |
|--------------------|----------------------------|----------------------------|----------------------|-----------------------|---------------------------|-----------------------------------|-------------------------------|--------------------|--------------------------|--------------------------|
| Onboard Clai       | m from Device              |                            |                      |                       |                           |                                   |                               |                    |                          |                          |
| Claim Device       |                            |                            |                      |                       |                           |                                   |                               |                    |                          |                          |
| he Onboarding Qu   | eue holds devices before   | they are added to your acc | ount. Devices must b | e approved in orde    | r to complete the onboard | ing process and be mana           | aged by cnMaestro             | . You can pre-pro- | ision devices before the | ry are approved by setti |
| xcation, configura | tion, or software version. | Learn more                 |                      |                       |                           |                                   |                               |                    |                          |                          |
| All 💌 S            | earch                      | Q                          | Device Type: All     | Managed A             | ccount: All+              |                                   |                               |                    | Export +                 | Approve All              |
| Туре               | Serial Number              | Device                     | MAC                  | IP Address            | Managed Account           | Added By                          | Status                        | Duration           | Configure                | Actions                  |
| cnPilot E500       |                            | Rajesh                     | -                    | 10.110.208.167        | Base Infrastructure       | Administrator<br>Unsolicited      | Onboarded                     | 3d 22h 8m          | Summary                  | ONBOARDED A              |
| cnPilot E400       |                            | E400-cnPilot-182-RGVN      |                      | <u>10.110.212.182</u> | BesK0M                    | Unsolicited                       | Onboarded                     | 4d 2h 45m          | Summary                  | ONBOARDED                |
| cnPilot E400       | 1000                       | E400-B5ADE0                |                      | 10.110.202.103        | BesK0M                    | Administrator<br>Using MAC Addres | <ul> <li>Onboarded</li> </ul> | 6d 5h 17m          | Summary                  | ONBOARDED A              |
| ,                  |                            |                            |                      |                       |                           |                                   |                               |                    |                          |                          |
|                    |                            |                            |                      |                       |                           |                                   |                               |                    |                          |                          |

Figure 13 Claim through static URL without Cambium ID and onboarding key

### Claim through static URL with Cambium ID and onboarding key

Inorder to claim the devices using the static URL with Cambium ID and onboarding key, please follow the below steps:

- 1. Login to On-Premises server using default username and password (admin/admin) or the username and password set by the Administrator at the time of installation.
- 2. Navigate to Home > Onboard Devices > Claim from Device page.
- 3. Select the checkbox for "Enable Cambium ID based authentication to onboard devices".
- 4. Click on **Add new** and select the username from the drop-down list and specify the onboarding key and click **Save**.
- 5. Login to device UI and navigate to Configure > System > Management > cnMaestro.
- 6. Provide static URL of On-Premises https://ON-PREMISESIPADDRESSORHOSTNAME and Cambium ID (cnMaestro\_On-Premises) and onboarding key for that user and click **Save**.
- 7. Device will come to the onboarding queue in the cnMaestro Home > Onboard Devices > Onboard page and the user can approve the device.

| 🖶 Home       | 🖵 Monitor 🗸                    | 📽 Config       | ure 🗸 🛛 🐣 Operate     | ∽ 📰 Manage ∨   |                             |                  |                  |             |  |  |
|--------------|--------------------------------|----------------|-----------------------|--|-----------------------------|------------------|------------------|-------------|--|--|
| Onboard      | Dnboard Devices                |                |                       |  |                             |                  |                  |             |  |  |
| Claim from c | nMaestro                       | Onboard        | Claim from Device     | Unclaim  |                             |                  |                  |             |  |  |
| Claim [      | Claim Devices Using Cambium ID |                |                       |  |                             |                  |                  |             |  |  |
| Cambiun      | n ID: cnmae                    | stro_on_pi     | remises               |  |                             |                  |                  |             |  |  |
| 🖌 Enable     | Cambium ID ba                  | ased authentio | cation to onboard dev | ices   |                             |                  |                  |             |  |  |
| 0            |                                |                | ,                     | g the Cambium ID and Onboarding Key o<br>or can have their own Onboarding Key. | on the device. This informa | ation can be set | on the device vi | ia its user |  |  |
| The followin | ng users can cla               | aim devices us | sing the cnMaestro Ca | mbium ID and the user's Onboarding Ke  | у.                          |                  |                  |             |  |  |
| User:        | Adm                            | in             | ٣                     | Onboarding Key:  |                             | ×                | ۲                | Delete      |  |  |
| Add New      |                                |                |                       |  |                             |                  | Cancel           | Save        |  |  |

Figure 14 Claim through static URL with Cambium ID and onboarding key

# Chapter 5: UI Navigation

You can manage cnPilot device using User Interface (UI) which is accessible from any network devices such as computer, mobile, tabs, etc. cnPilot device accessibility is explained in **Chapter 3**.

This chapter describes the following topics:

- Login screen
- Home page (Dashboard)

### Login screen

To log to the UI, enter the following credentials:

- Username: **admin**
- Password: admin

#### Figure 15 UI Login page



### Home page (Dashboard)

On logging into cnPilot AP login page, the UI Home page is displayed. Figure 16 displays the parameters that are displayed in cnPilot AP Home page.



| Number | Element                | Description   |
|--------|------------------------|---|
|        | Menu                   | This section contains multiple tabs that helps user to configure, monitor and troubleshoot cnPilot device. Menu consists of the following:  |
|        |                        | Dashboard   |
|        |                        | • Monitor   |
|        |                        | Configure   |
|        |                        | Operations  |
|        |                        | Troubleshoot  |
| 2      | Reboot                 | Global button to reboot cnPilot device ( 🕐 ).   |
| 3      | Logout                 | Global button to logout user from cnPilot device ( [ ).   |
| 4      | Content                | Information in the area of web interface varies based on the tab selected<br>in Menu section. Usually, this area contains details of configuration or<br>statistics or provision to configure cnPilot device. |
| 5      | UI path                | Provides UI navigation path information to user.  |
| 6      | UI refresh<br>interval | Provision to reload updated statistics at regular intervals.  |
| 7      | Model<br>number        | Provides information related to cnPilot model number and configured hostname.   |

#### Table 12 cnPilot AP web interface elements

### Monitor

The Monitor section provides information such as current configuration, traffic statistics across all interfaces configured on device and device details. Based on information provided in this section, it is categorized and displayed under following categories:

- **System**: Provides information related to cnPilot device such as Software Image, host name, Country code etc.
- **Radio**: Provides information such as RF Statistics, Neighbour list and current radio configuration of device.
- WLAN: Provides information on WLANs and Mesh configurations.
- Network: Provides information related to interfaces such as, default route, interface statistics, etc.
- Services: Provides information related to entities that support Bonjour.

### Configure

This section allows user to configure cnPilot device based on deployment requirement. This tab has multiple sections as follows:

- **System**: Provision to configure System UI parameter.
- Radio: Provision to configure Radio settings (2.4GHz/5GHz).

- WLAN: Provision to configure WLAN parameters as per the end user requirement and type of wireless station.
- **Network**: Provides information related to VLAN, Routes, Ethernet ports etc.
- Services: Provides information related to Network and Bonjour Gateway.

#### Operations

This section allows user to perform maintenance of device such as:

- Firmware update: Provision to upgrade cnPilot devices.
- System: Provides different methods of debugging field issues and recovering device.
- **Configuration**: Provision to modify configuration of device.

#### Troubleshoot

The section provides users to debug and troubleshoot remotely. This tab has multiple sections and are as follows:

- WiFi Analyzer: When this is initialized, device provides information related to air quality.
- **Spectrum Analyzer**: Provides real-time cumulative distribution format view of RF environment and it is generated by the AP across 2.4 and 5GHz frequency bands.
- WiFi Perf Speed Test: Provision for the user to check the speed of link connectivity, either wireless or wired.
- **Connectivity**: Provides different modes network reachability of cnPilot device.
- Packet Capture: Provides feasibility for the user to capture packets on operational interfaces.
- Logs: Feasibility to check logs of different modules of cnPilot devices which will help support and the customer to debug an issue.
- Unconnected Clients: This section displays clients that are not connected/denied connection.

# Chapter 6: Configuration - System

This chapter describes the following topics:

- System
- Management
- Time settings
- Event Logging

### System

Table 10 lists configurable parameters that are available under Configuration > System UI tab:

| Table 13 Configu | ration: System | parameters |
|------------------|----------------|------------|
|------------------|----------------|------------|

| Parameter    | Description   | Range | Default   |
|--------------|---|-------|---|
| Name         | Hostname of the device. Configurable maximum length of hostname is 64 characters.   | _     | cnPilot Model<br>Number-Last<br>3 Bytes of<br>ESN |
| Location     | The location where the device is placed. The maximum length of location is 64 characters.   | _     | _   |
| Contact      | Contact information for the device.   | -     | -   |
| Country-Code | To be set by the administrator to the country-of-<br>operation of the device. The allowed operating<br>channels and the transmit power levels on those<br>channels depends on the country of operation.<br>Radios remain disabled unless this is set. The list of<br>countries supported depends on the SKU of the<br>device (FCC, ROW etc.). | _     | _   |
| Placement    | <ul> <li>cnPilot device supports both Indoor and Outdoor deployments. Based on deployment user can configure it as follows:</li> <li>Indoor         <ul> <li>When selected, only Indoor channels for country code configured will be available and operational.</li> <li>Outdoor             <ul></ul></li></ul></li></ul>                    | _     | Indoor  |
| PoE Output   | Provision to power on standard 802.3af devices or Cambium devices.  | _     | Disabled  |

| Parameter | Description   | Range | Default |
|-----------|---|-------|---------|
|           | <ul><li>Cambium-PoE</li><li>802.3af</li></ul>                                 |       |         |
| LED       | Select the LED checkbox for the device LEDs to be ON during operation.        | -     | Enabled |
| LLDP      | Provision to advertise device capabilities and information in the L2 network. | -     | Enabled |

To configure the above parameters, navigate to the **Configuration > System** tab and provide the details as given below:

- 1. Enter the hostname of the device in the **Name** textbox.
- 2. Enter the location where this device is placed in the **Location** textbox.
- 3. Enter the contact details of the device is placed in the **Contact** textbox.
- 4. Select the appropriate country code for the regulatory configuration from the **Country-Code** drop-down list.
- 5. Select **Placement** checkbox parameter **Indoor** or **Outdoor** to configure the AP placement details.
- 6. Select **PoE Output** from the drop-down list.
- 7. Enable **LED** checkbox.
- 8. Enable **LLDP** checkbox.
- 9. Click Save.

#### Figure 17 Configuration: System page

| System       |   |  |
|--------------|---|--|
| _ ,          |   |  |
| Name         | E500-B99DDC                                 | Hostname of the device (max 64 characters)                             |
| Location     |   | Location where this device is placed (max 64 characters)               |
| Contact      |   | Contact information for the device (max 64 characters)                 |
| Country-Code | Ţ   | For appropriate regulatory configuration                               |
| Placement    | Indoor Outdoor Configure the AP placement   | nt details   |
| PoE Output   | Off   | Enable Power-over-Ethernet to an auxiliary device connected to<br>ETH2 |
| LED          | Whether the device LEDs should be ON during | operation  |
| LLDP         | Whether the AP should transmit LLDP packets |  |
|              |   |  |

### Management

Table 11 lists configurable fields that are displayed in the **Configuration > System > Management** tab:

| Parameter           | Description   | Range   | Default  |
|---------------------|---|---------|----------|
| Admin<br>Password   | Password for authentication of UI and CLI sessions.   | -       | Admin    |
| Autopilot           | Provision to configure mode of cnPilot device when<br>Autopilot is enabled in network:  | -       | Default  |
|                     | • Default   |         |          |
|                     | Every cnPilot device by default operates as Auto-<br>Pilot slave.   |         |          |
|                     | • Master  |         |          |
|                     | When selected, cnPilot device will take the role of controller.   |         |          |
|                     | Disabled  |         |          |
|                     | When selected, auto-pilot mode is disabled on the device.   |         |          |
| Telnet              | Enables Telnet access to the device CLI.  | -       | Disabled |
| SSH                 | Enables SSH access to the device CLI.   | _       | Enabled  |
| SSH Key             | Provision to login to device using SSH Keys. User needs<br>to add Public Key in this section. If configured, user has<br>to login to AP using Private Keys. This is applicable for<br>both CLI and GUI.   | _       | Disabled |
| HTTP                | Enables HTTP access to the device UI.   | -       | Enabled  |
| HTTP Port           | Provision to configure HTTP port number to access device UI.  | 1-65535 | 80       |
| HTTPS               | Enables HTTPS access to the device UI.  | -       | Enabled  |
| HTTPS Port          | Provision to configure HTTPS port number to access device UI.   | 1-65535 | 443      |
| RADIUS Mgmt<br>Auth | User has provision to control login to AP using RADIUS<br>authentication. If enabled, every credential that are<br>provided by user undergo RADIUS authentication. If<br>success, allowed to login to UI of AP. This is applicable<br>for both CLI and GUI. | _       | Disabled |
| RADIUS Server       | Provision to configure RADIUS IPv4 server for Management Authentication.  | -       | -        |
| RADIUS Secret       | Provision to configure RADIUS shared secret for Management authentication.  | -       | -        |
| cnMaestro           | ·   | 1       | 1        |

 Table 14 Configuration: System > Management parameters
| Parameter                      | Description   | Range | Default |
|--------------------------------|---|-------|---------|
| Cambium<br>Remote Mgmt.        | Enables support for Cambium Remote Management of this device.                             | -     | Enabled |
| Validate Server<br>Certificate | This allows HTTPs connection between cnMaestro and cnPilot device.                        | -     | Enabled |
| cnMaestro URL                  | Static provision to onboard devices either using IPv4/IPv6/URL.                           | -     | -       |
| Cambium ID                     | Cambium ID used for provisioning cnMaestro<br>(Cambium Remote Management) of this device. | -     | -       |
| Onboarding<br>Key              | Password used for onboarding the device to cnMaestro.                                     | -     | -       |
| SNMP                           |   | •     | •       |
| Enabled                        | Provision to enable SNMPv2 or SNMPv3 support on device                                    | -     | -       |
| SNMPv2c RO<br>community        | SNMP v2c read-only community string.  | -     | -       |
| SNMPv2c RW<br>community        | SNMP v2c read-write community string.   | -     | -       |
| Trap Receiver<br>IP            | Provision to configure SNMP trap receiver IPv4 server.                                    | -     | -       |
| SNMPv3<br>Username             | Enter username for SNMPv3.  | -     | -       |
| SNMPv3<br>Password             | Enter password for SNMPv3.  | -     | -       |
| Authentication                 | choose Authentication type as MD5 or SHA.   | -     | MD5     |
| Access                         | Choose Access type as RO or RW.   | -     | RO      |
| Encryption                     | Choose ON or OFF.   | -     | ON      |

To configure the above parameters, navigate to the **Configuration > System** tab and provide the details as given below:

- 1. Enter the admin password of the device in the **Admin Password** textbox.
- 2. Select **Default, Master** or **Disabled** to enable/disable the **Autopilot** management of APs from the drop-down list.
- 3. Enable the **Telnet** checkbox to enable telnet access to the device CLI.
- 4. Enable the **SSH** checkbox to enable SSH access to the device CLI.
  - a. If certificate-based login is required, enter SSH Key in the textbox else disabled

- 5. Enable the HTTP checkbox to enable HTTP access to the device UI.
- 6. If custom port other than default is required, enter **HTTP port** number value for HTTP access in the textbox.
- 7. Enable the HTTPS checkbox to enable HTTPS access to the device UI.
- 8. If custom port other than default is required, enter **HTTP port** number value for HTTP access in the textbox.
- 9. If RADIUS based login is required, enable **RADIUS Mgmt Auth** checkbox and enter the details of RADIUS server as follows:
  - a. Enter **RADIUS Server** parameter in the textbox.
  - b. Enter **RADIUS Secret** parameter in the textbox.

### To configure **cnMaestro**:

- 1. Enable **Remote Management** checkbox to support for Cambium Remote Management of this device.
- 2. Enable Validate Server Certificate checkbox to support HTTPS connection between cnMaestro and cnPilot.
- 3. Enter the URL for cnMaestro in the **cnMaestro URL** textbox.
- 4. Enter the Cambium ID of the user in the **Cambium ID** textbox.
- 5. Enter the onboarding Key in the **Onboarding Key** textbox.

### To configure SNMP:

- 1. Select Enable checkbox to enable SNMP functionality.
- 2. Enter the SNMP v2c read-only community string in the SNMPv2c RO community textbox.
- 3. Enter the SNMP v2c read-write community string in the **SNMPv2c RW community** textbox.
- 4. Enter the **Trap Receiver IPv4** (Currently Cambium support SNMP only v1 and v2c Traps) in the textbox.
- 5. Enter the SNMP V3 username in the **SNMPv3 Username** textbox.
- 6. Enter the SNMP V3 password in the **SNMPv3 Password** textbox.
- 7. Select MD5 or SHA from the Authentication drop-down list.
- 8. Select **RO** or **RW** from the **Access** drop-down list.
- 9. Select **ON** or **OFF** from the **Encryption** drop-down list.
- 10. Click Save.

| Management                      |   |  |   |
|---------------------------------|---|--|---|
| Admin Password                  | Admin Password  |  | Configure password for authentication of GUI and CLI sessions |
| Autopilot                       | Default   | Ŧ  | Autopilot Management of APs                                   |
| Telnet                          | Enable Telnet access to the device CL                               | U  |   |
| SSH                             | Enable SSH access to the device CLI                                 |  |   |
| SSH Key                         | ssh-rsa AAAAB3NzaC1yc2EAAAA   | ABJQAAAQEAgO3YDa4jh/UtB3VJgA9s2                                | Use SSH keys instead of password for authentication           |
| НТТР                            | Enable HTTP access to the device GL                                 |  |   |
| HTTP Port                       | 80  |  | Port No for HTTP access to the device GUI(1-65535)            |
| UTTOC                           | Enable HTTPS access to the device GUI                               |  |   |
|                                 |   |  | Part No for HTTPS access to the device GUI(1-65535)           |
|                                 | HTTPS Port 443  |  | Fuit No for HTTPS access to the device Gold (-00000)          |
|                                 | RADIUS Mgmt Auth 🖉 Enable RADIUS authentication of GUI/CLI sessions |  | RADIUS server IP/Hostname                                     |
|                                 | RADIUS Server 10.110.211.97   |  |   |
| RADIUS Secret                   |   |  | RADIUS server shared secret                                   |
| - cnMaestro                     |   |  |   |
| Remote Man                      | agement   |  |   |
| Validate Server Certificate 🛛 🕏 |   |  |   |
| cnMaestro URL cloud.cambium     |   | cloud.cambiumnetworks.com                                      |   |
| Cambium ID                      |   |  |   |
| Onboarding                      | boarding Key  |  |   |
|                                 |   |  |   |
| SNMP                            |   |  |   |
|                                 |   |  |   |
| Enable                          |   | ✓ Enable/Disable SNMP  |   |
| SNMPv2c RC                      | ) community   | cambium_r_@123   |   |
| SNMPv2c RV                      | Community   | SNMP v2c read-only community string (max 64 o                  | cnaracters)   |
| Shire V2C KV                    | community   | cambium_w_@123<br>SNMP v2c read-write community string (max 64 | characters)   |
| Trap Receive                    | r IP  | 10.110.211.97  |   |
|                                 |   | SNMP trap server ip address                                    |   |
| SNMPv3 Use                      | rname   | cambium-snmpv3<br>SNMPv3 user name (max 32 characters)         |   |
| SNMPv3 Pas                      | sword   |  |   |
|                                 | SNMPv3 password (8 to 32 characters)                                |  |   |
| Authenticatio                   | uthentication MD5   |  | Υ   |
| Access                          |   | Read-Only  | •   |
| Encryption                      |   | On   | Ŧ   |
|                                 |   |  |   |
|                                 |   |  |   |

Figure 18 Configuration: Management page

## Time settings

User can configure up to two NTP servers. These are used by the AP to set its internal clock to respective time zones configured on the device. While powering ON the AP, the clock will reset to default and resyncs the time as the cnPilot AP does not have battery backup. The servers can be specified as an IPv4 addresses or as a hostname (Eg: pool.ntp.org). If NTP is not configured on device, device synchronizes time with cnMaestro if onboarded.

Table 12 lists the fields that are displayed in the Configuration > System > Time Settings section:

| Parameter    | Description   | Range | Default |
|--------------|---|-------|---------|
| NTP Server 1 | Name or IPv4 address of a Network Time Protocol server 1. | _     | -       |
| NTP Server 2 | Name or IPv4 address of a Network Time Protocol server 2. | _     | _       |

Table 15 Configuration: System > Time Settings parameters

| Parameter | Description  | Range | Default |
|-----------|--|-------|---------|
| Time zone | Time zone can be set according to the location where the AP is installed. By selecting the appropriate time zone from the drop-down list, ensures that the device clock is synced with the wall clock time.<br>Note Accurate time on the AP is critical for features such as WLAN Scheduled Access, Syslogs etc. | _     | _       |

To configure the above parameters, navigate to the **Configuration > System** tab and provide the details as given below:

- 1. Enter the name or IPv4 address of the NTP server 1 in the **NTP Server 1** textbox.
- 2. Enter the name or IPv4 address of the NTP server 2 in the **NTP Server 2** textbox.
- 3. Select the time zone settings for the AP from the **Time Zone** drop-down list.
- 4. Click Save.

### Figure 19 Configuration: Time settings page

| Time Settings |   |  |
|---------------|---|--|
| NTP Server 1  |   | Name or IP address of a Network Time Protocol server |
| NTP Server 2  |   |  |
| Time Zone     | Ţ   | Configure Timezone                                   |
|               | Current System Time Tue 01 Sep 2015<br>00:01:05 UTC |  |

# Event Logging

cnPilot devices supports multiple troubleshooting methods. Event Logging or Syslog is one of the standard troubleshooting processes. If you have Syslog server in your network, you can enable it on cnPilot device.

Table 13 lists the fields that are displayed in the Configuration > System > Event Logging section.

| Parameter       | Description  | Range | Default |
|-----------------|--|-------|---------|
| Syslog Server 1 | Hostname or IPv4/IPv6 address of the Syslog server and respective port number. | _     | 514     |
| Syslog Server 2 | Hostname or IPv4/IPv6 address of the Syslog server and respective port number. | _     | 514     |

Table 16 Configuration: System > Event Logging parameters

| Parameter       | Description  | Range | Default |
|-----------------|--|-------|---------|
| Syslog Severity | Provision to configure severity of Logs that must be forwarded to the server. The Log levels supported are as per RFC. | -     | Debug   |

To configure the above parameters, navigate to the **Configuration > System** tab and provide the details as given below:

- 1. Enter the FQDN or IPv4/IPv6 address of the **Syslog Server 1** along with customized port number in the textbox. If the port number is not entered, AP will take default value as **514**.
- 2. Enter the FQDN or IPv4/IPv6 address of the **Syslog Server 2** along with customized port number in the textbox. If the port number is not entered, AP will take default value as **514**.
- 3. Select the **Syslog Severity** from the drop-down list.
- 4. Click Save.

### Figure 20 Configuration: Event Logging page

| Syslog Server 1 | 10.110.211.97    | Port       | 514 Name or IPv4/IPv6 address of syslog server |  |
|-----------------|------------------|------------|--|--|
| Syslog Server 2 | 10.110.219.10    | Port       | 1234   |  |
| Syslog Severity | Debug (level 7 • | Specify se | verity of events forwarded to Syslog servers   |  |
|                 |                  |            |  |  |

Maximum of two Syslog servers can be configured on cnPilot device. Events are sent to both configured Syslog servers if they are up and running.

# Chapter 7: Configuration – Radio

This chapter describes the following topics:

- Overview
- Configuring Radio parameters

### Overview

cnPilot devices support numerous configurable radio parameters to enhance the quality of service as per the deployment.

# Configuring Radio parameters

All cnPilot devices support dual concurrent radio operations, i.e. both 2.4GHz and 5GHz can be turned on in parallel and hence each radio can be configured independently. **Radio 1** represents configuration of **2.4GHz Wi-Fi radio** and **Radio 2** represents configuration of **5GHz Wi-Fi radio** of cnPilot device. Information of each band radio configurable parameters are listed in Table 14.

| Parameter         | Description   | Range  | Default  |  |
|-------------------|---|--|--|--|
| Radio             |   |  |  |  |
| Enable            | Enables operation of radio.   | -  | Enabled  |  |
| Channel           | User can select the channel from the drop-down list.<br>Channels in drop-down list is populated based on  | • 2.4GHz:<br>1 - 14  | Auto   |  |
|                   | Country selected in <b>Configuration &gt; System</b> UI.  | • 5GHz:<br>36 - 173  |  |  |
| Channel<br>Width  | <ul> <li>User can select operating width of the channel.</li> <li>For 2.4GHz:<br/>Only 20MHz channel width is supported.</li> <li>For 5GHz:<br/>20MHz, 40MHz and 80MHz channel width is supported.</li> </ul>   | _  | <ul> <li>20MHz<br/>for<br/>2.4GHz</li> <li>80MHz<br/>for 5GHz</li> </ul> |  |
| Transmit<br>Power | User can configure transmit power of each radio based<br>on coverage and SLA. Unit of transmit power is in dBm<br>and its range is from 4 to 30. Maximum transmit power of<br>cnPilot devices varies based on model number. More<br>details of transmit power supported by each cnPilot<br>device is available at<br>https://www.cambiumnetworks.com/products/wifi/.<br>Transmit power drop-down box varies as per the country<br>selected in Configuration > System UI. Default value is | <ul> <li>2.4GHz:<br/>4 - 30</li> <li>5GHz:<br/>4 - 30</li> </ul> | Auto   |  |

Table 17 Configure: Radio parameters

| Parameter                  | Description  | Range  | Default   |
|----------------------------|--|--|---|
|                            | AUTO, which means radio transmit power is configured<br>to maximum as per the county configured selected in<br>Configuration > System UI.  |  |   |
| Beacon<br>Interval         | User can configure time durations between two consecutive Beacon's. It is termed as Beacon interval.   | 50ms -<br>3400ms.  | 100   |
| Minimum<br>Unicast<br>rate | Provision to adjust the coverage area of cnPilot device.<br>Higher the rate selected, lesser the range. User can<br>configure this value based on SLA in deployment. Drop-<br>down list contains all values that are advertised by<br>cnPilot device which includes legacy, HT and VHT rates.  | Standard<br>802.11b and<br>802.11g<br>data rates                   | 1Mbps   |
| Multicast<br>data rate     | Provision to configure multicast traffic rate. This is<br>modified based on type of wireless station that will be<br>connected to cnPilot device. Drop-down list contains<br>highest-basic, lowest-basic and highest-supported.  | _  | <ul> <li>Highest<br/>Basic for<br/>2.4GHz</li> <li>Lowest<br/>Basic for<br/>5GHz</li> </ul> |
| Airtime<br>Fairness        | Airtime Fairness is a solution on APs to increase the<br>performance of 11n and 11ac clients (HT clients) in the<br>presence of legacy 11abg clients. Legacy clients need<br>more airtime to transmit/receive the data compared to<br>HT clients (11n and 11ac clients). Because of this the<br>overall throughput of the HT clients falls down. Enabling<br>this feature improves the performance of HT clients by<br>throttling the legacy clients.<br>Compared to faster clients (802.11n/802.11ac), the slower<br>clients (802.11a/802.11bg) consumes more airtime to<br>transmit the same size data, in turn the throughput of<br>faster clients fall as they get lesser chance to transmit | _  | Disabled  |
|                            | (lesser airtime). Enabling this feature improves the<br>performance of faster clients in a wireless network which<br>is dominated by slower clients. This is achieved by<br>controlling the airtime of slower clients.   |  |   |
| Candidate<br>Channels      | <ul> <li>cnPilot provides user to configure selective channels based on their requirement. Options vary based on band of operation and is as follows:</li> <li>For 2.4GHz: <ul> <li>All</li> <li>Specific</li> </ul> </li> <li>For 5GHz: <ul> <li>All</li> <li>Specific</li> <li>Prefer Non-DFS</li> <li>Prefer DFS</li> </ul> </li> </ul>   | <ul> <li>2.4GHz:<br/>1 - 14</li> <li>5GHz:<br/>36 - 173</li> </ul> | All   |

| Parameter                           | Description  | Range   | Default  |
|-------------------------------------|--|---|--|
| Mode                                | All cnPilot devices are either 802.11ac Wave 1 or 802.11ac<br>Wave 2 supported. There are few legacy clients which<br>might not work as expected, hence this parameter can be<br>tuned to backward compatibility based on wireless<br>clients. | <ul> <li>2.4GHz:<br/>b, bg, n,<br/>gn</li> <li>5GHz: a,<br/>ac, an,<br/>n, n-ac.</li> </ul> | <ul> <li>11n mixed<br/>mode for<br/>2.4GHz</li> <li>11ac for<br/>5GHz</li> </ul> |
| Short<br>Guard<br>Interval          | Standard 802.11 parameter to increase the throughput of cnPilot device.  | -   | Enabled  |
| Off Channel                         | Scan (OCS)   |   |  |
| Enable                              | Provision to enable OCS on device to capture neighbour clients and APs.  | _   | -  |
| Dwell-time                          | Configure the time period to spend scanning of Wi-Fi devices on a channel.   | 50-300  | 50ms   |
| Auto-RF                             |  |   |  |
|                                     |  |   |  |
| Enable                              | Provision to enable Auto-RF on device.   | -   | Disabled   |
| Channel<br>Selection<br>Mode        | <ul><li>Auto-RF supports two modes of channel selection:</li><li>Interference based</li><li>Channel Utilization based</li></ul>  | _   | Interference   |
| Channel<br>Hold Time                | Configure time period for the device to be on same<br>channel selected by Auto-RF algorithm, irrespective of<br>quality of channel after selection.  | 5-1800  | 120 Min  |
| Channel<br>Utilization<br>Threshold | Configure the utilization thresholds to trigger channel selection by Auto-RF.  | 20-40   | 25%  |
| Auto-RF                             |  |   |  |
|                                     | Note<br>. System release 3.11.4<br>2. Post releases of 3.11.4  |   |  |

| Parameter                         | Description  | Range            | Default  |  |  |
|-----------------------------------|--|------------------|----------|--|--|
| Enable                            | Provision to enable Auto-RF on device.   | _                | Disabled |  |  |
| Packet<br>Error Rate              | Parameter to measure the unsuccessful packet transmissions by AP.  | 0-100 %          | -        |  |  |
| Channel<br>Utilization            | Parameter to measure the Channel efficiency.   | 0-100 %          | -        |  |  |
| Noise                             | Parameter to measure Noise Level on current operating channel of AP.   | 0 to -106<br>dBm | -        |  |  |
| Interference                      | Avoidance  |                  |          |  |  |
| Packet<br>Error Rate<br>Threshold | This is a trigger mechanism to move out of current channel when configured threshold is met.                                       | 0-100            | 30%      |  |  |
| Enhanced Ro                       | Enhanced Roaming   |                  |          |  |  |
| Enable                            | Provision to enable enhanced roaming on device.  | -                | Disabled |  |  |
| Roam SNR<br>threshold             | cnPilot device triggers de-authentication of wireless<br>station, when the wireless station is seen at configured<br>SNR or below. | 1-100            | 15dB     |  |  |

To configure the above parameters, navigate to the **Configure > Radio** tab and select **Radio 1 (2.4GHz)** or **Radio 2 (5GHz)** tab and provide the details as given below:

- 1. Select the **Enable** checkbox to enable the operations of this radio.
- 2. Select the primary operating channel from the Channel drop-down list.
- 3. Select the operating width (20 MHz, 40 MHz, or 80 MHz) of the channel from the **Channel Width** drop-down list for 5 GHz only. cnPilot do not support 40 MHz and 80 MHz in 2.4 GHz.
- 4. Select radio transmit power from the Transmit Power drop-down list.
- 5. Enter the beacon interval in the **Beacon Interval** textbox.
- 6. Select Minimum Unicast Rate from the drop-down list
- 7. Select **Highest Basic, Lowest Basic** or **Highest Supported** from the **Multicast data rate** dropdown list.
- 8. Enable Airtime Fairness checkbox.
- 9. Select the preferred Candidate Channels from the drop-down list.
- 10. Select **Mode** details from the drop-down list.
- 11. Enable Short Guard Interval checkbox.
- 12. Click Save.

To configure **Off Channel Scan**:

- 1. Select **Enable** checkbox to enable the operations of this radio.
- 2. Enter **Dwell-Time** in milliseconds in the textbox.

3. Click Save.

To configure Auto-RF:

- 1. Select **Enable** checkbox to enable the operations of this radio.
- 2. Select Channel Selection Mode from the drop-down list.
- 3. Enter Channel Hold Time in minutes in the textbox.
- 4. Enter Channel Utilization Threshold parameter in the textbox.
- 5. Click Save.

To configure Interference Avoidance:

- 1. Enter **Packet Error Rate Threshold** parameter in the textbox.
- 2. Click Save.

### Figure 21 Configure: Radio parameters

| Enable * Enable operation of this nado   Channel Automatic   Operating values Operating values   Mittigeness Enable   Out of the numburno uncest management rule (Mago)   Mode Operating values   Out of the analysis All modes cleants are allowed   Short Guand Interval * Enable Autome Fairness   Out of the analysis All modes cleants are allowed   Short Guand Interval * Enable of S   Out of the analysis Sold operating values   Autor RF Enable   Enable * Enable Autor   Channel Selection Mode Inforternon   Channel Selection Mode Inforternon   Channel Selection Mode Inforternon   Channel Valuzation Threshold 25   Channel Valuzation Threshold 25   Channel Valuzation Threshold 25  | Radio                         |                                |  |
|--|-------------------------------|--------------------------------|--|
| Channel Automatic Pinnary openating channel   Channel Wilthi 20MHz Opening with of the channel   Transnil Power 6 Rado transmit power in dBin (4 to 30, Subject to regulatory imit)   Beacon interval 100 Decon interval in mSec (50 to 340)   Minimum Unicast rate 1 Configure the minimum unicast management rate (Mepa)   Mutticast data rate Highest Basic Data-rate to use for transmission of muticast/broadcast packets   Airtime Fairness Enable Artime Fairness   Candidate Channel All   Mode default Immension   Mode Enable short guard interval   Off Channel Scan   Enable Enable OCS   Dweil-dime 50   Configure Off-Channel-Scan dweltime in mitteeconds (50-300)   Auto RF   Enable Enable Auto RF   Channel Hold Time 120   Channel Hold Time 150  | Enable                        | Enable operation of this radio |  |
| Channel Width Operating width of the channel   Channel Width 20hlHz   G Rado transmit power in dBm (4 to 30, Subject to regulatory limit)   Beacon interval 100   Beacon interval in mSec (50 to 340)   Minimum Unicast rate 1   Multicast data rate Highest Basic   All modes clearts are allowed   Airtine Fairness   Candidate Channels   Minimum Unicast rate   Mode   default   Mode   default   Mode   default   All modes clearts are allowed      Off Channel Scan   Enable   Enable   Short Guard Interval   Enable Autor PF  Channel Scient of the channel (50-300) Configure Off-Channel-Scan dweltime in militecconds (50-300) Auto RF Enable Enable Autor PF  Channel Selection Mode Channel Hild Time 120 Channel Willization Threshold 25  Channel Utilization Threshold 120 Configure channel hold time in minutes (5-100) Configure channel hold time in minutes (5-100) Configure channel Hold time in minutes (5-100) Configure channel Hold time in the index of in the forence Channel Utilization Threshold 26 Channel Villization Threshold 27 Channel Villization Threshold 26 28 29 20  |                               |                                | Primary operating channel  |
| Autor RF     Enable   Enable   Enable   Enable   Enable   Enable   Enable   Configure Off-Channel-Scan dwelfame in milliseconds (50-300) Channel Hold Time   Interference   Autor RF Channel Hold Time   Interference   Autor RF Channel Hold Time   Interference   Configure channel dubtation threshold in % (20-40) Configure channel dubtation threshold in % (20-40)  |                               |                                |  |
| Beacon interval in mSec (50 to 3400)<br>Minimum Unicast rate 100<br>Minimum Unicast rate 11<br>Minimum |                               |                                |  |
| Minimum Unicast rate 1   Minimum Unicast rate 1   Multicast data rate Highest Basic   Orf Channels All   Nocie Gefault   Mode Enable Auto RF   Channel Scan Configure off-Channel-Scan dweffime in millesconds (50-300)   Auto RF Channel Multilation Threshold   Interference Channel Auto RF   Channel Hold Time 120   Channel Auto Threshold 15 (20-40)   | Transmit Power                | 6 •                            | Radio transmit power in dBm (4 to 30, Subject to regulatory limit) |
| Multicast data rate Highest Basic   Airtime Fairness Enable Airtime Fairness   Candidate Channels All   Mode default   Mode default   All modes clients are allowed   Off Channel Scan   Enable Enable Acto RF   Enable Enable Auto RF   Channel Selection Mode Interference   Channel Hold Time 120   Channel Hold Time 120   Channel Utilization Threshold 25   Interference Avoidance   | Beacon Interval               | 100                            | Beacon interval in mSec (50 to 3400)                               |
| Airtime Fairness   Enable Airtime Fairness   Candidate Channels   All   Mode   default   Mode   Gefault   Short Guard Interval   Configure Off-Channel-Scan dwelltme in milliseconds (50-300) Auto RF Enable Enable Auto RF Channel Selection Mode Interference Channel Selection Mode Interference Channel Selection Threshold 25 Configure channel utilization Threshold 25 Configure channel utilization threshold in % (20-40) Interference Avoidance  | Minimum Unicast rate          | 1 <b>v</b>                     | Configure the minimum unicast management rate (Mbps)               |
| Candidate Channels All   Mode default   Short Guard Interval     Off Channel Scan   Enable Enable OCS   Dwell-time     50 Configure Off-Channel-Scan dwelltime in milliseconds (50-300)   Auto RF   Enable     Channel Selection Mode Interference   Channel Hold Time 120   Channel Utilization Threshold 25   Interference Avoidance   | Multicast data rate           | Highest Basic v                | Data-rate to use for transmission of multicast/broadcast packets   |
| Mode defauit   Mode defauit   Short Guard Interval Imable short guard interval   Off Channel Scan   Enable Imable OCS   Dweil-time 50   Configure Off-Channel-Scan dweiltime in milliseconds (50-300)   Auto RF   Enable Imable Auto RF   Channel Selection Mode Interference   Channel Selection Mode Interference   Channel Hold Time 120   Channel Utilization Threshold 25   Configure channel utilization threshold in % (20-40)  | Airtime Fairness              | Enable Airtime Fairness        |  |
| Short Guard Interval     Short Guard Interval     Off Channel Scan     Enable        Configure Off-Channel-Scan dwellime in milliseconds (50-300)     Auto RF        Channel Selection Mode   Interference   Channel Hold Time   120   Configure channel hold time in minutes (5-1800)   Configure channel utilization Threshold   25   | Candidate Channels            | All                            |  |
| Off Channel Scan  Enable Enable OCS  Dwell-time 50  Configure Off-Channel-Scan dwelltime in miliseconds (50-300)  Auto RF  Enable Enable Auto RF  Channel Selection Mode Interference Channel Hold Time 120 Configure channel hold time in minutes (5-1800) Channel Utilization Threshold 25  Interference Avoidance   | Mode                          | default                        | All modes clients are allowed                                      |
| Enable Enable OCS   Dwell-time 50   Configure Off-Channel-Scan dwelltime in milliseconds (50-300)     Auto RF   Enable Enable Auto RF   Channel Selection Mode Interference   Channel Selection Mode 120   Channel Hold Time 120   Channel Utilization Threshold 25   Interference Avoidance   | Short Guard Interval          | Enable short guard interval    |  |
| Enable Enable OCS   Dwell-time 50   Configure Off-Channel-Scan dweltime in milliseconds (50-300)     Auto RF   Enable Enable Auto RF   Channel Selection Mode Interference   Channel Hold Time 120   Channel Utilization Threshold 25   Interference Avoidance   |                               |                                |  |
| Dwell-time       50       Configure Off-Channel-Scan dwelltime in milliseconds (50-300)         Auto RF       Enable       Enable       Enable Auto RF         Channel Selection Mode       Interference       Channel selection done based on interference         Channel Hold Time       120       Configure channel hold time in minutes (5-1800)         Channel Utilization Threshold       25       Configure channel utilization threshold in % (20-40)  | Off Channel Scan              |                                |  |
| Dwell-time       50       Configure Off-Channel-Scan dwelltime in milliseconds (50-300)         Auto RF       Enable       Enable       Enable Auto RF         Channel Selection Mode       Interference       Channel selection done based on interference         Channel Hold Time       120       Configure channel hold time in minutes (5-1800)         Channel Utilization Threshold       25       Configure channel utilization threshold in % (20-40)  |                               |                                |  |
| Auto RF  Enable Channel Selection Mode Interference Channel Selection Mode Interference Channel Hold Time 120 Channel Utilization Threshold 25 Interference Avoidance  | Enable                        | Enable OCS                     |  |
| Enable       Image: Enable Auto RF         Channel Selection Mode       Interference       Channel selection done based on interference         Channel Hold Time       120       Configure channel hold time in minutes (5-1800)         Channel Utilization Threshold       25       Configure channel utilization threshold in % (20-40)  | Dwell-time                    | 50                             | Configure Off-Channel-Scan dwelltime in milliseconds (50-300)      |
| Enable       Image: Enable Auto RF         Channel Selection Mode       Interference       Channel selection done based on interference         Channel Hold Time       120       Configure channel hold time in minutes (5-1800)         Channel Utilization Threshold       25       Configure channel utilization threshold in % (20-40)  |                               |                                |  |
| Channel Selection Mode       Interference       Channel selection done based on interference         Channel Hold Time       120       Configure channel hold time in minutes (5-1800)         Channel Utilization Threshold       25       Configure channel utilization threshold in % (20-40)   | Auto RF                       |                                |  |
| Channel Hold Time     120     Configure channel hold time in minutes (5-1800)       Channel Utilization Threshold     25     Configure channel utilization threshold in % (20-40)  | Enable                        | Enable Auto RF                 |  |
| Channel Utilization Threshold 25 Configure channel utilization threshold in % (20-40)  | Channel Selection Mode        | Interference •                 | Channel selection done based on interference                       |
| Interference Avoidance   | Channel Hold Time             | 120                            | Configure channel hold time in minutes (5-1800)                    |
|  | Channel Utilization Threshold | 25                             | Configure channel utilization threshold in % (20-40)               |
|  |                               |                                |  |
|  | Interference Avoidance        |                                |  |
| Packet Error Rate Threshold 30 Configure packet error rate threshold in % (0-100)  |                               |                                |  |
|  | Packet Error Rate Threshold   | 30                             | Configure packet error rate threshold in % (0-100)                 |
|  |                               |                                |  |
| Save   |                               | Save Cancel                    |  |

### Auto-RF: System release 3.11.4

| Enable                            | Enable Auto RF                          |
|-----------------------------------|---|
| Dynamic Channel Change<br>Options |   |
| Packet Error Rate                 | Enable Packet Error Rate                |
| Channel Utilization               | Enable Channel Utilization              |
| Noise                             | Enable Channel change with higher Noise |

To configure Enhanced Roaming:

- 1. Select the **Enable** checkbox to enable the operations of this radio.
- 2. Enter **Roam SNR threshold** parameter in the textbox.
- 3. Click Save.

Figure 22 Configure: Radio > Enhanced Roaming parameters

| Enable             | Enable active disconnection of clients with weak signal |   |
|--------------------|---|---|
| Roam SNR threshold | 15  | SNR below which clients will be forced to roam (1-100 dB) |
|                    | Save  |   |

# Chapter 8: Configuration - Wireless LAN

This chapter describes the following topics:

- Overview
- Configuring WLAN parameters

### Overview

cnPilot devices support up-to 32 unique WLANs. Each of these WLANs can be configured as per the customer requirement and type of wireless station.

# Configuring WLAN parameters

Configurable parameters under WLAN profile are categorized into two sections:

- 1. Basic
- 2. Advanced

Table 15 lists the configurable parameters for a WLAN profile which is common across bands.

### Table 18 Configure: WLAN > Basic parameters

| Parameters   | Description  | Range | Default                   |
|--------------|--|-------|---------------------------|
| WLAN > Basic |  |       |                           |
| Enable       | Option to enable a WLAN profile. Once enabled, a Beacon<br>is broadcasted with SSID and respective configured<br>parameters in a WLAN profile.   | -     | -                         |
| Mesh         | This parameter is required when a WDS connection is<br>established with cnPilot devices. Four options are<br>available under this parameter:   | -     | OFF<br>(Access<br>Profile |
|              | <ol> <li>Base         A WLAN profile configured with mesh-base will<br/>operate like a normal AP. Its radio will beacon on<br/>startup so its SSID can be seen by radios configured<br/>as mesh-clients.     </li> </ol> |       | Mode)                     |
|              | 2. Client  |       |                           |
|              | A WLAN profile configured with mesh-client will scan<br>all available channels on startup, looking for a mesh-<br>based AP to connect.   |       |                           |
|              | 3. Recovery  |       |                           |
|              |  |       |                           |

| Parameters | Description   | Range  | Default            |
|------------|---|--------|--------------------|
|            | <ul> <li>A WLAN profile configured as mesh-recovery will<br/>broadcast pre-configured SSID upon detection of<br/>mesh link failure after a successful connection. This<br/>needs to be exclusively configured on mesh-base<br/>device. Mesh-client will auto scan for mesh-recovery<br/>SSID upon failure of mesh link.</li> <li>Off<br/>Mesh support disable on WLAN profile.</li> </ul> |        |                    |
| SSID       | SSID is the unique network name that wireless stations scans and associates.  | _      | _                  |
| VLAN       | VLAN is configured to segregate wireless station traffic<br>from AP traffic in the network. Wireless stations obtain IP<br>address from the subnet configured in VLAN field of<br>WLAN profile.   | 1-4094 | 1                  |
| Security   | This parameter determines key values that is encrypted<br>based on selected algorithm. Following security methods<br>are supported by cnPilot devices:  | -      | Open               |
|            | 1. Open   |        |                    |
|            | This method is preferred when Layer 2 authentication<br>is built in the network. With this configured on cnPilot<br>device, any wireless station will be able to connect.   |        |                    |
|            | 2. Osen   |        |                    |
|            | This method is extensively used when Passpoint 2.0 is<br>enabled on cnPilot devices. If Passpoint 2.0 is<br>disabled, this security plays no role in wireless station<br>association.   |        |                    |
|            | 3. WPA2-Pre-Shared Keys   |        |                    |
|            | This mode is supported with AES and TKIP<br>encryption. WPA-TKIP and WPA-AES can be enabled<br>from the CLI with the "allow-tkip" CLI option.   |        |                    |
|            | 4. WPA2 Enterprise  |        |                    |
|            | This security type uses 802.1x authentication to<br>associate wireless stations. This is a centralized<br>system of authentication method. WPA-TKIP and<br>WPA-AES can be enabled from the CLI with the<br>"allow-tkip" CLI option.   |        |                    |
| Passphrase | String that is a key value to generate keys based on security method configured.  | -      | 12345678           |
| Radios     | Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options available to configure transmit mode of SSID:  | _      | 2.4GHz<br>and 5GHz |
|            | • 2.4GHz and 5GHz   |        |                    |

| Parameters       | Description   | Range                        | Default  |
|------------------|---|------------------------------|----------|
|                  | • 2.4GHz  |                              |          |
|                  | • 5GHz  |                              |          |
|                  | For mesh profile, options available are:  |                              |          |
|                  | • 2.4GHz  |                              |          |
|                  | • 5GHz  |                              |          |
| VLAN Pooling     | This parameter is required when user requires to<br>distribute clients across multiple subnets. Different modes<br>of VLAN pooling is supported by cnPilot devices, based<br>on infrastructure available at deployment site. Modes<br>supported are as follows:   | _                            | Disabled |
|                  | 1. Disabled   |                              |          |
|                  | This feature is disabled for this WLAN.   |                              |          |
|                  | 2. Radius Based   |                              |          |
|                  | User is expected to configure WPA2 Enterprise for<br>this mode to support. During association phase,<br>cnPilot obtains pool name form RADIUS transaction<br>and based on present distribution of wireless station<br>across VLANs, cnPilot selects appropriate VLAN and<br>wireless station requests an IP address from the VLAN<br>selected by cnPilot device.  |                              |          |
|                  | 3. Static   |                              |          |
|                  | For this mode to support, user requires to configure<br>VLAN Pool details available under <b>Configure &gt;</b><br><b>Network &gt; VLAN</b> pool. During association phase,<br>cnPilot obtains pool and based on present distribution<br>of wireless station across VLANs, cnPilot selects<br>appropriate VLAN and wireless station requests an<br>IPv4/IPv6 address from the VLAN selected by cnPilot<br>device. |                              |          |
| Max Clients      | This specifies the maximum number of wireless stations<br>that can be associated to a WLAN profile. This varies<br>based on cnPilot device model number. Refer <b>Table 16</b> for<br>more details.   | 1-512<br>(Refer<br>Table 16) | 127      |
| Client Isolation | This feature needs to be enabled when there is a need for<br>prohibition of wireless station to station communication<br>either over the network or on an AP. Three options are<br>available to configure based on requirement:   | _                            | Disabled |
|                  | 1. Disable  |                              |          |
|                  | This option when selected disables client isolation feature. i.e. any wireless station can communicate to other wireless station.   |                              |          |
|                  | 2. Local  |                              |          |

| Parameters                      | Description  | Range         | Default  |
|---------------------------------|--|---------------|----------|
|                                 | This options when selected enables client isolation feature. This option prevents wireless station communications connected to same AP.  |               |          |
|                                 | 3. Network Wide*   |               |          |
|                                 | This options when selected enables client isolation feature. It prevents wireless station communications connected to different AP deployed in same network.   |               |          |
|                                 | 4. Network Wide Static*  |               |          |
|                                 | This option when configured enables client isolation feature across network. User has to configure gateway MAC to access device across subnets.  |               |          |
|                                 | <b>*Note:</b> When selected, user has provision to add MAC addresses to the Client isolation MAC List. Maximum 64 MAC addresses can be added.  |               |          |
| cnMaestro<br>Managed<br>Roaming | By default, cnPilot devices support Layer 2 roaming. This<br>option enables Layer 3 roaming. It is mandatory that<br>cnPilot devices are connected to cnMaestro. Layer 3<br>roaming is valid only for Guest Access.  | _             | Disabled |
| Hide SSID                       | This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.   | _             | Disabled |
| Session<br>Timeout              | This field is specific to non-guest wireless stations. When a<br>wireless station connects, a session timer is triggered.<br>Once session time expires, wireless station must undergo<br>either re-authentication or re-association based on state<br>of wireless station. By default, it is enabled.    | 60-<br>604800 | 28800    |
| Inactivity<br>Timeout           | Inactivity timer triggers whenever there is no<br>communication between cnPilot device and wireless<br>station associated to cnPilot device. Once the timer<br>reaches the configured Inactivity timeout value, APs sends<br>a de-authentication to that wireless station. By default, it<br>is enabled. | 60-28800      | 1800     |
| Drop Multicast<br>Traffic       | When enabled, will drop all multicast flowing in or out of that WLAN.  | -             | Disabled |

To configure the above parameters, navigate to the **Configure > WLAN > Basic** tab and provide the details as given below:

- 1. Select the **Enable** checkbox to enable a particular WLAN.
- 2. Select the operating parameters from the **Mesh** drop-down list.
- 3. Enter the SSID name for this WLAN in the **SSID** textbox.
- 4. Enter the default VLAN assigned to the clients on this WLAN in the **VLAN** textbox.
- 5. Select **Security** type from the drop-down list.
- 6. Enter WPA2 Pre-shared security passphrase or key in the **Passphrase** textbox.

- 7. Select the radio type (2.4GHz, 5GHz) on which the WLAN should be supported from the **Radios** drop-down list.
- 8. Select the required VLAN Pooling parameters from the drop-down list.
- 9. Select Max Clients parameter value from the drop-down list.
- 10. Select the required **Client Isolation** parameter from the drop-down list.
- 11. Enable cnMaestro Managed Roaming checkbox for layer2/layer 3 roaming.
- 12. Enable Hide SSID checkbox.
- 13. Enter the session timeout value in the **Session Timeout** textbox.
- 14. Enter the inactivity timeout value in the **Inactivity timeout** textbox.
- 15. Select Drop Multicast Traffic checkbox to enable dropping multicast traffic.
- 16. Click Save.

Table 19 WLAN (Max Clients) parameters

| Number of Clients            | 2.4GHz | 5GHz | Concurrent |
|------------------------------|--------|------|------------|
| e600 and e700                | 512    | 512  | 512        |
| e410/e410b/e430 and<br>e510  | 256    | 256  | 256        |
| E400 and<br>E500/E501S/e502S | 256    | 128  | 256        |
| e425H and e505               | 100    | 100  | 100        |

### Figure 23 Configure: WLAN > Basic parameter

| - Basic                   |   |  |
|---------------------------|---|--|
| Busic                     |   |  |
| Enable                    | 2   |  |
| Mesh                      | Off   | Mesh Base/Client/Recovery mode   |
| SSID                      | \$I22I_Test_TSK_Base  | The SSID of this WLAN (upto 32 characters)   |
| VLAN                      | 1   | Default VLAN assigned to clients on this WLAN. (1-4094)  |
| Security                  | WPA2 Pre-shared Keys  | Set Authentication and encryption type   |
| Passphrase                |   | WPA2 Pre-shared Security passphrase or key   |
| Radios                    | 5GHz v  | Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported   |
| VLAN Pooling              | Disable •   | Configure VLAN pooling   |
| Max Clients               | 126   | Default maximum Client assigned to this WLAN. (1-256)  |
| Client Isolation          | Disable   | When selected, it allows wireless clients connected to the same AP or different APs to<br>communicate with each other in the same VLAN |
| cnMaestro Managed Roaming | Enable centralized management of roaming for wireless clients | hrough cnMaestro   |
| Hide SSID                 | Do not broadcast SSID in beacons                              |  |
| Session Timeout           | 28800   | Session time in seconds (60 to 604800)   |
| Inactivity Timeout        | 1800  | Inactivity time in seconds (60 to 28800)   |
| Drop Multicast Traffic    | Drop the send/receive of multicast traffic                    |  |
|                           |   |  |

| Parameters       | Description  |  |  |                              | Range           | Default     |          |
|------------------|--|--|--|------------------------------|-----------------|-------------|----------|
| WLAN > Adva      | inced  |  |  |                              |                 |             |          |
| UAPSD            | When enabled, cnPilot devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming etc. is in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by cnPilot device. |  |  |                              |                 | 5           | Disabled |
|                  | Priority   | 802.1D Priority<br>(= UP)  | 802.1D Designation   | Access Category              | WMM Designation |             |          |
|                  | lowest   | 1  | BK   |                              |                 |             |          |
|                  | Iowest   | 2  | 2  | AC_BK                        | Background      |             |          |
|                  |  | 0  | BE   |                              |                 |             |          |
|                  |  | 3  | EE   | AC_BE                        | Best Effort     |             |          |
|                  |  | 4  | CL   |                              |                 |             |          |
|                  |  | 5  | VI   | AC_VI                        | Video           |             |          |
|                  |  | 6  | VO   |                              |                 |             |          |
|                  | highest  | 7  | NC   | AC_VO                        | Voice           |             |          |
| DTIM<br>interval | Availabl<br>in this IE<br>This par<br>support<br>field wh  | ivity. Stat<br>le admissio<br>ameter pla<br>ed mobile s<br>en enabled<br>ticast fram | 1-255  | 1                            |                 |             |          |
| Monitored Hos    | st   |  |  |                              |                 |             |          |
| Host             | backboı<br>reachab   | ne network<br>pility of host   | ired where th<br>. cnPilot devic<br>:name/IP con<br>:ate of WLAN | ce monitors<br>figured in th | the             | -           | Disabled |
| Interval         | The frequency of monitoring the network health based on<br>the status of keep-alive mechanism w.r.t configured<br>monitored host.  |  |  |                              |                 | 60-3600 Sec | 300      |
| Attempts         | The number of packets in the keep-alive mechanism to determine the status.   |  |  |                              |                 | 1-20        | 1        |

### Table 20 Configure: WLAN > Advanced parameters

| Parameters                    | Description   | Range | Default  |
|-------------------------------|---|-------|----------|
| DNS<br>Logging<br>Host        | This feature is required when an Administrator requires to<br>monitor the websites accessed by wireless stations<br>connected to WLAN profile.  | -     | Disabled |
| Connection<br>Logging<br>Host | When enabled provides information of all TCP connections accessed by a wireless station that is associated to WLAN.   | -     | Disabled |
| Band<br>Steering              | <ul> <li>This feature when enabled, steers wireless stations to connect to 5GHz. There are three modes supported by cnPilot device. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces wireless station to connect to 5GHz band.</li> <li>Low</li> <li>Normal</li> <li>Aggressive</li> </ul> | _     | Disabled |
| Proxy ARP                     | Provision to avoid ARP flood in wireless network. When<br>enabled, AP responds to ARP requests for the wireless<br>stations connected to that AP. This is for IPv4<br>infrastructure.   | -     | Enabled  |
| Proxy ND                      | Provision to avoid ARP flood in wireless network. When<br>enabled, AP responds to ARP requests for the wireless<br>stations connected to that AP. This is for IPv6<br>infrastructure.   | -     | Disabled |
| Unicast<br>DHCP               | Provision to transmit DHCP offer and ACK/NACK packets as Unicast packets to wireless stations.  | -     | Enabled  |
| Insert DHCP<br>Option 82      | When enabled, DHCP packets generated from wireless<br>stations that are associated to APs are appended with<br>Option 82 parameters. Option 82 provides provision to<br>append Circuit ID and Remote ID. Following parameters<br>can be selected in both Circuit ID and Remote ID:  | _     | Disabled |
|                               | Hostname  |       |          |
|                               | AP MAC  |       |          |
|                               | BSSID   |       |          |
|                               | • SSID  |       |          |
|                               | VLAN ID   |       |          |
|                               | <ul><li>Site ID</li><li>Custom</li></ul>  |       |          |
|                               | All   |       |          |
|                               | - / All   |       |          |

| Parameters                    | Description  | Range  | Default  |
|-------------------------------|--|--|----------|
| Tunnel Mode                   | This option is enabled when user traffic is tunneled to DMZ network either using L2TP or L2GRE.  | _  | Disabled |
| Fast-<br>Roaming<br>Protocol  | <ul> <li>One of the important aspects to support voice applications on Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 msec to avoid any call drop. This is easily achievable when WPA2-PSK security mechanism is in use. However, in enterprise environments there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with AAA server and hence depending on the location of AAA server the roaming-time will be above 700 msec.</li> <li>Select any one of the following:</li> <li><b>1.</b> OKC</li> <li>This roaming method is a proprietary solution to bring scalability to the roaming problem. This method avoids the need to authenticate with AAA server every time a client moves to new AP.</li> <li><b>802.11r</b></li> <li>This is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). Two modes of FT roaming are supported: <ul> <li>Over-the-Air</li> <li>By default, this is enabled.</li> <li>Over-the-DS</li> </ul> </li> </ul> |  | Disabled |
| Re-<br>association<br>Timeout | It's the number of seconds after which the reassociation<br>attempt of a client to an AP should timeout. This is<br>applicable only when FT roaming is enabled.  | 1-100  | 20       |
| RRM<br>(802.11k)              | <ul> <li>AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 11k clients.</li> <li>Following parameters needs to be enabled: <ul> <li>Enable OCS</li> <li>Enable RRM</li> <li>Support for WPA2 authentication method</li> </ul> </li> </ul>  | _  | Disabled |
| PMF<br>(802.11w)              | 802.11w, also termed as Protected Management Frames<br>(PMF) Service, defines encryption for management<br>frames. Unencrypted management frames makes wireless<br>connection vulnerable to DoS attacks as well as they<br>cannot protect important information exchanged using<br>management frames from eavesdroppers.   | <ul><li> Optional</li><li> Mandatory</li><li> Disabled</li></ul> | _        |

| Parameters                      | Description  | Range   | Default |
|---------------------------------|--|---------|---------|
| SA Query<br>Retry Time          | The legitimate 802.11w client must respond with a<br>Security Association (SA) Query Response frame within a<br>pre-defined amount of time (milliseconds) called the SA<br>Query Retry time. | 100-500 | 100ms   |
| Association<br>Comeback<br>Time | This value is included in the Association Response as<br>an Association Comeback Time information element. AP<br>will deny association for the configured interval.                          | 1-20    | 1 Sec   |

To configure the above parameters, navigate to the **Configure > WLAN > Basic** tab and provide the details as given below:

- 1. Select the **UAPSD** checkbox to enable UAPSD.
- 2. Select the **QBSS** checkbox to enable QBSS.
- 3. Enter the value in the **DTIM interval** textbox to configure DTIM interval.
- 4. Enter IP address or Hostname in Host textbox.
- 5. Enter **Interval** time duration in the textbox.
- 6. Select number of attempts to check the reachability of monitored host in the **Attempts** dropdown list.
- 7. Enter an IP Address or Hostname in the Monitored Host textbox.
- 8. Enter the FQDN or IP address of the Server where all the client DNS requests will be logged in the **DNS Logging Host** server along with customized port number in the textbox. If the port number is not entered, AP will take default value as 514.
- 9. Enter the FQDN or IP address of the Server where all wireless client connectivity events/logs will be displayed in the configured **Connection Logging Host** server along with customized port number in the textbox. If the port number is not entered, AP will take default value as 514.
- 10. Select Band Steering parameter for 5GHz band from the drop-down list.
- 11. Enable **Proxy ARP** checkbox to avoid ARP flood in wireless network.
- 12. Enable Proxy ND checkbox to avoid ARP flood in wireless network.
- 13. Enable **Unicast DHCP** checkbox to Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients.
- 14. Enable Insert DHCP Option 82 checkbox.
- 15. Select Option 82 Circuit ID to enable DHCP Option-82 from the drop-down list.
- 16. Select **Option 82 Remote ID** to choose the MAC address of the AP from the drop-down list.
- 17. Select Tunnel Mode checkbox to enable tunnelling of WLAN traffic over configured tunnel.
- 18. Enable the required **OKC or 802.11r** configure roaming protocol in the **Fast-Roaming Protocol** checkbox.
- 19. Enable RRM (802.11k) checkbox.
- 20. Select PMF (802.11w) parameter from the drop-down list.
  - a. Enter **SQ Query Retry Time** in the textbox.
  - b. Enter Association Comeback Time in the textbox.
- 21. Click Save.

|                             | UAPSD           | Enable UAPS   | D                  |              |  |
|-----------------------------|-----------------|---------------|--------------------|--------------|--|
|                             | QBSS            | Enable QBSS   | load element       |              |  |
|                             | DTIM interval   | 1             |                    |              | Number of beacons (1-255)  |
|                             | - Monitored     | Host          |                    |              |  |
|                             | Host            |               |                    |              | or Hostname that should be<br>or this WLAN to be active              |
|                             | Interval        | 300           |                    | Duration in  | seconds (60-3600)  |
|                             | Attempts        | 5             |                    |              | attempts to check the reachability<br>d host (1-20)                  |
| DN                          | IS Logging Host |               | Port               | 514          | Syslog server where all client DNS requests will be logged           |
| Connectio                   | on Logging Host |               | Port               | 514          | Syslog server where all client connection requests will be<br>logged |
| Band Steering               |                 | Disabled      |                    | •            | Steer dual-band capable clients towards 5GHz radio                   |
|                             | Proxy ARP       | Respond to A  | RP requests autor  | matically on | behalf of clients  |
|                             | Proxy ND        | Respond to ip | v6 ND requests a   | utomatically | on behalf of clients   |
|                             | Unicast DHCP    | Convert DHCI  | P-OFFER and DH     | CP-ACK to    | unicast before forwarding to clients                                 |
| Insert                      | DHCP Option 82  | Enable DHCP   | Option 82          |              |  |
|                             | Tunnel Mode     | Enable tunnel | ling of WLAN traff | ic over conf | gured tunnel   |
| Fast-Re                     | paming Protocol | ☑ OKC ☑ 802.  | 11r Configure      | roaming pro  | otocol   |
|                             | Over-the-DS     | 0             |                    |              |  |
| Re-asso                     | ciation Timeout | 20            |                    |              | Number of seconds (1-100)  |
|                             | RRM (802.11k)   | Enable Radio  | Resource Measu     | rements (80  | 2.11k)   |
|                             | PMF (802.11w)   | Optional      |                    | Ŧ            |  |
| SAG                         | uery Retry Time | 100           |                    |              | Number of msec (100-500)   |
| Association Comeback Time 1 |                 |               |                    |              | Number of seconds (1-20)   |

Figure 24 Configure: WLAN > Advanced parameter

| Parameters                    | Description  | Range | Default         |
|-------------------------------|--|-------|-----------------|
| Authentication<br>Server      | Provision to configure RADIUS Authentication server<br>details such as Hostname/IPv4/IPv6, Shared Secret, Port<br>Number and Realm. Maximum of three RADIUS server<br>can be configured.           | -     | Disabled        |
| Accounting<br>Server          | Provision to configure Accounting server details such as<br>Hostname/IPv4/IPv6, Shared Secret, Port Number.<br>Maximum of three RADIUS server can be configured.                                   | _     | Disabled        |
| Timeout                       | Wait time period for response from AAA server.   | 1-30  | 3               |
| Attempts                      | Parameter to configure number of attempts that a device<br>should send AAA request to server if no response is<br>received within configured timeout period.                                       | 1-3   | 1               |
| Accounting<br>Mode            | This field is enabled based on customer requirement.<br>Accounting packet is transmitted based on mode<br>selected.  | _     | Disabled        |
|                               | 1. Start-Stop  |       |                 |
|                               | Accounting packets are transmitted by AP to AAA server when a wireless station is connected and then disconnects.  |       |                 |
|                               | 2. Start-Interim-Stop  |       |                 |
|                               | Accounting packets are transmitted by AP to AAA<br>server when a wireless station connects and then at<br>regular intervals of configured Interim Update Interval<br>and then when it disconnects. |       |                 |
|                               | 3. None  |       |                 |
|                               | Accounting mode will be disable.   |       |                 |
| Accounting<br>Packet          | When enabled, Accounting-On is sent for every client when connected.   | _     | Disabled        |
| Sync<br>Accounting<br>Records | When enabled, will share the accounting records when<br>wireless stations move across different AP that are Layer<br>2 connected.  | -     | Disabled        |
| Server Pool<br>Mode           | User can configure multiple Authorization and Accounting servers. Based on number of wireless stations, user can choose either Failover or Load Balance mode.                                      | _     | Load<br>Balance |
|                               | 1. Load Balance  |       |                 |
|                               | AP communicates with multiple servers and ensures<br>that authorization and accounting are equally shared<br>across configured servers.  |       |                 |
|                               | 2. Failover  |       |                 |

### Table 21 Configure: WLAN > Radius Server parameters

| Parameters                 | Description   | Range    | Default                     |
|----------------------------|---|----------|-----------------------------|
|                            | AP selects the RADIUS server which is up and running based on the order of configuration.   |          |                             |
| NAS Identifier             | This is configurable parameter and is appended in RADIUS request packet.  | _        | Hostname/<br>System<br>Name |
|                            | 1. AP-ETHO-MAC:   |          |                             |
|                            | NAS identifier attribute will be ETH0 MAC address   |          |                             |
|                            | 2. WLAN-BSSID:  |          |                             |
|                            | NAS identifier attribute will be WLAN-BSSID   |          |                             |
|                            | 3. Custom:  |          |                             |
|                            | Any custom value  |          |                             |
| NAS IP                     | NAS-IP attribute for use in RADIUS request packets.<br>Default is set to device IP and option to configure custom<br>IP address with the option <b>Custom.</b>                        | -        | AP-IP                       |
| Interim Update<br>Interval | This field is used when RADIUS accounting is enabled, and mode selected as Start-Interim-Stop.  | 10-65535 | 1800                        |
| Dynamic<br>Authorization   | This option is required, where there is a CoA requests from AAA/RADIUS server.  | -        | Disabled                    |
| Dynamic<br>VLAN            | When enabled, AP honors the VLAN information<br>provided in RADIUS transaction. Wireless station<br>requests IP address from the same VLAN learnt through<br>RADIUS.                  | -        | Enabled                     |
| Proxy through<br>cnMaestro | This option is enabled, whenever cnMaestro is required to<br>act as proxy server to RADIUS authentication requests<br>coming from cnPilot devices that are connected to<br>cnMaestro. | -        | Disabled                    |
| Called Station<br>ID       | Following information can be communicated to RADIUS server:   |          | AP-MAC:<br>SSID             |
|                            | • AP-MAC  |          |                             |
|                            | AP-MAC: SITE-NAME   |          |                             |
|                            | AP-MAC: SSID  |          |                             |
|                            | AP-MAC: SSID-SITE-NAME  |          |                             |
|                            | • AP-NAME   |          |                             |
|                            | AP-NAME: SITE-NAME  |          |                             |
|                            | AP-NAME: SSID   |          |                             |
|                            | • SITE-NAME   |          |                             |
|                            | • SSID  |          |                             |
|                            | CUSTOM  |          |                             |

To configure the above parameters, navigate to the **Configure > WLAN** tab and select **Radius Server** tab and provide the details as given below:

- 1. Enter the RADIUS Authentication server details such as Hostname/Shared Secret/Port Number/ Realm in the **Authentication Server 1** textbox.
- 2. Enter the time in seconds of each request attempt in **Timeout** textbox.
- 3. Enter the number of attempts before a request is given up in the **Attempts** textbox.
- 4. Select the configuring Accounting Mode from the drop-down list.
- 5. Enable Accounting Packet checkbox.
- 6. Enable Sync Accounting Records checkbox to enable sync accounting records configuration.
- 7. Enable Load Balance/Failover in the Server Pool Mode checkbox.
- 8. Enter the NAS Identifier parameter in the textbox.
- 9. Enter the Interim Update Interval parameter value in the textbox.
- 10. Enable Dynamic Authorization checkbox to configure dynamic authorization for wireless clients.
- 11. Enable **Dynamic VLAN** checkbox.
- 12. Enable **Proxy through cnMaestro** checkbox.
- 13. Select Called Station ID from the drop-down list.
- 14. Click Save.

#### Table 22 NAS IP with AP dual stack

| IPv6 preference | AP Address Mode | NAS ID |
|-----------------|-----------------|--------|
| Yes             | DUAL STACK      | IPv6   |
| No              | DUAL STACK      | IPv4   |
| Yes             | IPv6 only       | IPv6   |
| No              | IPv6 only       | IPv6   |
| Yes             | IPv4 only       | IPv4   |
| No              | IPv4 only       | IPv4   |

|                         | Radius Server | Guest Access      | Usage Limits | Scheduled Access                                 | Access  | Passpoint          |                         |                                 |  |
|-------------------------|---------------|-------------------|--------------|--|---|--------------------|-------------------------|---------------------------------|--|
| Authentication Server 1 |               | Host              | Se           | ecret  |   | Port               | Realm                   |                                 |  |
|                         |               |                   | 10.110.200.  | •  | •••••   |                    | 1812                    |                                 |  |
|                         |               | 2                 | Host         | Se   | ecret   |                    | Port                    | Realm                           |  |
|                         |               |                   |              |  |   |                    | 1812                    |                                 |  |
|                         |               | 3                 | Host         | Se   | ecret   |                    | Port                    | Realm                           |  |
|                         |               |                   |              |  |   |                    | 1812                    |                                 |  |
|                         |               | Timeout           | 3            | Timeo  | ut in seconds of e  | ach request att    | tempt (1-30)            |                                 |  |
|                         |               | Attempts          | 1            | Numb   | er of attempts bel  | ore giving up (1   | (-3)                    |                                 |  |
|                         | Acc           | ounting Server 1  | Host         | Se   | ecret   |                    | Port                    |                                 |  |
|                         |               |                   |              |  |   |                    | 1813                    |                                 |  |
|                         |               | 2                 | Host         | Se   | ecret   |                    | Port                    |                                 |  |
|                         |               |                   |              |  |   |                    | 1813                    |                                 |  |
|                         |               | 3                 | Host         | Se   | ecret   |                    | Port                    |                                 |  |
|                         |               |                   |              |  |   |                    | 1813                    |                                 |  |
|                         |               | Timeout           | 3            | Timeo  | ut in seconds of e  | ach request att    | tempt (1-30)            |                                 |  |
|                         |               | Attempts          | 1            | Numb   | er of attempts bel  | ore giving up (1   | (-3)                    |                                 |  |
|                         |               | Accounting Mode   | None         | ✓ Cont   | figure accounting   | mode               |                         |                                 |  |
|                         | A             | ccounting Packet  | Enable Acc   | ounting-On messages                              |   |                    |                         |                                 |  |
|                         | s             | Server Pool Mode  |              | ce Load balance requi<br>ove down server list wh |   |                    |                         |                                 |  |
|                         |               | NAS Identifier    | AP-HOSTNA    | ME   | ✓ NAS-la  | entifier attribute | e for use in Request pa | ackets. Defaults to system name |  |
|                         |               | NAS IP            | AP-IP        |  | ✓ NAS-IF  | attribute for us   | e in Request packets.   | Defaults to Device IP           |  |
|                         | Interir       | n Update Interval | 1800         | Interva  | Interval for RADIUS Interim-Accounting updates (10-65535 Seconds) |                    |                         |                                 |  |
|                         | Dynar         | nic Authorization | Enable RAD   | IUS dynamic authoriza                            | tion (COA, DM m   | essages)           |                         |                                 |  |
|                         |               | Dynamic VLAN      | ✓ Enable RAD | IUS assigned VLANs                               |   |                    |                         |                                 |  |
|                         | Proxy th      | rough cnMaestro   | Proxy RADI   | US packets through cnl                           | Maestro (on-prem  | ises) instead of   | f directly to the RADIU | S server from the AP            |  |
|                         | -             | Called Station ID | AP-MAC:SSI   |  |   |                    |                         | d in the RADIUS packet          |  |
|                         |               |                   |              | _  | ave Cancel  |                    |                         |                                 |  |

| Figure 25 Configure: WLAN | Radius Server parameter |
|---------------------------|-------------------------|
|---------------------------|-------------------------|

### Table 23 Configure: WLAN > Guest Access > Internal Access Point parameters

| Parameters                                  | Description  | Range | Default      |  |
|---|--|-------|--------------|--|
| WLAN > Guest Access > Internal Access Point |  |       |              |  |
| Enable                                      | Enables the Guest Access feature.  | -     | Disabled     |  |
| Access Policy                               | There are four types of access types provided for the user:                                  | _     | Clickthrough |  |
|   | 1. Clickthrough  |       |              |  |
|   | This mode allows the users to get access data without any authentication mechanism. User can |       |              |  |

| Parameters           | Description   | Range                   | Default   |
|----------------------|---|-------------------------|---|
|                      | access internet as soon as he is connected and accepts <b>Terms and Conditions</b> .  |                         |   |
|                      | 2. RADIUS   |                         |   |
|                      | This mode when selected, user has to provide<br>username and password, which is then redirected<br>to RADIUS server for authentication. If successful,<br>user is provided with data access.  |                         |   |
|                      | 3. LDAP   |                         |   |
|                      | This mode when selected, user has to provide<br>username and password, which is then redirected<br>to LDAP server for authentication. If successful,<br>user is provided with data access.  |                         |   |
|                      | 4. Local Guest Account  |                         |   |
|                      | User must configure username and password on device, which has to be provided in the redirection page for successful authentication and data access.  |                         |   |
| Redirect Mode        | This option helps the user to configure the HTTP or HTTPS mode of redirection URL.  | _                       | HTTP  |
|                      | 1. HTTP   |                         |   |
|                      | AP sends a HTTP POSTURL to the associated client, which will be http:// <pre-defined-url>.</pre-defined-url>  |                         |   |
|                      | 2. HTTPS  |                         |   |
|                      | AP sends HTTPS POSTURL to the successful associated client, which will be https:// <pre-defined-url>.</pre-defined-url>   |                         |   |
| Redirect<br>Hostname | User can configure a friendly hostname, which is added<br>in DNS server and is resolvable to cnPilot IP address.<br>This parameter once configured will be replaced with IP<br>address in the redirection URL provided to wireless<br>stations. | _                       | -   |
| Title                | User can configure a Title to the splash page. Configured<br>text in this parameter will be displayed in the redirection<br>page. This text is usually Bold.  | Up to 255<br>characters | Welcome To<br>Cambium<br>Powered<br>Hotspot                         |
| Contents             | User can configure the contents of Splash page using<br>this field. Displays the text configured under the Title<br>section of redirection page.  | Up to 255<br>characters | Please enter<br>username<br>and<br>password to<br>get Web<br>Access |
| Terms                | Splash page displays the text configured when user accepts <b>Terms and Agreement</b> .   | Up to 255<br>characters | -   |

| Parameters                             | Description  | Range | Default                 |
|--|--|-------|-------------------------|
| Logo                                   | Displays the logo image updated in URL<br>http(s):// <ipaddress>/logo.png. Either PNG or JPEG<br/>format of logo are supported.</ipaddress>  | _     | _                       |
| Background<br>Image                    | Displays the background image updated in URL<br>http(s):// <ipaddress>/backgroundimage.png. Either<br/>PNG or JPEG format of logo are supported.</ipaddress>   | -     | -                       |
| Success<br>Action                      | Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL:   | -     | Internal<br>Logout page |
|  | 1. Internal Logout Page  |       |                         |
|  | After successful login, wireless client is redirected to logout page hosted on AP.   |       |                         |
|  | 2. Redirect user to External URL   |       |                         |
|  | Here users will be redirected to URL which is<br>configured on device in Redirection URL<br>configurable parameter.  |       |                         |
|  | 3. Redirect user to Original URL   |       |                         |
|  | Here users will be redirected to URL that is accessed by user before successful captive portal authentication.   |       |                         |
| Redirect user<br>to External<br>URL    | Provision to configure re-direction URL after successful login and an additional information of AP and wireless station information can be appended in the URL.  | -     | -                       |
|  | Prefix Query Strings in Redirect URL   |       |                         |
|  | This option is selected by default. Following information is appended in the redirection URL:  |       |                         |
|  | o SSID   |       |                         |
|  | o AP MAC   |       |                         |
|  | • NAS ID   |       |                         |
|  | ο ΑΡΙΡ   |       |                         |
|  | <ul> <li>Client MAC</li> </ul>   |       |                         |
|  | • Redirection URL  |       |                         |
|  | • User can provide either HTTP or HTTPS URL  |       |                         |
| Redirection<br>user to<br>Original URL | Users will be redirected to URL that is accessed by user<br>before successful captive portal authentication. There is<br>additional parameter Prefix Query Strings in Redirection<br>URL that is enabled by default and details given below: | -     | _                       |
|  | Prefix Query Strings in Redirect URL   |       |                         |
|  | This option is selected by default. Following information is appended in the redirection URL:  |       |                         |

| Parameters                             | Description  | Range           | Default  |
|--|--|-----------------|----------|
|  | <ul> <li>SSID</li> <li>AP MAC</li> <li>NAS ID</li> <li>AP IP</li> <li>Client MAC</li> </ul>  |                 |          |
| Success<br>message                     | Provision to configure text to display upon successful<br>Guest Access authentication. This is applicable only<br>when Success Action mode is Internal Logout Page.  | _               | -        |
| Redirect                               | <ul> <li>If enabled, only HTTP URLs will be redirected to<br/>Guest Access login page.</li> <li>If disabled, both HTTP and HTTPs URLs will be<br/>redirected to Guest Access login page.</li> </ul>                                  | -               | Enabled  |
| Redirect User<br>Page                  | IPv4/IPv6 address configured in this field is used as<br>logout URL for Guest Access sessions. IPv4/IPv6<br>address configured should be not reachable to internet.  | _               | 1.1.1.1  |
| Proxy<br>Redirection<br>Port           | Proxy port can be configured with which proxy server is<br>enabled. This allows URL's accessed with proxy port to<br>be redirected to login page.  | 1 - 65535       | -        |
| Session<br>Timeout                     | This is the duration of time, client will be allowed to<br>access internet if quota persists, after which AP sends<br>de-authentication. Wireless station has to undergo Guest<br>Access authentication after session timeout.       | 60 -<br>2592000 | 28800    |
| Inactivity<br>Timeout                  | Provision to configure timeout period to disconnect<br>wireless stations that are associated but no data traffic.<br>AP starts timer when there is no data received from a<br>wireless station and disconnects when timer reaches 0. | 60 -<br>2592000 | 1800     |
| MAC<br>Authentication<br>Fallback      | It's a mechanism in which wireless stations will be<br>redirected to Guest Access login page after any<br>supported type of MAC address authentication fails.  | _               | Disabled |
| Extend<br>Interface                    | Provision to support Guest Access on Ethernet interface.   | -               | Disabled |
| Whitelist                              | Provision to configure either IPv4/IPv6 or URLs to<br>bypass traffic, therefor user can access those IPs or<br>URLs without Guest Access authentication.   | -               | -        |
| Captive Portal<br>bypass User<br>Agent | Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.  | _               | -        |

To configure the above parameters, navigate to the **Configure > WLAN > Guest Access** tab and provide the details as given below:

- 1. Select **Enable** checkbox to enable the Guest Access feature.
- 2. Enable Internal Access Point checkbox.
- 3. Enable the required access types from the Access Policy checkbox.
- 4. Enable HTTP or HTTPS from the Redirect Mode checkbox.
- 5. Enter **Redirect Hostname** in the textbox.
- 6. Enter the title to appear in the splash page in the **Title** textbox.
- 7. Enter the content to appear in the splash page in the **Contents** textbox.
- 8. Enter the terms and conditions to appear in the splash page in the **Terms** textbox.
- 9. Enter the logo to be displayed in the **Logo** textbox.
- 10. Select the **Background Image** to be displayed on the splash page in the textbox.
- 11. Enable configured modes of redirection URL in **Success Action** checkbox.
- 12. Enter Success message to appear in the textbox.
- 13. Enable **Redirect** checkbox for HTTP packets.
- 14. Enter configuring IP address in the **Redirect User Page** textbox.
- 15. Enter Port number in the Proxy Redirection Port textbox.
- 16. Enter the session timeout in seconds in the **Session Timeout** textbox.
- 17. Enter the inactivity timeout in seconds in the Inactivity Timeout textbox.
- 18. Enable **MAC Authentication Fallback** checkbox if guest-access is used only as fallback for clients failing MAC-authentication.
- 19. Enter the name of the interface that is extended for guest access in the **Extend Interface** textbox.
- 20. Click Save.

To configure Whitelist parameter:

- 1. Enter the IP address or the domain name of the permitted domain in the **IP Address** or **Domain Name** textbox.
- 2. Click Save.

### To configure the Captive Portal bypass User Agent parameter:

- 1. Select **Index** parameter value from the drop-down list.
- 2. Enter User Agent String parameter in the textbox.
- 3. Select Status Code from the drop-down list.
- 4. Enter HTML Response in the textbox.
- 5. Click Save.

| Basic Radius Server Guest Access Usage Limits Scheduled Acce | ess Access Passpoint   |
|--|--|
|  |  |
| Enable 🗎   |  |
| Portal Mode  | Internal Access Point   External Hotspot  cnMaestro  |
|  | Clickthrough Splash-page where users accept terms & conditions to get on the network   |
|  | Radius Splash-page with username & password, authenticated with a RADIUS server<br>LDAP Redirect users to a login page for authentication by a LDAP server |
|  | Local Guest Account Redirect users to a login page for authentication by local guest user account  |
|  | HTTP Use HTTP URLs for redirection   |
| Redirect Hostname  | HTTPS Use HTTPS URLs for redirection   |
|  | direct Hostname for the splash page (up to 255 chars)  |
| Title  |  |
| Titl   | le text in splash page (up to 255 chars)   |
| Contents   |  |
|  | ain contents of the splash page (up to 255 chars)  |
| Terms  | ms 2 conditions displayed in the solach name (in to 255 chare)   |
|  | rms & conditions displayed in the splash page (up to 255 chars)  |
|  | g: http://domain.com/logo.png<br>.ogo to be displayed on the splash page   |
|  | g: http://domain.com/backgroundImage.jpg   |
|  | Background image to be displayed on the splash page  |
| Success Action   | Internal Logout Page @ Redirect user to External URL @ Redirect user to Original URL   |
| Success message  |  |
| Redirect @   | HTTP-only Enable redirection for HTTP packets only   |
| Redirect User Page 1   | .1.1.1   |
|  | Configure IP address for redirecting user to guest portal splash page  |
| Proxy Redirection Port                                       | Port number(1 to 65535)  |
| Session Timeout 28   | 8800 Session time in seconds (60 to 2592000)   |
| Inactivity Timeout 1   | 800 Inactivity time in seconds (60 to 2592000)   |
|  | Use guest-access only as fallback for clients failing MAC-authentication   |
| Extend Interface   | Configure the interface which is extended for guest access   |
|  | Save Cancel  |
| -  |  |
|  | Add Whitelist Caplive Portal bypass User Agent   |
|  |  |
|  | IP Address or Domain Name Save   |
|  |  |
|  | IP Address   Domain Name  V Action   |
|  |  |
|  | No white list available  |
|  |  |
|  |  |
|  |  |
|  | y.   |
|  | I I L1 I I I I I I I I I I I I I I I I I   |
|  |  |

### Figure 26 Configure: WLAN > Guest Access > Internal Access Point parameter

| Parameters                       | Description  | Range | Default      |
|----------------------------------|--|-------|--------------|
| WLAN > Guest A                   | Access > External Hotspot  |       |              |
| Access Policy                    | There are four types of access types provided for the end user:  | -     | Clickthrough |
|                                  | 1. Clickthrough  |       |              |
|                                  | This mode allows users to get access data without<br>any authentication mechanism. User can access<br>internet as soon as he is connected and accepts<br><b>Terms and Conditions</b> . |       |              |
|                                  | 2. RADIUS  |       |              |
|                                  | User has to provide username and password, which<br>is then redirected to RADIUS server for<br>authentication. If successful, user is provided with<br>data access.                    |       |              |
|                                  | 3. LDAP  |       |              |
|                                  | User must provide username and password, which<br>is then redirected to LDAP server for<br>authentication. If successful, user is provided with<br>data access.                        |       |              |
|                                  | 4. Local Guest Account   |       |              |
|                                  | User has to configure username and password on device, which has to be provided in the redirection page for successful authentication and data access.                                 |       |              |
| LDAP Server<br>baseDN            | Provision to configure the point from where the server will search for users.  | -     | _            |
| LDAP Server<br>adminDN           | Provision to configure the Admin Domain which binds with LDAP server for successful search of LDAP/AD server.  | -     | _            |
| LDAP Server<br>Admin<br>Password | Provision to configure Admin password of LDAP/AD<br>server to search all organizational unit defined in a<br>Domain component.   | -     | -            |
| Redirect Mode                    | Provision to configure the HTTP or HTTPS mode of redirection URL.  | -     | НТТР         |
|                                  | 1. HTTP  |       |              |
|                                  | AP sends a HTTP POSTURL to the associated client, which will be http:// <pre-defined-url>.</pre-defined-url>   |       |              |
|                                  | 2. HTTPS   |       |              |
|                                  | AP sends HTTPS POSTURL to the successful associated client, which will be https:// <pre-defined-url>.</pre-defined-url>  |       |              |

| Parameters                                   | Description  | Range  | Default                    |
|--|--|--------|----------------------------|
| Redirect<br>Hostname                         | User can configure a friendly hostname, which is added<br>in DNS server and is resolvable to cnPilot IP address.<br>This parameter once configured will be replaced with IP<br>address in the redirection URL provided to wireless<br>stations.  | _      | _                          |
| WISPr Clients<br>External Server<br>Login    | Provision to enable re-direction of guest access portal URL obtained through WISPr.  | -      | Disabled                   |
| External Page<br>URL                         | User can configure landing/login page which is posted to wireless stations that are not Guest Access authenticated.  | _      | -                          |
| External Portal<br>Post Through<br>cnMaestro | This is required when HTTPS is only supported by<br>external guest access portal. This option when enabled<br>minimizes certification. Certificate is required to install<br>only in cnMaestro On-Premises.  | -      | Disabled                   |
| External Portal<br>Type                      | <ul> <li>Two modes of portal types are supported by cnPilot products.</li> <li><b>1.</b> Standard <ul> <li>This mode is selected, for all third-party vendors whose Guest Access services is certified and integrated with cnPilot products.</li> </ul> </li> <li><b>2.</b> XWF <ul> <li>This mode is selected for Facebook Express Wi-Fi deployment.</li> </ul> </li> </ul> | _      | Standard                   |
| XWF Version                                  | <ol> <li>XWF-v1 is also called as XWF-Lite</li> <li>XWF-v2 is also called as XWF-Full</li> <li>XWF-v3</li> </ol>   | -      | 1                          |
| XWF Key                                      | This is applicable when XWF portal mode is selected irrespective of XWF version.   | -      | -                          |
| XWF Access<br>Token                          | XWF Access token in URL encoded format.  | -      | -                          |
| XWF SSE<br>Server Timeout                    | This is applicable when XWF portal mode is selected.<br>Provision to configure XWF SSE Server Timeout.   | 5-1800 | 60                         |
| Success Action                               | <ul> <li>Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL:</li> <li>1. Internal Logout Page After successful login, Wireless client is redirected to logout page hosted on AP. </li> </ul>  | _      | Internal<br>Logout<br>Page |

| Parameters                             | Description  | Range | Default |
|--|--|-------|---------|
|  | <ol> <li>Redirect user to External URL         Here users will be redirected to URL which is configured on device in Redirection URL configurable parameter.     </li> <li>Redirect user to Original URL</li> </ol>  |       |         |
|  | Here users will be redirected to URL that is accessed by user before successful captive portal authentication.   |       |         |
| Redirect user<br>to External<br>URL    | Provision to configure re-direction URL after successful login and an additional information of AP and wireless station information can be appended in the URL.  | _     | _       |
|  | <ul> <li>Prefix Query Strings in Redirect URL         This option is selected by default. Following             information is appended in the redirection URL:             <ul> <li>SSID</li> <li>AP MAC</li> <li>NAS ID</li> <li>AP IP</li> <li>Client MAC</li> </ul> </li> <li>Redirection URL         <ul> <li>User can provide either HTTP or HTTPS URL.</li> </ul> </li> </ul>   |       |         |
| Redirection<br>user to Original<br>URL | Users will be redirected to URL that is accessed by user<br>before successful captive portal authentication. There<br>is additional parameter Prefix Query Strings in<br>Redirection URL that is enabled by default and details<br>given below:<br>• Prefix Query Strings in Redirect URL<br>This option is selected by default. Following<br>information is appended in the redirection URL:<br>• SSID<br>• AP MAC<br>• NAS ID<br>• AP IP<br>• Client MAC |       |         |
| Success<br>message                     | Provision to configure text to display upon successful<br>Guest Access authentication. This is applicable only<br>when Success Action mode is Internal Logout Page.  | -     | _       |

| Parameters                         | Description  | Range           | Default  |
|------------------------------------|--|-----------------|----------|
| Redirection<br>URL Query<br>String | <ul> <li>Following information is appended in the redirection URL, if "Prefix Query Strings in Redirect URL" is enabled.</li> <li>Client IP</li> <li>RSSI</li> <li>AP Location</li> </ul>  | _               | Disabled |
| Redirect                           | <ul> <li>If enabled, only HTTP URLs will be redirected to<br/>Guest Access login page.</li> <li>If disabled, both HTTP and HTTPs URLs will be<br/>redirected to Guest Access login page.</li> </ul>                                  | _               | Enabled  |
| Redirect User<br>Page              | IP address configured in this field is used as<br>logout/disconnect/redirect to captive portal URL for<br>Guest Access sessions. IP address configured should<br>not be reachable to internet.                                       | _               | 1.1.1.1  |
| Proxy<br>Redirection<br>Port       | Proxy port can be configured with which proxy server is<br>enabled. This allows URL's accessed with proxy port to<br>be redirected to login page.  | 1 - 65535       | -        |
| Session<br>Timeout                 | This is the duration of time, client will be allowed to<br>access internet if quota persists, after which AP sends<br>de-authentication. Wireless station has to undergo<br>Guest Access authentication after session timeout.       | 60 -<br>2592000 | 28800    |
| Inactivity<br>Timeout              | Provision to configure timeout period to disconnect<br>wireless stations that are associated but no data traffic.<br>AP starts timer when there is no data received from a<br>wireless station and disconnects when timer reaches 0. | 60 -<br>2592000 | 1800     |
| MAC<br>Authentication<br>Fallback  | It's a mechanism in which wireless stations will be<br>redirected to Guest Access login page after any<br>supported type of MAC address authentication failures.   | _               | Disabled |
| Extend<br>Interface                | Provision to support Guest Access on Ethernet interface.   | -               | Disabled |
| Traffic Class 1                    | This is exclusively applicable for XWF portal type. This traffic class includes IP and URLs related to XWF for successful re-direction, login and payments.  | _               | -        |
| Traffic Class 2                    | This is exclusively applicable for XWF portal type. This traffic class includes whitelist IP/URLs that can be accessed without Guest Access authentication.  | -               | -        |
| Internet                           | This is exclusively applicable for XWF portal type. This traffic class includes whitelist IP/URLs that can be accessed after successful Guest Access authentication.   | -               | -        |

| Parameters                             | Description  | Range | Default |
|--|--|-------|---------|
| Whitelist                              | Provision to configure either IPs or URLs to bypass<br>traffic, such that user can access those IPs or URLs<br>without Guest Access authentication. This parameter is<br>valid for standard portal type. | _     | -       |
| Captive Portal<br>bypass User<br>Agent | Provision to limit the auto-popup to a certain browser<br>as configured based on User-agent of browsers. This is<br>valid for standard portal type.  | -     | _       |

To configure the above parameters, navigate to the **Configure > WLAN > Guest Access** tab and provide the details as given below:

- 1. Enable the required access types from the **Access Policy** checkbox.
- 2. Enable **HTTP** or **HTTPS** from the **Redirect Mode** checkbox.
- 3. Enter **Redirect Hostname** in the textbox.
- 4. Enable WISPr Clients External Server Login checkbox.
- 5. Enter External Page URL in the textbox.
- 6. Enable External Portal Post Through cnMaestro checkbox.
- 7. Select External Portal Type from the drop-down list.
- 8. Enable configured modes of redirection URL in **Success Action** checkbox.
- 9. Enter Success message to appear in the textbox.
- 10. Enable the required **Redirection URL Query String** checkbox.
- 11. Enable **Redirect** checkbox for HTTP packets.
- 12. Enter configuring IP address in the **Redirect User Page** textbox.
- 13. Enter Port number in the Proxy Redirection Port textbox.
- 14. Enter the session timeout in seconds in the **Session Timeout** textbox.
- 15. Enter the inactivity timeout in seconds in the Inactivity Timeout textbox.
- 16. Select the **MAC Authentication Fallback** checkbox if guest-access is used only as fallback for clients failing MAC-authentication.
- 17. Enter the name of the interface that is extended for guest access in the **Extend Interface** textbox.
- 18. Click Save.
- 19. Select Traffic Class 1 and Traffic Class 2 tabs and enter the following:
  - 1. Enter **Name** in the textbox.
  - 2. Enter **Policy** in the textbox.
  - 3. Click Save.
- 20. Select Internet tab and enter Name in the textbox.
  - 1. Click Save.

To configure Whitelist:

- 1. Enter the IP address or the domain name of the permitted domain in the **IP Address** or **Domain Name** textbox.
- 2. Click Save.

### To configure Captive Portal bypass User Agent:

- 1. Select **Index** parameter value from the drop-down list.
- 2. Enter **User Agent String** parameter in the textbox.
- 3. Select **Status Code** from the drop-down list.
- 4. Enter **HTML Response** in the textbox.
- 5. Click Save.
Figure 27 Configure: WLAN > Guest Access > External Hotspot (Standard) parameter

| Ended Important data   Fortal Matio Important data   Access Poirsi Important data   Calculation of the data data data data data data data dat  | Radius Server Guest Acces    | s Usage Limits           | Scheduled Access               | Access          | Passpoint             |                              |      |
|--|------------------------------|--------------------------|--------------------------------|-----------------|-----------------------|------------------------------|------|
| Portal Mode       Internal Access Point © External Hotspot © cnMaestro         Access Pointy       Clickthrough: Splash-page with usersame & password, authenticated with a FADUX Server         DADAP Redirect turne to a login page of authentication by Docal guest user account         Redirect Mode       # HTTP: Use HTTP USE for redirection         Redirect Hostman       Redirect Hostmane for the splash page (up to 255 churs)         Bits of the splash page (up to 255 churs)         Bits of the splash page (up to 255 churs)         Bits of the splash page         External Post         External Post         Bits of the splash page         External Post         Bits of the splash page         External Post         Dyst of the splash page         External Post         Dyst of the splash page         External Post         Dyst of the splash page         External Post In Type         XWF         Success Token         Eg: XWF Key in hexadocimal format Let 1122BBFF         XWF Set Server Timeout         Success Token         Eg: XWF Access Token in URL encoded format         XWF Set Server Timeout         Success Action         Redirection URL Query String         Redirect User Page <t< td=""><td>For the second</td><td></td><td></td><td></td><td></td><td></td><td></td></t<>  | For the second               |                          |                                |                 |                       |                              |      |
| Access Policy <ul> <li>Clickthrough</li> <li>Splash-page with usemane &amp; password authenticated with a PADUX server</li> <li>LOAP</li> <li>Redire to a skyrn page to authenticated by a LAP server</li> <li>LOAP</li> <li>Redirect wathen to a skyrn page to authentication by Load guest user account</li> <li>Redirect Hostmane</li> <li>Redirect Hostmane</li> <li>Redirect Hostmane</li> <li>Redirect Hostmane</li> <li>Redirect Hostmane</li> <li>Redirect Hostmane</li> <li>External Server</li> <li>Logi</li> <li>External Server</li> <li>Logi</li> <li>External Postal Type</li> <li>Success Token</li> <li>Ep: http://external.com/login.html</li> <li>URL</li> <li>URL</li> <li>URL</li> <li>Context and application ap</li></ul>  |                              |                          |                                | 1111            |                       |                              |      |
| Radius Signat-page with username & password, authenticated with a RADUS Server     E. Local Guest Account . Redirect auter to a login page for authentication by local guest user account.     Redirect Motion     HTTPS Use HTTPS URLs for redirection     Redirect Hostname     Redirect Hostname     Redirect Hostname for the splash page (up to 255 chars)      WISPr Clients External Page     Local     Local     Redirect Hostname for the splash page (up to 255 chars)      External Page     Local     Local     Redirect Hostname for the splash page (up to 255 chars)      External Page     Local     Local     Redirect Hostname for the splash page (up to 255 chars)      External Page     Local     Local     Redirect Hostname for the splash page     External Portal Type     Swr     Local     Local     Redirect Hostname for the splash page     External Portal Type     XWF     WF     Swr     External Portal Type     XWF     Swr     External Portal Type     XWF Key     Eg XWF key in hexadocimal format i.e. 1122BBFF     XWF Access Token     Eg XWF key in hexadocimal format i.e. 1122BBFF     XWF Access Token     Eg XWF key in hexadocimal format i.e. 1122BBFF     XWF SSE Server Timeout     60     XWF SSE Server Timeout     60     XWF SSE Server timeout in seconds (5 to 1000)     Success Action     # Internal Looput Page     Redirect in the redirection urd query stings     Redirect Minit Provide Pad charts for the redirection urd query stings     Redirect Minit Provide Pad charts for the charts and the page     Proxy Redirection Port     Pad dress for redirecting user to guest potal a plash page     Proxy Redirection Port     Pad dress for redirecting user to guest potal a plash page     Proxy Redirection Port     Pad dress for redirecting user to guest potal a plash page     Proxy Redirection Port     Pad dress for redirecting user to guest potal a plash page     Proxy Redirection Port     Pad dress for redirecting user to guest potal a plash page     Proxy Redirection Page     Cancel     Prot number(1 to 6535)     Session       |                              |                          |                                |                 |                       |                              |      |
| UDAP       Redirect users to a kgin page for authentication by a LDAP server             UDAP       Redirect Mode             WISPr Clients External Server         Login           WISPr Clients External Server         Login             WISPr Clients External Server         Login               WISPr Clients External Server         Login               WISPr Clients External Server         Login               WISPr Clients External Server         Login               WISPr Clients External Server         Login               WISPr Clients External Server         Login               WISPr Clients External Portal Type           External Portal Type             WIF Version         30           WIF Version           Success Token             External Portal Type           ZVWF key in hexadocimal format Lie           Success Token             Success Token           Egi XWF Access Token           Egi XWF Access Token             Success Action             Egi XWF Access Token             Redirect Versiting           Client IIP - Include IP of cleent in the redirection unt query strings   |                              | -                        |                                |                 | -                     |                              |      |
| Redirect Mode <ul> <li>HTTP: Use HTTPS URL for redirection</li> <li>HTTPS: Use HTTPS URL for redirection</li> <li>Redirect Hostname</li> <li>Redirect Hostname</li> <li>Redirect Hostname</li> <li>Redirect Hostname for the splash page (up to 255 chars)</li> <li>WISPT Clients External Savorr<br/>Login</li> <li>External Post</li> <li>External Post Through</li> <li>External Post Through</li> <li>External Post Through</li> <li>External Post Type</li> <li>XWF Key</li> <li>External Post Through</li> <li>XWF Key</li> <li>External Post Type</li> <li>XWF Key</li> <li>External Post Type StandardXWF</li> <li>XWF Key</li> <li>External Post Type StandardXWF</li> <li>XWF Key</li> <li>External Post Type StandardXWF</li> <li>XWF SSE Server timeouth</li> <li>80</li> <li>XWF SSE Server timeout is accords (5 to 1800)</li> <li>Success Action</li> <li>Internal Extend Lagout Page Redirect user to External RL Redirect user to Original URL</li> <li>Success Action</li> <li>Internal Extend Post Through</li> <li>Redirect I Cleart IP Include IP of client in the redirection uf query strings</li> <li>RSI Include rsi value of client in the redirection uf query strings</li> <li>RSI Include RSI for redirection for HTTP packets only</li> <li>Redirect I Traffic Class 1 Internet</li> <li>De guest-access only as follback for clients failing MAC-authentication</li> <li>External Parkets only as follback for clients failing MAC-authentication</li> <li>External Post 2 Internet</li> <li>Redirect I Traffic Class 2 Internet</li> <li>Proof gues ID onain Name</li> <li>Action</li> <li>PA ddress I Domain Name</li> <li>Action</li> <li>PA ddress I Domain Name</li> <li></li></ul>  | (                            | LDAP Redirect user       | rs to a login page for authe   | entication by a | LDAP server           |                              |      |
| Image: Control of the second secon                                |                              |                          |                                | n page for au   | thentication by local | guest user account           |      |
| Redirect Hosthume for the splash page (up to 255 chars)         WISPT Clients External Page         External Portal Post Through<br>URL         External Portal Type         XWF Version         30         XWF Key         Eg: XWF Access Token         Success Action         Internal Pode is a variable of diert in the redirection and query strings         Redirect User Page         Redirect Werthig         Redirect Werthig         Redirect User Page         Redirect Werthig         Redirec   |                              |                          |                                |                 |                       |                              |      |
| WISPr Clients External Server<br>Login       Eg: http://external.com/login.html         External Portal Pose<br>URL       Eg: http://external.com/login.html         URL of external splash page         External Portal Type         XWF         XWF Version         3.0         XWF Key         Eg: XWF Access Token         Eg: XWF Access Token         Eg: XWF Access Token in URL encoded format         XWF SSE Server Timeout         60       XWF SSE Server timeout in seconds (5 to 1900)         Success Action       Internal Logout Page         Redirection URL Query String       Client IP         Success Token       Eg: XWF Access Token in URL encoded format         Success Action       Internal Logout Page         Redirection URL Query String       Client IP         Redirect WHTP-only       Enable redirection urd query strings         Redirect User Page       1.1.1         Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 6535)         Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       inactivity time in seconds (60 to 2592000)         Inactivity Timeout       Use guest-access only as falback for clien  |                              |                          |                                |                 |                       |                              |      |
| Login         External Portal Post         Eg: http://external.com/login.html         URL       URL         URL       orderad splash page         External Portal Type       XWF         External Portal Type       XWF         SWF Version       3.0         3.0       XWF Version         3.0       XWF Version         XWF Access Token       Eg: XWF Access Token in URL encoded format         Eg: XWF Access Token       Eg: XWF Access Token in URL encoded format         Success Action       Internal Logout Page         Redirection URL Query String       Client IP         Client IP       Include IP of client in the redirection uf query strings         B       Resist         Include IP of client in the redirection uf query strings       B         B       PLOsation       Include AP Location in the redirection uf query strings         B       Configure IP address for redirecting user to guest poral splash page         Proxy Redirection Port       Port number(1 to 65535)         Session Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication       Fatternet       Configure the interface which is artended for guest access:         Suve       Cancel       Imateriol (Cloope 1 porel avol  |                              |                          | ne splash page (up to 255      | chars)          |                       |                              |      |
| URL       URL of external splash page         External Portal Post Inrough<br>cnMaestro <ul> <li>Sternal Portal Type</li> <li>XWF</li> <li>Sternal Portal Type</li> <li>XWF Version</li> <li>XWF Key</li> <li>Eg: XWF Access Token</li> <li>Eg: XWF Access Token in URL encoded format</li> <li>XWF SSE Server Timeout</li> <li>XWF SSE Server timeout in accords (5 to 1600)</li> <li>Success Action</li> <li>Internal Logout Page</li> <li>Redirect user to External URL</li> <li>Redirection URL Query String</li> <li>Cleint IP: Include IP of cleint in the redirection uf query strings</li> <li>Redirect With the redirection for HTTP packets only</li> <li>Redirect With Theout</li> <li>Port number(1 to 65535)</li> <li>Session Timeout</li> <li>Session Time in seconds (60 to 2592000)</li> <li>Inactivity Timeout</li> <li>B00</li> <li>Inactivity Time ont</li> <li>B00</li> <li>Inactivity Time ont</li> <li>B00</li> <li>Inactivity time in seconds (60 to 2592000)</li> </ul> <li>MAC Authentication Fallback</li> <li>Use guest-access only as fallback for clients failing MAC-authentication</li> <li>Extend Interface</li> <li>Configure the interface which is extended for guest access</li> <li>Sovo Cancel</li>  |                              |                          |                                |                 |                       |                              |      |
| External Portal Post Through       Image: Children Stream Portal Type Standard/XWF         External Portal Type       XWF       F         XWF Version       3.0       •       XWF Version 1.02.03.0         XWF Key       Eg: XWF key in hexadecimal formatile. 1122BBFF       XWF Version 1.02.03.0         XWF Key       Eg: XWF Access Token in URL encoded format       60       xWF SSE Server timeout in seconds (5 to 1600)         Success Action       Internal Logout Page Redirect user to External URL ® Redirect user to Original URL       Success message         Redirection URL Query String       Chent IP include IP of clent in the redirection ut query strings       RSSI: include rssi value of client in the redirection ut query strings         Redirect       HTTP-only       Enable redirection for HTTP packets only       Redirect         Redirect       Int.1.1       Configure IP address for redirection for HTTP packets only       Redirect User Page         Proxy Redirection Port       Pot number(1 to 6535)       Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)       Inactivity Timeout       Sore         Store       Onfigure the interface which is extended for guest access       Sore       Sore       Sore         Fradicess 1       Trefic Class 2       Internet   | External Page                | Eg: http://external.c    | com/login.html                 |                 |                       |                              |      |
| cnMaestro         External Portal Type         XWF         XWF Version         3.0         XWF Key         Eg: XWF Key in hexadecimal format i.e. 1122BBFF         XWF Access Token         Eg: XWF Access Token in URL encoded format         60       XWF SSE Server timeout in seconds (5 to 1800)         Success Action       Internal Logout Page Redirect user to External URL® Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL® Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL® Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL® Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL® Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL® Redirect user to Original URL         Redirection URL Query String       Cleant IP Indudes Poteler in the redirection urd query strings         Redirect User Page       11.1.1         Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Pot number(1 to 65535)         Session Timeout       28800       session time in seconds (60 to 2592000)         Inactivity Timeout <td>URL</td> <td>IRL of external splash p</td> <td>age</td> <td></td> <td></td> <td></td> <td></td>  | URL                          | IRL of external splash p | age                            |                 |                       |                              |      |
| External Portal Type       XWF       External Portal Type Standard/XWF         XWF Version       3.0       •       XWF Version 1.02.0.0         XWF Key       Eg: XWF Access Token       Eg: XWF Access Token       I122.081F         XWF SSE Server Timeout       60       XWF SSE Server timeout in seconds (5 to 1000)         Success Action       Internal Logout Page Redirect user to External URL © Redirect user to Original URL         Success message       Internal Logout Page © Redirect ouer to External URL © Redirect user to Original URL         Success message       Internal Logout Page © Redirect ouer our query strings         Redirection URL Query String       Client IP       Include RP location in the redirection uf query strings         Redirect       HTTP-only       Enable redirection for HITP packets only         Redirect User Page       11.1.1       Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 65535)       Session Timeout         Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication Fallback       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       O onfigure the interface which is extended for guest access <td></td> <td>1</td> <td></td> <td></td> <td></td> <td></td> <td></td>  |                              | 1                        |                                |                 |                       |                              |      |
| XWF Version       3.0       XWF Version 1.02.03.0         XWF Key       Eg: XWF Key in hexadecimal format i.e. 1122BBFF         XWF Access Token       Eg: XWF Access Token in URL encoded format         XWF SSE Server Timeout       6.0       XWF SSE Server timeout in seconds (5 to 1800)         Success Action       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success Action       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Redirect USE Page       Interview String         Redirect User Page       11.1.1         Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 65535)         Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication Fallback       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Save       Cancle         Yeadress   Subnet   Domain N  |                              | XWE                      | Ŷ                              | External P      | Portal Type Standard  | VXWF                         |      |
| XWF Key       Eg: XWF key in hexadecimal format i.e. 1122BBFF         XWF Access Token       Eg: XWF Access Token in URL encoded format         XWF SSE Server Timeout       60       xWF SSE Server timeout in seconds (5 to 1800)         Success Action       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success message       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Redirection URL Query String       Client IP Include IP of client in the redirection url query strings         Redirect User Page       1.1.1         Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 65535)         Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication Fallback       Use guest-access only as faltback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Savo       Cancel         Traffic Class 1       Internot   |                              |                          |                                |                 |                       |                              |      |
| XWF Access Token       Eg: XWF Access Token in URL encoded format         XWF SSE Server Timeout       60       XWF SSE Server timeout in seconds (5 to 1800)         Success Action       Internal Logout Page       Redirect user to External URL       Redirect user to Original URL         Success message  |                              |                          | <b>*</b>                       |                 |                       |                              |      |
| XWF SSE Server Timeout       60       XWF-SSE Server timeout in seconds (6 to 1800)         Success Action       Internal Logout Page © Redirect user to External URL © Redirect user to Original URL         Success message  |                              |                          |                                |                 |                       |                              |      |
| Success Action       Internal Logout Page Redirect user to External URL Redirect user to Original URL         Success message  |                              |                          |                                |                 |                       |                              |      |
| Success message         Redirection URL Query String         Client IP         Include PS of client in the redirection und query strings         AP Location         Include AP Location in the redirection und query strings         AP Location         Include PS of client in the redirection und query strings         Redirect         HTTP-only         Enable redirection for HTTP packets only         Redirect User Page         1.1.1         Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port         Port number(1 to 65535)         Session Timeout         28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800         Inactivity Timeout       1800         Inactivity Timeout       1800         Inactivity Timeout       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Save       Cancel             Interfic Class 1       Traffic Class 2         Internet       Internet         Policy       Save         Profile       Close         IP Address   Domain N   | KWF SSE Server Timeout       | 60 XWF SS                | SE Server timeout in secor     | nds (5 to 1800  | )                     |                              |      |
| Redirection URL Query String       Client IP       Include IP of client in the redirection und query strings         Redirect       RSSI       Include AP Location in the redirection und query strings         Redirect       HTTP-only       Enable redirection for HTTP packets only         Redirect User Page       1.1.1       Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 65535)       Session Timeout         Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication Fallback       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Save       Cancel         Traffic Class 1       Traffic Class 2         Internet       Internet         Name       IP Address   Subnet   Domain Name         Policy       Save         IP Address   Domain Name       Action   | Success Action               | Internal Logout Page     | e CREDIRECT USER TO EXT        | ernal URL 🔍     | Redirect user to C    | riginal URL                  |      |
| Restinct User Page     AP Location Include AP Location in the redirection url query strings     AP Location Include AP Location in the redirection url query strings     Redirect User Page     I.1.1     Configure IP address for redirecting user to guest portal splash page Proxy Redirection Port     Part number(1 to 65535)     Session Timeout     28800 Session time in seconds (60 to 2592000)     Inactivity Timeout     1800 Inactivity time in seconds (60 to 2592000)     Inactivity Timeout     1800 Inactivity time in seconds (60 to 2592000)     Inactivity Timeout     1800 Inactivity time in seconds (60 to 2592000)     Inactivity Timeout     Extend Interface     Configure the interface which is extended for guest access     Save     Cancel      Traffic Class 1 Traffic Class 2 Internet     O     Policy     O Save     IP Address   Subnet   Domain Name     Action     Traffic Class 1 the pot portal bypase     IP Address   Domain Name   | Success message              |                          |                                |                 |                       |                              |      |
| AP Location Include AP Location in the redirection url query strings     Redirect     Proxy Redirect User Page     1.1.1     Configure IP address for redirecting user to guest portal splash page     Proxy Redirection Port     Port number(1 to 65535)     Session Timeout     28800 Session time in seconds (60 to 2592000)     Inactivity Timeout     1800 Inactivity time in seconds (60 to 2592000)     Inactivity Timeout     1800 Inactivity time in seconds (60 to 2592000)     MAC Authentication Fallback     Use guest-access only as fallback for clients failing MAC-authentication     Extend Interface     Configure the interface which is extended for guest access     Save     Cancel      Traffic Class 1 Traffic Class 2 Internet     O     Policy     O Save     PAddress   Subnet   Domain Name   |                              |                          |                                |                 |                       |                              |      |
| Redirect User Page       1.1.1.1         Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 65535)         Session Timeout       28800         Session Timeout       28800         Inactivity Timeout       1800         Inactivity Timeout       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Save       Cancel         Traffic Class 1       Traffic Class 2         Internet       Internet         Policy       Save         IP Address 1       Domain Name   |                              |                          |                                |                 |                       |                              |      |
| Configure IP address for redirecting user to guest portal splash page         Proxy Redirection Port       Port number(1 to 65535)         Session Timeout       28800         Session Timeout       28800         Inactivity Timeout       1800   | Redirect                     | HTTP-only Enable         | redirection for HTTP pack      | ets only        |                       |                              |      |
| Proxy Redirection Port       Port number(1 to 65535)         Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication Fallback       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Save       Cancel         Traffic Class 1       Traffic Class 2         Internet       Ø         Policy       Ø         Save       Save         IP Address I Subnet   Domain Name       Action         Traffic Class 1       Traffic Class 2  | Redirect User Page           | 1.1.1.1                  |                                |                 |                       |                              |      |
| Session Timeout       28800       Session time in seconds (60 to 2592000)         Inactivity Timeout       1800       Inactivity time in seconds (60 to 2592000)         MAC Authentication Fallback       Use guest-access only as fallback for clients failing MAC-authentication         Extend Interface       Configure the interface which is extended for guest access         Save       Cancel         Traffic Class 1       Traffic Class 2         Internet       0         Policy       0         Save       Save         IP Address   Subnet   Domain Name       Action         Traffic Class 1       Top t over ide bio  |                              |                          |                                | t portal splash | n page                |                              |      |
| Inactivity Timeout IB00 Inactivity time in seconds (60 to 2592000) MAC Authentication Fallback Use guest-access only as fallback for clients failing MAC-authentication Extend Interface Configure the interface which is extended for guest access Save Cancel  Traffic Class 1 Traffic Class 2 Internet  Mame  IP Address   Subnet   Domain Name  IP Address   Subnet   Domain Name  IP Address   Domain Name  Action  IP Address   Domain Name  Action  IP Address   Domain Name  Action  Action  IP Address   Domain Name  IP Address   Domain Name  Action  IP Address   Domain Name  IP Address   Domain Name  Action  IP Address   Domain Name  IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domain Name IP Address   Domai |                              | Port nun                 | nber(1 to 65535)               |                 |                       |                              |      |
| MAC Authentication Fallback Use guest-access only as fallback for clients failing MAC-authentication Extend Interface Configure the interface which is extended for guest access Save Cancel Traffic Class 1 Traffic Class 2 Internet Name  Policy  P Address 1 Subnet   Domain Name Action  P Address 1 Subnet   Domain Name Action  Traffic Class 1 pot a variable a   | Session Timeout              | 28800 Session            | time in seconds (60 to 25      | 92000)          |                       |                              |      |
| Extend Interface       Configure the interface which is extended for guest access.         Save       Cancel         Traffic Class 1       Traffic Class 2         Internet       Internet         Policy       Image: Save         IP Address   Subnet   Domain Name       Action         Traffic Class 1       Traffic Class 2         IP Address   Subnet   Domain Name       Action  | Inactivity Timeout           | 1800 Inactivity          | y time in seconds (60 to 2     | 592000)         |                       |                              |      |
| Save       Cancel         Traffic Class 1       Traffic Class 2         Name       Ø         Policy       Ø         IP Address   Subnet   Domain Name       Action         Traffic Class 1       Traffic Class 2         IP Address   Subnet   Domain Name       Action         Traffic Class 1       Domain Name         Policy       Ø         Save       IP Address   Domain Name         Traffic Class 1       Domain Name         Action       IP Address   Domain Name   | Authentication Fallback      | Use guest-access on      | nly as fallback for clients fa | iling MAC-aut   | thentication          |                              |      |
| Traffic Class 1       Traffic Class 2       Internet       Add Whitelist       Captive Portal bypass User Agent         Name          •         •         •  | Extend Interface             | Configur                 | re the interface which is ea   | tended for gu   | lest access           |                              |      |
| Name       Ø         Policy       Ø         IP Address   Subnet   Domain Name       × Action         IP Address   Subnet   Domain Name       × Action  |                              | Save Cancel              |                                |                 |                       |                              |      |
| Name       Ø         Policy       Ø         IP Address   Subnet   Domain Name       × Action         IP Address   Subnet   Domain Name       × Action  |                              |                          |                                |                 |                       |                              |      |
| Name       Ø         Policy       Ø         IP Address   Subnet   Domain Name       × Action         IP Address   Subnet   Domain Name       × Action  | ffic Class 1 Traffic Class 3 | Internet                 | Addata                         | hitolist        | Cantivo Portal hum    | ass Liser Agent              |      |
| Policy Ø Savo IP Address   Subnet   Domain Name × Action IP Address   Domain Name × Action   | ITE GIASS T THAIIIC GIASS 2  | Internet                 | Add W                          | micenst (       | зариче Ропагрура      | 255 USEI AGENI               |      |
| Policy   | lame                         | 0                        |                                |                 |                       |                              | Save |
| IP Address   Subnet   Domain Name V Action   | Policy                       | 0                        |                                | nain Name       |                       |                              |      |
| Troffie Close 1 pot evoileble  | Address   Subnet   Domain Ma | me <u>×</u> Action       |                                |                 |                       |                              |      |
| Traffic Class 1 not available No white list available  |                              | A0001                    | IP Ad                          | dress   Dom     | ain Name              | <ul> <li>Action .</li> </ul> |      |
| Traffic Class 1 not available No white list available  |                              | 201 - 2021 - 4- 4- 4-    |                                |                 |                       |                              | *    |
|  | Traffic Class 1              | not availabl             | е                              | Νo              | white list a          | available                    |      |
|  |                              |                          |                                |                 |                       |                              |      |
|  |                              |                          |                                |                 |                       |                              |      |
|  |                              |                          |                                |                 |                       |                              |      |
|  |                              |                          |                                |                 |                       |                              |      |
|  |                              |                          | *                              |                 |                       |                              | *    |
|  |                              |                          |                                |                 |                       |                              |      |

Figure 28 Configure: WLAN > Guest Access > External Hotspot (XWF) parameter

| Parameters                             | Description  | Range           | Default  |  |  |  |  |  |  |
|--|--|-----------------|----------|--|--|--|--|--|--|
| WLAN > Guest                           | WLAN > Guest Access > cnMaestro  |                 |          |  |  |  |  |  |  |
| Guest Portal<br>Name                   | Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.  | -               | -        |  |  |  |  |  |  |
| Redirect                               | <ul> <li>If enabled, only HTTP URLs will be redirected to<br/>Guest Access login page.</li> <li>If disabled, both HTTP and HTTPs URLs will be<br/>redirected to Guest Access login page.</li> </ul>                                  | _               | Enabled  |  |  |  |  |  |  |
| Redirect User<br>Page                  | IP address configured in this field is used as logout URL<br>for Guest Access sessions. IP address configured should<br>be not reachable to internet.  | _               | 1.1.1.1  |  |  |  |  |  |  |
| Proxy<br>Redirection<br>Port           | Proxy port can be configured with which proxy server is<br>enabled. This allows URL's accessed with proxy port to<br>be redirected to login page.  | 1 - 65535       | -        |  |  |  |  |  |  |
| Inactivity<br>Timeout                  | Provision to configure timeout period to disconnect<br>wireless stations that are associated but no data traffic.<br>AP starts timer when there is no data received from a<br>wireless station and disconnects when timer reaches 0. | 60 -<br>2592000 | 1800     |  |  |  |  |  |  |
| MAC<br>Authentication<br>Fallback      | It's a mechanism in which wireless stations will be<br>redirected to Guest Access login page after any<br>supported type of MAC address authentication fails.  | _               | Disabled |  |  |  |  |  |  |
| Extend<br>Interface                    | Provision to support Guest Access on Ethernet interface.   | _               | Disabled |  |  |  |  |  |  |
| Whitelist                              | Provision to configure either IPs or URLs to bypass<br>traffic, such that user can access those IPs or URLs<br>without Guest Access authentication.  | -               | -        |  |  |  |  |  |  |
| Captive Portal<br>bypass User<br>Agent | Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.  | -               | -        |  |  |  |  |  |  |

| Table 25 Configure: WLAN > 0 | Guest Access > cnMaestro parameters |
|------------------------------|-------------------------------------|
|------------------------------|-------------------------------------|

To configure the above parameters, navigate to the **Configure > WLAN > cnMaestro** tab and provide the details as given below:

- 1. Enter Guest Portal Name which is hosted on cnMaestro in the textbox.
- 2. Enable **Redirect** checkbox for HTTP packets.
- 3. Enter configuring IP address in the **Redirect User Page** textbox.
- 4. Enter Port number in the **Proxy Redirection Port** textbox.
- 5. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.
- 6. Select the **MAC Authentication Fallback** checkbox if guest-access is used only as fallback for clients failing MAC-authentication.

- 7. Enter the name of the interface that is extended for guest access in the **Extend Interface** textbox.
- 8. Click Save.

To configure the Whitelist parameter:

- 1. Enter the IP address or the domain name of the permitted domain in the **IP Address** or **Domain Name** textbox.
- 2. Click Save.

To configure the Captive Portal bypass User Agent parameter:

- 1. Select **Index** parameter value from the drop-down list.
- 2. Enter **User Agent String** parameter in the textbox.
- 3. Select Status Code from the drop-down list.
- 4. Enter HTML Response in the textbox.
- 5. Click Save.

#### Figure 29 Configure: WLAN > Guest Access > cnMaestro parameter

| Basic Radius Server Guest Access Usage Limits Scheduled | Access Access Passpoint   |  |
|---|---|--|
| Enable  | 8   |  |
| Portal Mode   | <ul> <li>Internal Access Point</li></ul>                            |  |
| Guest Portal  |   |  |
| Name  | SIT_GuestAccess Guest Portal Name which is hosted on cnMaestro      |  |
| Redirect  | HTTP-only Enable redirection for HTTP packets only                  |  |
| Redirect User Page                                      | 1.1.1.1   |  |
|   | Configure IP address for redirecting user to guest portal splash pa | ige                                      |
| Proxy Redirection Port                                  | Port number(1 to 65535)   |  |
| Inactivity Timeout                                      | 1800 Inactivity time in seconds (60 to 2592000)                     |  |
| MAC Authentication Fallback                             | Use guest-access only as fallback for clients failing MAC-auther    | ntication                                |
| Extend Interface  | Configure the interface which is extended for guest                 | access                                   |
|   | Save Cancel   |  |
|   |   |  |
|   | Add Whitelist Captive Portal bypass User Agent                      |  |
|   | IP Address or Domain Name   | Save                                     |
|   |   |  |
|   | IP Address   Domain Name  | ~ Action                                 |
|   |   | *  |
|   | No wi   | nite list available                      |
|   |   |  |
|   |   |  |
|   |   |  |
|   |   |  |
|   |   | ▼<br>I ↓ 1 ↓ 1 ► ► 1 10 ▼ items per page |
|   |   |  |

| Parameters               | Description   | Range | Default          |
|--------------------------|---|-------|------------------|
| Rate Limit per<br>Client | Provision to limit throughput per client. Default allowed<br>throughput per client is unlimited. i.e., maximum allowed<br>by 802.11 protocols. The traffic from/to each client on a<br>SSID can be rate-limited in either direction by<br>configuring Client rate limit available in usage-limits<br>inside the WLAN Configuration. This is useful in<br>deployments like public hotspots where the backhaul is<br>limited and the network administrator would like to<br>ensure that one client does not monopolize all available<br>bandwidth.  | _     | 0<br>[Unlimited] |
| Rate Limit per<br>WLAN   | Provision to limit throughout across WLAN irrespective<br>of number of associated wireless stations to WLAN. All<br>upstream/downstream traffic on an SSID (aggregated<br>across all wireless clients) can be rate-limited in either<br>direction by configuring usage-limits inside the WLAN<br>Configuration section of the GUI. This is useful in cases<br>where multiple SSIDs are being used and say one is for<br>corporate use, and another for guests. The network<br>administrator can ensure that the guest VLAN traffic is<br>always throttled, so it will not affect the corporate<br>WLAN. | _     | O<br>[Unlimited] |

# Table 26 Configure: WLAN > Usage Limits parameters

To configure the above parameters, navigate to the **Configure > WLAN > Usage Limits** tab and provide the details as given below:

- 1. Enter **Upstream** and **Downstream** parameters in the **Rate Limit per Client** textbox.
- 2. Enter Upstream and Downstream parameters in the Rate Limit per WLAN textbox.
- 3. Click Save.

| Basic | Radius Server | Guest Access | Usage Limits        | Scheduled Access | Access | Passpoint |      |                         |
|-------|---------------|--------------|---------------------|------------------|--------|-----------|------|-------------------------|
|       |               | R            | ate Limit per Clien | t Upstream:      |        |           |      | Downstream:             |
|       |               | Ra           | te Limit per WLAI   |                  |        |           |      | Kbps Downstream: 0 Ktac |
|       |               |              |                     | Tupo<br>Tupo     |        |           | Save | Kbps<br>Cancel          |

## Figure 30 Configure: WLAN > Usage Limits parameters

| Parameters          | Description  | Range                   | Default  |
|---------------------|--|-------------------------|----------|
| Scheduled<br>Access | Provision to configure the availability of Wi-Fi services<br>for a selected time duration. cnPilot has capability of<br>configuring the availability of Wi-Fi services on all days<br>or on specific day (s) of a week. Time format is in Hours. | 00:00 Hrs<br>23:59 Hrs. | Disabled |

To configure the above parameter, navigate to the **Configure > WLAN > Scheduled Access** tab and provide the details as given below:

- 1. Enter the start and end time to enable the Wi-Fi access in the respective textboxes.
- 2. Click Save.

| Basic | Radius Server | Guest Access | Usage Limits | Scheduled Access | Access | Passpoint |          |              |
|-------|---------------|--------------|--------------|------------------|--------|-----------|----------|--------------|
|       |               |              | Sunda        | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              | Monda        | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              | Tuesda       | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              | Wednesda     | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              | Thursda      | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              | Frida        | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              | Saturda      | y Start Time     |        |           | End Time | HH:MM format |
|       |               |              |              |                  |        |           | Save     |              |

## Table 28 Configure: WLAN > Access parameters

| Parameters | Description   | Range            | Default |
|------------|---|------------------|---------|
| ACL        |   |                  |         |
| Precedence | Provision to configure index of ACL rule. Packets are validated and processed based on precedence value configured. | 1-256            | 1       |
| Policy     | Provision to configure whether to allow, deny or route traffic.   | Allow/deny/Route | Deny    |
| Direction  | Provision to apply the ACLs rules configured either in any direction or specific direction.                         | _                | -       |
| Туре       | cnPilot devices support three layers of ACLs. A rule can be configured as below:                                    | -                | IP      |

| Parameters              | Description   | Range | Default |
|-------------------------|---|-------|---------|
|                         | <ul> <li>MAC</li> <li>IP<br/>This type is for IPv4 based IP ACL.</li> <li>IP6<br/>This type is for IPv6 based IP ACL.</li> <li>Proto<br/>This type is for protocol supported in IPv4.</li> <li>Proto6<br/>This type is for protocol supported in IPv6.</li> </ul> |       |         |
| Source<br>IP/Mask       | This option is available when ACL type is<br>configured to an IPv4/IPv6 address. This field helps<br>user to configure if rule needs to be applied for a<br>single IPv4/IPv6 address or range of IPv4/IPv6<br>addresses.  | _     | _       |
| Destination<br>IP/Mask  | This option is available when ACL type is<br>configured to an IPv4/IPv6 address. This field helps<br>user to configure if rule needs to be applied for a<br>single IPv4/IPv6 address or range of IPv4/IPv6<br>addresses.  | _     | _       |
| Source<br>MAC/Mask      | This option is available when ACL type is<br>configured to a MAC address. This field helps user<br>to configure if rule needs to be applied for a single<br>device MAC address or range of MAC addresses.   | _     | -       |
| Destination<br>MAC/Mask | This option is available when ACL type is<br>configured to MAC address. This field helps user to<br>configure if rule needs to be applied for a single<br>device MAC address or range of MAC addresses.   | _     | -       |
| Protocol                | <ul> <li>This option is available when user selects ACL type as proto/proto6. User can select following protocols:</li> <li>TCP</li> <li>UDP</li> <li>ICMP</li> <li>Any</li> </ul>  | _     | ТСР     |
| Source Port             | Provision to apply ACL with combination of protocol and port.   | -     | -       |
| Destination<br>Port     | Provision to apply ACL with combination of protocol and port.   | -     | _       |

| Parameters                      | Description   | Range | Default |
|---------------------------------|---|-------|---------|
| Description                     | To make administrator easy to understand, a text string can be added for each ACL rule.   | _     | -       |
| DNS-ACL                         |   |       |         |
| Precedence                      | Provision to configure index of ACL rule. Packets<br>are validated and processed based on Precedence<br>value configured.   | _     | 1       |
| Action                          | Provision to configure whether to allow or deny traffic.  | -     | Deny    |
| Domain                          | Provision to configure domain names and rules are applied based on Action configured.   | _     | -       |
| MAC Authentica                  | tion  |       |         |
| MAC<br>Authentication<br>Policy | <ul> <li>cnPilot supports multiple methods of MAC authentication. Following are details of each mode:</li> <li><b>Permit</b> <ul> <li>Wireless station MAC addresses listed will be allowed to associate to AP.</li> </ul> </li> <li><b>Deny</b> <ul> <li>When user configures a MAC address, those wireless station shall be denied to associate and the non-listed MAC address will be allowed.</li> </ul> </li> <li><b>Radius</b> <ul> <li>For every wireless authentication, cnPilot sends a radius request and if radius accept is received, then wireless station is allowed to associate.</li> </ul> </li> <li><b>cnMaestro</b> <ul> <li>This option is preferable when administrator prefers centralized MAC authentication, AP sends query to cnMaestro if it allowed or disallowed to connect. Based on the configuration, wireless stations are either allowed or denied.</li> </ul></li></ul> |       | Deny    |

To configure the above parameter, navigate to the **Configure > WLAN > Access** tab and provide the details as given below:

To configure **ACL**:

- 1. Select **Precedence** from the drop-down list.
- 2. Select type of **Policy** from drop-down list.
- 3. Select **Direction** from the drop-down list.
- 4. Select **Type** from the drop-down list.

- 5. Enter IP address of source in the **Source IP/Mask** textbox.
- 6. Enter IP address of destination in the **Destination IP/Mask** textbox.
- 7. Enter **Description** in the textbox.
- 8. Click Save.

To configure **DNS ACL**:

- 1. Select **Precedence** from the drop-down list.
- 2. Select type of action from Action drop-down list.
- 3. Enter domain name in the **Domain** textbox.
- 4. Click Save.

#### To configure MAC Authentication:

- 1. Select MAC Authentication Policy from the drop-down list.
- 2. Enter **MAC** in the textbox.
- 3. Enter **Description** in the textbox.
- 4. Click Save.

#### Table 29 Behavior of IP ACL when dual stack is enabled

| IPv4 ACL Rule    | IPv6 ACL Rule    | Remark                    |  |  |
|------------------|------------------|---------------------------|--|--|
| No rule          | No rule          | All IPv4 and IPv6 allowed |  |  |
| IPv4 permit rule | No rule          | All IPv6 packets dropped  |  |  |
| No rule          | IPv6 rule        | All IPv4 packets dropped  |  |  |
| IPv4 permit rule | IPv6 permit rule | All IPv4 and IPv6 allowed |  |  |

| Radius Server Guest Access ACL Precedence 1 Type iP Description Precedence  Precedence  Precedence  Policy | Vage Limits Scheduled Access                                     | Access Passpoint Policy Deny Source IP/Mask V Rule | ▼ Directio   | n<br>tion IP/Mask | •<br>Sare                             |
|--|--|--|--------------|-------------------|---------------------------------------|
| Precedence 1 Type IP Description   | Y  | Deny<br>Source IP/Mask                             | • In         |                   |                                       |
| 1<br>Type<br>IP<br>Description   | Y  | Deny<br>Source IP/Mask                             | • In         |                   |                                       |
| 1<br>Type<br>IP<br>Description   | Y  | Deny<br>Source IP/Mask                             | • In         |                   |                                       |
| Type<br>IP<br>Description  | Y  | Source IP/Mosk                                     |              | tion IP/Mask      |                                       |
| IP<br>Description  |  |  | Destina      | tion IP/Mask      | Save                                  |
| Description  |  | ~ Rule   |              |                   | Save                                  |
|  | <ul> <li>Direction          <ul> <li>Type</li> </ul> </li> </ul> | ~ Rule   |              |                   | Save                                  |
| Precedence V Policy  | <ul> <li>Direction</li> <li>Type</li> </ul>                      | ~ Rule   |              |                   |                                       |
| Precedence V Policy  | <ul> <li>Direction</li> <li>Type</li> </ul>                      | ✓ Rule   |              |                   |                                       |
|  |  |  | ~ Action     | Description       | ~                                     |
|  |  | No Rules available                                 |              |                   |                                       |
|  |  |  |              |                   | ▼ Items per page                      |
|  |  |  |              |                   |                                       |
| DNS-ACL  |  |  |              |                   |                                       |
|  |  |  |              |                   |                                       |
| Precedence   | Action     Deny  | Domain   |              |                   | Save                                  |
|  |  | · · · · · · · · · · · · · · · · · · ·              |              |                   | ~ Action                              |
| Precedence V Policy  | <ul> <li>Domain Name</li> </ul>                                  |  |              |                   | <ul> <li>Action</li> </ul>            |
|  |  |  |              |                   |                                       |
|  |  | N. D. D. J. B. B. B. B. B. B.                      |              |                   |                                       |
|  |  | No Rules available                                 |              |                   |                                       |
|  |  | No Rules available                                 |              |                   |                                       |
|  |  | NO Rules avaliable                                 |              | 14 4 1            |                                       |
|  |  | No Rules avaliable                                 |              |                   | ↓<br>1 ► ►I TO ▼ items per page       |
|  |  | NO Rules avaliable                                 |              | Id d I            | ₹<br>1 ► ►I TO ▼ items per page       |
| MAC Authentication   |  |  |              |                   | I I I I I I I I I I I I I I I I I I I |
|  | Authentication Policy Deny                                       |  | Ŧ            |                   | (1 ► ►1 10 ▼ Rems per page            |
|  | ,  |  | •<br>•       |                   |                                       |
|  | MAC  |  | •            | [4] (4) T         |                                       |
| MAC  | ,  |  |              |                   |                                       |
|  | MAC  |  | ▼<br>Inption |                   | See                                   |
| MAC  | MAC  |  | ription      |                   | Save                                  |
|  | MAC  | <ul> <li>Action</li> <li>Desc</li> </ul>           | ription      |                   | Save                                  |

## Figure 32 Configure: WLAN > Access parameters

# Table 30 Configure: WLAN > Passpoint parameters

| Parameters                             | Description  | Range | Default  |  |  |  |  |  |  |
|--|--|-------|----------|--|--|--|--|--|--|
| Configuration > Hotspot2.0 / Passpoint |  |       |          |  |  |  |  |  |  |
| Enable                                 | Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning. | _     | Disabled |  |  |  |  |  |  |

| Parameters             | Description  | Range    | Default  |
|------------------------|--|----------|----------|
| DGAF                   | Downstream Group Addressed Forwarding, when<br>enabled the WLAN doesn't transmit any multicast and<br>broadcast packets.   | -        | Disabled |
| ANQP Domain<br>ID      | ANQP domain identifier included when the HS 2.0 indication element is in Beacon and Probe Response frames.   | 0-65535  | 0        |
| Comeback<br>Delay      | Comeback Delay in milliseconds.  | 100-2000 | 0        |
| Access<br>Network Type | <ul> <li>The configured Access Network Type is advertised to STAs. Following are the different network types supported:</li> <li>Private</li> <li>Chargeable Public</li> <li>Emergency Services</li> <li>Free Public</li> <li>Personal Device</li> <li>Private with Guest</li> <li>Test</li> </ul> | _        | Private  |
| ASRA                   | Wildcard Indicates that the network requires a further step for  |          | Disabled |
| ASKA                   | access.  | _        | Disabled |
| Internet               | The network provides connectivity to the Internet if not specified.  | _        | Disabled |
| HESSID                 | Configures the desired specific HESSID network identifier or the wildcard network identifier.  | _        | -        |
| Venue Info             | Configure venue group and venue type.  | -        | -        |
| Roaming<br>Consortium  | The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.  | _        | -        |
| ANQP<br>Elements       | <ul> <li>Select any one of the following:</li> <li>3GPP Cellular Network Information</li> <li>Connection Capability</li> <li>Domain Name List</li> <li>Icons</li> <li>IP Address Type information</li> </ul>   | _        | -        |

| Parameters | Description                 | Range | Default |
|------------|-----------------------------|-------|---------|
|            | NAI Realm List              |       |         |
|            | Network Authentication Type |       |         |
|            | Operating Class Indication  |       |         |
|            | Operator Friendly Names     |       |         |
|            | OSU Provider List           |       |         |
|            | Venue Name Information      |       |         |
|            | WAN Metrics                 |       |         |

To configure the above parameter, navigate to the **Configure > WLAN > Passpoint** tab and provide the details as given below:

- 1. Select **Enable** checkbox to enable passpoint functionality.
- 2. Select **DGAF** checkbox to enable Downstream Group Addressed Forwarding functionality.
- 3. Enter the domain identifier value in **ANQP Domain ID** textbox.
- 4. Enter **Comeback Delay** in milliseconds in the textbox.
- 5. Choose the Access Network Type value from the drop-down list.
- 6. Enable **ASRA** checkbox if the network requires additional steps for access.
- 7. Enable Internet checkbox for the network to provide connectivity to the Internet.
- 8. Enter the **HESSID** to configure the desired specific HESSID network identifier or the wildcard network identifier.
- 9. Select Venue Info from the drop-down list.
- 10. To add **Roaming Consortium** value, enter the value in the textbox and click **Add**. To delete a **Roaming Consortium** value, select from the drop-down list and click **Delete**.
- 11. Click Save.

| Radius Server Guest Acce  | ess Usage Limits So | cheduled Access | Access          | Passpoint          |                     |                    |                      |   |                 |                            |   |  |
|---|---------------------|-----------------|-----------------|--------------------|---------------------|--------------------|----------------------|---|-----------------|----------------------------|---|--|
| onfiguration  |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| Hotspot2.0 / Passpoint  |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| notspotz.orr ussponn  |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
|   |                     | Enable Pas      | spoint (Release | 2) enables a sec   | cure hotspot n      | etwork access, onl | ne sign up and Polic | Provisioning                            |                 |                            |   |  |
|   |                     | DGAF Dov        | vnstream Group  | Addressed Forv     | varding, When       | enabled the WLA    | doesn't transmit an  | multicast and broad                     | cast packets    |                            |   |  |
|   | ANQP D              | omain ID 0      |                 |                    |                     |                    | ANQP domai           | identifier (0-65535)                    | included when   | the HS 2.0 Indication ele  | ment is in Beacon and Probe                         | Response frames  |
|   | Comeba              | ck Delay 0      |                 |                    |                     |                    | Comeback de          | ay in milliseconds. S                   | upported range  | is 100-2000 ms, use 0      | o disable   |  |
|   | Access Netw         | ork Type Priva  | ate             |                    |                     | ,                  | The configure        | Access Network Ty                       | oe is advertise | to STAs.                   |   |  |
| ASRA Additional Step Required for Access, indicate that the network requires a further step for access  |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| Also      Also |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
|   |                     | HESSID          | notifon provide | is connectivity to | , and inserticity . | onermae anapeer    |                      | lesired specific HES                    | SID network id  | entifier or the wildcard n | twork identifier                                    |  |
|   |                     |                 |                 |                    |                     |                    |                      | ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, |                 |                            | Configure Venue group a                             | ad Manua Arma  |
|   |                     |                 | ise select      |                    |                     |                    |                      |   |                 | · ·                        |   |  |
|   | Roaming Cor         | nsortium        |                 |                    |                     | Add                |                      |   | ۳               | Delete                     | The roaming consortium<br>used to authenticate with | and/or SSP whose security credentials can be<br>the AP |
|   |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| ANQP Elements (Access   | Network Query Proto | col)            |                 |                    |                     |                    |                      |   |                 |                            |   |  |
|   |                     | ANQP Plea       | ise Select      |                    |                     |                    |                      | T                                       |                 |                            |   |  |
|   |                     | Plea            | ise Select      |                    |                     |                    |                      | •                                       |                 |                            |   |  |
|   |                     |                 |                 |                    |                     | _                  |                      |   |                 |                            |   |  |
|   |                     |                 |                 |                    |                     | Sav                | Cancel               |   |                 |                            |   |  |
|   |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| immary  |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| otspot2.0 / Passpoint   |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
|   |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
| Status  | Disable             |                 |                 |                    |                     | DGAF               | Disable              |   |                 | Domain ID                  | 0   |  |
| Access Network Type   | Private             |                 |                 |                    |                     | ASRA               | No                   |   |                 | Internet                   | Not Available                                       |  |
| HESSID  |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |
|   |                     |                 |                 |                    |                     |                    |                      |   |                 |                            |   |  |

## **Figure 33** Configure: WLAN > Passpoint parameters

# Chapter 9: Configuration - Network

This chapter describes the following topics:

- Overview
- Configuring Network parameters

# Overview

This chapter gives an overview of cnPilot configurable parameters related to LAN, VLAN, Routes, DHCP server, Tunnel, ACL and Firewall.

# Configuring Network parameters

cnPilot network configuration parameters are segregated into following sections:

- VLAN
- Routes
- Ethernet Ports
- Security
- DHCP
- Tunnel
- PPPoE
- VLAN Pool

# IPv4 network parameters

# VLAN

#### Table 31 Configure: Network > VLAN > IPv4 parameters

| Parameters  | Description   | Range | Default |
|-------------|---|-------|---------|
| VLAN > IPv4 |   |       |         |
| Edit        | Provision to select the VLAN interface that user is intended to view/update configuration.                          | _     | VLAN 1  |
| Address     | Provision to configure mode of IPv4 address<br>configuration for an interface selected. Two modes are<br>supported: | _     | DHCP    |
|             | 1. DHCP   |       |         |
|             | This is the default mode in which cnPilot device tries to obtain IPv4 address from DHCP server.                     |       |         |
|             | 2. Static IP  |       |         |

| Parameters            | Description   | Range | Default             |
|-----------------------|---|-------|---------------------|
|                       | User must explicitly configure IPv4 address and Netmask for a VLAN selected.  |       |                     |
| NAT                   | This option is preferable when you defined local DHCP<br>servers. This option when selected, traffic from wireless<br>stations are NAT'ed to the default gateway interface IP.  |       | Disabled            |
| Zeroconf IP           | Zeroconf IP is recommended to be enabled. This interface<br>is available only on VLAN1 configuration section. If VLAN<br>1 is not allowed in Ethernet interfaces, this IP will not be<br>accessible.                        | _     | Enabled             |
| DHCP Relay<br>Agent   | This option is enabled when DHCP server is hosted on a VLAN which is not same as client that is requesting for DHCP IP. Enabling this appends Option 82 in the DHCP packets. Following information is allowed to configure: | -     | Disabled            |
|                       | 1. DHCP Option 82 Circuit ID  |       |                     |
|                       | Configurable parameters under this option are as follows:   |       |                     |
|                       | Hostname  |       |                     |
|                       | • APMAC   |       |                     |
|                       | BSSID   |       |                     |
|                       | • SSID  |       |                     |
|                       | Custom  |       |                     |
|                       | 2. DHCP Option 82 Remote ID   |       |                     |
|                       | Configurable parameters under this option are as follows:   |       |                     |
|                       | Hostname  |       |                     |
|                       | • APMAC   |       |                     |
|                       | BSSID   |       |                     |
|                       | • SSID  |       |                     |
|                       | • Custom  |       |                     |
| Request<br>Option All | This configuration decides the interface on which cnPilot AP will learn the following:  | _     | Enabled on<br>VLAN1 |
|                       | IPv4 default gateway  |       |                     |
|                       | • DHCP client options like Option 43 and Option 15<br>(Controller discovery like controller host name / IPv4<br>address)  |       |                     |
|                       | DNS Servers   |       |                     |
|                       | Domain Name   |       |                     |

To configure the above parameter, navigate to the **Configure > Network > VLAN** tab and provide the details as given below:

To configure VLAN IPv4:

- 1. Select **Edit** checkbox to enable VLAN1 functionality.
- 2. Enable **DHCP** or **Static IP** mode of IPv4 address configuration from the **Address** checkbox.
- 3. Enable **NAT** checkbox.
- 4. Enable **Zeroconf IP** checkbox.
- 5. Enter **DHCP Relay Agent** parameter in the textbox.
- 6. Select **DHCP Option 82 Circuit ID** from the drop-down list.
- 7. Select DHCP Option 82 Remote ID from the drop-down list.
- 8. Enable Request Option All checkbox.
- 9. Click Save.

#### Figure 34 Configure: Network > VLAN > IPv4 parameters

| VLAN | Routes   | Ethernet Ports | Security | DHCP                                | Tunnel         | PPPoE   | VLAN Pool |  |                      |
|------|--|----------------|----------|-------------------------------------|----------------|---|-----------|--|----------------------|
|      | LAN  | Edit VLAN 1    | v        | Del                                 | ete this inter | face  |           |  | Add new L3 Interface |
|      | Address<br>NAT<br>Zeroconf IP<br>DHCP Relay Agent<br>DHCP Option 82 Circuit ID<br>DHCP Option 82 Remote ID<br>Request Option All |                |          | Support<br>XXX.XXX.<br>None<br>None | t 169.254.x.x  | d, IP addresses und<br>local IP address<br>option all on this int | •         | Enables relay agent and assign DHCP server to it |                      |
|      |  | IPv6           |          |                                     |                |   |           |  |                      |

L

MTU

cnPilot devices honour MTU advertised in DHCP Option 26. Below are the criteria for selecting MTU:

- By default, MTU is updated only if option 26 value is between 1500 1600 bytes.
- If user requires MTU less than 1500 bytes as advertised in option 26, enable MTU option as follows:

E430-6E3A07(config)# interface vlan <VLAN ID> E430-6E3A07(config-vlan-<VLAN ID>)# ip dhcp mtu E430-6E3A07(config-vlan-<VLAN ID>)# save

## DHCP Client Options

cnPilot devices learn multiple DHCP options for all VLAN interfaces configured on the device. Based on configured criteria, values of these options are used by the system. Below table lists the different DHCP options.

| Options   | Description   | Usage   | Reference CLI               |
|-----------|---|---|-----------------------------|
| Option 1  | The subnet mask option specifies<br>the client's subnet mask as per RFC<br>950.   | Based on state of<br>"Request Option All",<br>device chooses subnet<br>mask from respective<br>VLAN interface.  | show ip route               |
| Option 3  | This option specifies a list of IP<br>addresses for routers on the client's<br>subnet.  | Based on state of<br>"Request Option All",<br>device chooses route<br>learnt from respective<br>VLAN interface. Only<br>first route is honored                          | show ip route               |
| Option 6  | The domain name server option<br>specifies a list of Domain Name<br>System (STD 13, RFC 1035) name<br>servers available to the client.<br>Servers SHOULD be listed in order<br>of preference. | Based on state of<br>"Request Option All",<br>device chooses subnet<br>mask from respective<br>VLAN interface. Top two<br>DNS servers are honored<br>by cnPilot device. | show ip name-server         |
| Option 15 | This option specifies the domain<br>name that client should use when<br>resolving hostnames via the<br>Domain Name System.  | More details are<br>provided in DHCP<br>Option 15/24.   | show ip dhcp-client<br>info |
| Option 26 | This option specifies MTU size in a network.  | More details are provided in MTU.   | show ip dhcp-client<br>info |

### Table 32 DHCP Options

| Options   | Description  | Usage  | Reference CLI                |
|-----------|--|--|------------------------------|
| Option 28 | This option specifies the broadcast address that client should use   | Broadcast address learnt<br>for all VLAN interfaces<br>are used respectively as<br>per standards                                   | show ip dhcp-client-<br>info |
| Option 43 | This option is used to help the AP in<br>obtaining cnMaestro IP address<br>from the DHCP server while DHCP<br>request to get an IP address is sent<br>to the DHCP server.  | More details are<br>provided in IPv4<br>DHCP Option 43/52<br>DHCP Option 15/24   | show ip dhcp-client<br>info  |
| Option 51 | This option is used in a client<br>request to allow the client to<br>request a lease time for the IP<br>address. In a server reply, a DHCP<br>server uses this option to specify<br>the lease time it is willing to offer. | cnPilot renew leases for<br>all VLAN interfaces<br>configured based on<br>lease time that has been<br>learned from DHCP<br>server. | show ip dhcp-client<br>info  |
| Option 54 | DHCP clients use the contents of<br>the 'server identifier' field as the<br>destination address for any DHCP<br>messages unicast to the DHCP<br>server.  | cnPilot learns DHCP<br>server IP for all VLAN<br>interfaces configured.  | show ip dhcp-client<br>info  |
| Option 60 | This option is used by DHCP clients<br>to optionally identify the vendor<br>type and configuration of a DHCP<br>client.  | For cnPilot device, value<br>is updated as Cambium-<br>WiFi-AP.  | show ip dhcp-client<br>info  |

# Routing & DNS

| Parameters         | Description  | Range | Default  |
|--------------------|--|-------|----------|
| Default<br>Gateway | Provision to configure default gateway. If this is provided,<br>cnPilot device installs this gateway as this is the highest<br>priority. | _     | -        |
| DNS Server         | Provision to configure Static DNS server on cnPilot device.<br>Maximum of two DNS servers can be configured.                             | _     | -        |
| Domain Name        | Provision to configure Domain Name. If this is provided,<br>cnPilot device installs this Domain Name as this is highest<br>priority.     | _     | -        |
| DNS Proxy          | cnPilot device can acts as DNS proxy server when this parameter is enabled.  | _     | Disabled |

#### Table 33 Configure: Network > VLAN > Routing & DNS > IPv4 parameters

To configure the above parameter, navigate to the **Configure > Network > VLAN > Routing & DNS** tab and provide the details as given below:

- 1. Enter **Default Gateway** IPv4 address in the textbox.
- 2. Enter **Domain Name** in the textbox.
- 3. Enter primary domain server name in the **DNS Server 1** textbox.
- 4. Enter secondary domain server name in the **DNS Server 2** textbox.
- 5. Enable **DNS Proxy** checkbox.
- 6. Click Save

#### Figure 35 Routing & DNS > IPv4 parameters

| Default Gateway |           | IP address of default gateway |
|-----------------|-----------|-------------------------------|
| DNS Server 1    |           | Primary Domain Name Server    |
| DNS Server 2    |           | Secondary Domain Name Server  |
| Domain Name     |           | Domain name                   |
| DNS Proxy       | DNS Proxy |                               |
|                 |           |                               |
| Pv6             |           |                               |

# Routes

| Parameters                       | Description  | Range | Default |
|----------------------------------|--|-------|---------|
| Gateway<br>Source<br>Precendence | Provision to prioritize default gateway and DNS servers<br>when cnPilot device has learnt from multiple ways. Default<br>order is Static, DHCP and PPPoE.  | _     | Static  |
| Add Multiple<br>Route Entries    | <ul> <li>User has provision to configure static Routes. Parameters that are required to configure static Routes are as follows:</li> <li>Destination IP</li> <li>Mask</li> <li>Gateway</li> </ul>  | _     | _       |
| Port<br>Forwarding               | <ul> <li>This feature is required when wireless stations are behind<br/>NAT. User can access the services hosted on wireless<br/>stations using this feature. Following configurable<br/>parameters are required to gain the access of services<br/>hosted on wireless stations which are behind:</li> <li>Port</li> <li>IP Address</li> <li>Type</li> </ul> | _     | _       |

#### Table 34 Configure: Network > Routes> IPv4 parameters

To configure the above parameter, navigate to the **Configure > Network > Routes** tab and provide the details as given below:

#### To configure Gateway Source Precedence:

- 1. Select **STATIC**, **DHCPC** or **PPPoE** from the **Gateway Source Precedence** checkbox.
- 2. Click Save.

#### To configure Add Multiple Route Entries:

- 1. Enter **Destination IP** address in the textbox.
- 2. Enter **Mask** IPv4 address in the textbox.
- 3. Enter Gateway IPv4 address in the textbox.
- 4. Click Save.

### To configure Port Forwarding:

- 1. Enter **Port** in the textbox.
- 2. Enter IP Address in the textbox.
- 3. Select **Type** from the drop-down list.
- 4. Click Save.

| Gateway Source Prece  | dence           |                                       |  |
|-----------------------|-----------------|---------------------------------------|--|
| IPv4                  |                 |                                       |  |
|                       |                 | IPv6                                  |  |
| STATIC                | ^ <b>^</b>      | STATIC                                |  |
| DHCPC<br>PPPoE        | · ·             | AUTO-CONFIG/DHCPC                     |  |
|                       | <b>•</b>        | <b></b>                               |  |
| Save                  |                 | Save                                  |  |
|                       | trice ID: 4     |                                       |  |
| Add Multiple Route Er | itries - IPV4   |                                       |  |
| Destination IP        | Mask            | Gateway                               | Save   |
| XXX.XXX.XXX.XXX       | XXX.XXX.XXX.XXX |                                       | ouve   |
| Destination IP        | ✓ Mask          | Y Gateway Y Action                    |  |
|                       |                 |                                       |  |
|                       | No route        | es available                          |  |
|                       |                 |                                       |  |
|                       |                 |                                       |  |
|                       |                 |                                       |  |
|                       |                 |                                       | -  |
|                       |                 | I I I I I I I I I I I I I I I I I I I | page   |
|                       |                 |                                       |  |
| Add Multiple Route Er | itries - IPv6   |                                       |  |
|                       |                 |                                       |  |
| Destination IP/prefix | Gateway         | Save                                  |  |
| Destination IP        | ~ Gateway       | ~ Action                              |  |
|                       | * Gateway       |                                       |  |
|                       | ~ Gateway       | Action                                | •  |
|                       | 2               |                                       |  |
|                       | 2               | es available                          | •  |
|                       | 2               |                                       | *  |
|                       | 2               |                                       | •  |
|                       | 2               |                                       |  |
|                       | 2               | es available                          | •  |
|                       | 2               |                                       | ↓<br>▼<br>page   |
|                       | 2               | es available                          | The second secon |
| Port Forwarding       | 2               | es available                          | ↓<br>▼<br>page   |
| -                     | No route        | es available                          | ↓<br>page  |
| Port Forwarding       | 2               | es available                          | page   |
| Port                  | IP Address      | es available                          |  |
| -                     | IP Address      | es available                          |  |
| Port                  | IP Address      | es available                          | Save   |
| Port                  | IP Address      | es available                          | Save   |
| Port                  | IP Address      | es available                          | Save   |
| Port                  | IP Address      | es available                          | Save   |
| Port                  | IP Address      | es available                          | Save   |
| Port                  | IP Address      | es available                          | Save   |
| Port                  | IP Address      | es available                          | Save   |

Figure 36 Routes > IPv4 parameters

# IPv6 network parameters

# VLAN

## Table 35 Configure: Network > VLAN > IPv6 parameters

| Parameters            | Description  | Range | Default             |
|-----------------------|--|-------|---------------------|
| Address               | Provision to configure mode of IPv6 address configuration for an interface selected. Five modes are supported:                               |       | AutoConfig          |
|                       | • Disabled   |       |                     |
|                       | AutoConfig   |       |                     |
|                       | • Static   |       |                     |
|                       | Stateless DHCPv6   |       |                     |
|                       | Stateful DHCpv6  |       |                     |
| Request<br>Option All | This configuration decides the interface on which cnPilot<br>AP will learn the following:  | _     | Enabled on<br>VLAN1 |
|                       | IPv6 default gateway   |       |                     |
|                       | <ul> <li>DHCP client options like Option 52 and Option 24<br/>(Controller discovery like controller host name / IPv6<br/>address)</li> </ul> |       |                     |
|                       | DNS Servers  |       |                     |
|                       | Domain Name  |       |                     |

To configure the above parameter, navigate to the **Configure > Network > VLAN** tab and provide the details as given below:

#### To configure VLAN IPv6:

- 1. Select required IPv6 address configuration from the Address drop-down list.
- 2. Enable Request Option All checkbox.
- 3. Click Save.

| VLAN         | Routes | Ethernet Ports | Security | DHCP     | Tunnel        | PPPoE         | VLAN Pool        |                           |  |
|--------------|--------|----------------|----------|----------|---------------|---------------|------------------|---------------------------|--|
| <b>،</b> _ ۱ | /LAN — |                |          |          |               |               |                  |                           |  |
|              |        | Edit VLAN 1    | ٣        | Delete t | his interface |               |                  | Add new L3 Interface      |  |
|              |        | IPv4           |          |          |               |               |                  |                           |  |
|              |        | IPv6           |          |          |               |               |                  |                           |  |
|              |        | Address        |          | A        | utoConfig     |               | •                |                           |  |
|              |        | Request Opt    | ion All  |          | Use IPv6 Ga   | teway, DNS, I | DHCPv6 options n | aceived on this interface |  |
|              |        | General        |          |          |               |               |                  |                           |  |
|              |        | -              |          |          |               |               |                  |                           |  |

### Figure 37 Configure: Network > VLAN > IPv6 parameters

# Routing & DNS

| Parameters         | Description  | Range | Default  |
|--------------------|--|-------|----------|
| Default<br>Gateway | Provision to configure default gateway. If this is provided,<br>cnPilot device installs this gateway as this is the highest<br>priority. | -     | _        |
| DNS Server         | Provision to configure Static DNS server on cnPilot device.<br>Maximum of two DNS servers can be configured.                             | _     | _        |
| Domain Name        | Provision to configure Domain Name. If this is provided,<br>cnPilot device installs this Domain Name as this is highest<br>priority.     | -     | -        |
| IPv6<br>Preference | When enabled, IPv6 is preferred over IPv4 bases on DNS response.   | _     | Disabled |

To configure the above parameter, navigate to the **Configure > Network > Routing & DNS** tab and provide the details as given below:

- 1. Enter **Default Gateway** IPv6 address in the textbox.
- 2. Enter primary domain server name in the **DNS Server 1** textbox.
- 3. Enter secondary domain server name in the **DNS Server 2** textbox.
- 4. Enter **Domain Name** in the textbox.
- 5. Enable IPv6 Preference checkbox.
- 6. Click Save

| ∎ IPv4          |                               |                                |
|-----------------|-------------------------------|--------------------------------|
| ⊐ IPv6          |                               |                                |
| Default Gateway |                               | IP address of default gateway  |
| DNS Server 1    |                               | Primary Domain Name Server     |
| DNS Server 2    |                               | Secondary Domain Name Server   |
| Domain Name     |                               | Domain name                    |
| IPv6 Preference | Prefer IPv6 address over IPv4 | for addresses resolved via DNS |

#### Figure 38 Routing & DNS > IPv6 parameters

# Routes

#### Table 37 Configure: Network > Routes> IPv6 parameters

| Parameters                       | Description   | Range | Default |
|----------------------------------|---|-------|---------|
| Gateway<br>Source<br>Precendence | Provision to prioritize default gateway and DNS servers<br>when cnPilot device has learnt from multiple ways. Default<br>order is Static and AUTO-CONFIG/DHCPC. | -     | Static  |
| Add Multiple<br>Route Entries    | User has provision to configure static Routes. Parameters that are required to configure static Routes are as follows:<br>• Destination IP/prefix               | -     | -       |
|                                  | Gateway   |       |         |

To configure the above parameter, navigate to the **Configure > Network > Routes** tab and provide the details as given below:

To configure Gateway Source Precedence:

- 1. Select STATIC or AUTO-CONFIG/DHCPC from the Gateway Source Precedence checkbox.
- 2. Click Save.

To configure Add Multiple Route Entries:

- 1. Enter **Destination IP/prefix** address in the textbox.
- 2. Enter Gateway IPv6 address in the textbox.
- 3. Click Save.

| Gateway Source Pre  | cedence                  | _                     |                                    |                            |   |
|---|--------------------------|-----------------------|------------------------------------|----------------------------|---|
| IPv4  |                          |                       | IPv6                               |                            |   |
| STATIC  | <b>A</b>                 |                       | STATIC                             | <b>^</b>                   |   |
| DHCPC<br>PPPoE  | ~                        |                       | AUTO-CONFIG/DHCPC                  |                            |   |
|   | -                        |                       |                                    | -                          |   |
| Save  |                          |                       | Save                               |                            |   |
|   |                          | L                     |                                    |                            |   |
| Add Multiple Route E                                      | ntries - IPv4            |                       |                                    |                            |   |
|   |                          |                       |                                    |                            |   |
| Destination IP  |                          | Mask                  | Gateway                            |                            |   |
| XXX.XXX.XXX   |                          | XXX.XXX.XXX.XXX       | XXX.XXX.XX0                        | XXX                        | Save  |
| Destination IP  | <ul> <li>Mask</li> </ul> | ~ Ga                  | iteway                             | <ul> <li>Action</li> </ul> |   |
|   |                          |                       |                                    |                            | *   |
|   |                          | No routes a           | wailablo                           |                            |   |
|   |                          | no roules a           | anable                             |                            |   |
|   |                          |                       |                                    |                            |   |
|   |                          |                       |                                    |                            |   |
|   |                          |                       |                                    |                            |   |
|   |                          |                       |                                    |                            |   |
|   |                          |                       |                                    |                            | <b>v</b>                                    |
|   |                          |                       | <b> </b> ◀ ◀ 1                     |                            | items per page                              |
|   |                          |                       |                                    |                            |   |
| Add Multiple Route E                                      |                          | Gateway               |                                    | Gurra                      |   |
|   |                          | Gateway<br>ateway     | <ul> <li>Actio</li> </ul>          | Save                       |   |
| Destination IP/prefix                                     |                          |                       | <ul> <li>Actio</li> </ul>          |                            |   |
| Destination IP/prefix                                     |                          | ateway                |                                    |                            |   |
| Destination IP/prefix                                     |                          |                       |                                    |                            | <u>ــــــــــــــــــــــــــــــــــــ</u> |
| Destination IP/prefix                                     |                          | ateway                |                                    |                            | •   |
| Destination IP/prefix                                     |                          | ateway                |                                    |                            | •   |
| Destination IP/prefix                                     |                          | ateway                |                                    |                            |   |
| Destination IP/prefix                                     |                          | ateway                |                                    |                            |   |
| Destination IP/prefix                                     |                          | ateway                | available                          | n                          | ▼ items per page                            |
| Destination IP/prefix                                     |                          | ateway                | available                          | n                          | vitems per page                             |
| Destination IP/prefix                                     |                          | ateway                | available                          | n                          | ▼<br>items per page                         |
| Destination IP/prefix                                     |                          | ateway                | available                          | n                          | v items per page                            |
| Destination IP/prefix Destination IP Port Forwarding      | ~ G                      | ateway<br>No routes a | available                          | n                          | ▼<br>items per page                         |
| Destination IP/prefix Destination IP                      |                          | ateway<br>No routes a | available                          | n                          |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | Type<br>TCP                        | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding      | ~ G                      | No routes a           | available                          | n                          |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | Type<br>TCP                        | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | available<br>Type<br>TCP<br>otocol | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | available<br>Type<br>TCP<br>otocol | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | available<br>Type<br>TCP<br>otocol | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | available<br>Type<br>TCP<br>otocol | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | available<br>Type<br>TCP<br>otocol | n<br>(1 ) 10               |   |
| Destination IP/prefix Destination IP Port Forwarding Port | V Gi                     | No routes a           | available<br>Type<br>TCP<br>otocol | n<br>(1 ) 10               |   |

Figure 39 Routes > IPv6 parameters

# General network parameters

| Parameters           | Description   | Range | Default                                     |
|----------------------|---|-------|---|
| Management<br>Access | <ul> <li>Provision to restrict the access of device in all modes CLI (Telnet, SSH), GUI (HTTP, HTTPs) and SNMP. User can configure restriction of device access as follows:</li> <li>Block</li> <li>Allow from Wired</li> <li>Allow from both wired and wireless</li> </ul> | -     | Allow from<br>both Wired<br>and<br>Wireless |

Table 38 Configure: Network > VLAN > General parameters

Select Management Access to configure restriction of device from the drop-down list.

### Figure 40 Configure: Network > VLAN > General parameters

| VLAN       Edit       VLAN 1       Delete this interface       Add new L3 Interface         Image: Pv4       Image: Pv4       Image: Pv4       Image: Pv4         Image: Image: Pv6       Image: Pv6       Image: Pv6       Image: Pv6         Image: Image: Pv6       Image: Pv6       Image: Pv6       Image: Pv6         Image: Image: Pv6       Image: Pv6       Image: Pv6       Image: Pv6         Image: Pv6       Image: Pv6       Image: Pv6       Image: Pv6 | VLAN | Routes | Ethernet Ports | Security | DHCP     | Tunnel        | PPPoE        | VLAN Pool  |  |
|--|------|--------|----------------|----------|----------|---------------|--------------|------------|--|
| IPv4     General   |      | VLAN   |                |          |          |               |              |            |  |
| IPv6 General   |      |        | Edit VLAN 1    | •        | Delete t | his interface |              |            | Add new L3 Interface                   |
| General  |      |        | DIPv4          |          |          |               |              |            |  |
|  |      |        | IPv6           |          |          |               |              |            |  |
| Management Access Allow from both Wired & Wireless via this interface  |      |        | General        |          |          |               |              |            |  |
|  |      |        | Managemen      | t Access | А        | llow from bo  | th Wired & V | Vireless 🔻 | CLI/GUI/SNMP access via this interface |
|  |      |        |                |          |          |               |              |            |  |

# Ethernet Ports

 Table 39 Configure: Network > Ethernet Ports parameters

| Parameters | Description   | Range | Default |
|------------|---|-------|---------|
| Ethernet   | cnPilot devices Ethernet port is provisioned to operate in following modes: | -     | Access  |
|            | 1. Access Single VLAN   |       |         |
|            | Single VLAN traffic is allowed in this mode.                                |       |         |
|            | 2. Trunk Multiple VLANs   |       |         |
|            | Multiple VLANs are supported in this mode.                                  |       |         |
|            | 3. Tunnel Mode  |       |         |

| Parameters                      | Description  | Range                       | Default     |
|---------------------------------|--|-----------------------------|-------------|
|                                 | Provision to enable L2GRE tunnel. It is applicable<br>only for Ethernet 2/3/4 ports of the cnPilot devices<br>based on model number.   |                             |             |
| Port Speed                      | Provision to configure ethernet link speed.  | -                           | Auto        |
|                                 | • Auto   |                             |             |
|                                 | • 10 Mbps  |                             |             |
|                                 | • 100 Mbps   |                             |             |
|                                 | • 1000 Mbps  |                             |             |
| Port Duplex                     | Provision to configure ethernet link duplex settings.  | Half Duplex/<br>Full Duplex | Full Duplex |
| MAC Authentica                  | ition  |                             |             |
| MAC<br>Authentication           | Provision to configure MAC Authentication.   | -                           | -           |
| MAC Auth<br>Failed              | Enabling this will allow traffic to pass on native VLAN when MAC Auth is rejected by RADIUS server.  | -                           | -           |
| MAC<br>Authentication<br>Policy | <ul> <li>Provision to set MAC ACL policy from external RADIUS server.</li> <li>Delimiter: Only colon (:) and hyphen (-) are accepted</li> <li>Upper-Case: MAC address sent in upper case only</li> </ul> | _                           | _           |
| Radius Server                   |  |                             |             |
| Authentication<br>Server        | Provision to configure RADIUS Authentication server<br>details such as Hostname/IPv4/IPv6, Shared Secret,<br>Port Number and Realm. Maximum of three RADIUS<br>server can be configured.                 | -                           | Disabled    |
| Accounting<br>Server            | Provision to configure Accounting server details such as<br>Hostname/IPv4/IPv6, Shared Secret, Port Number.<br>Maximum of three RADIUS server can be configured.   | _                           | Disabled    |
| Timeout                         | Wait time period for response from AAA server.   | 1-30                        | 3           |
| Attempts                        | Parameter to configure number of attempts that a device should send AAA request to server if no response is received within configured timeout period.   | 1-3                         | 1           |
| Accounting<br>Mode              | This field is enabled based on customer requirement.<br>Accounting packet is transmitted based on mode<br>selected.<br>1. <b>Start-Stop</b>  | _                           | None        |

| Parameters           | Description  | Range | Default                     |
|----------------------|--|-------|-----------------------------|
|                      | Accounting packets are transmitted by AP to AAA server when a wireless station is connected and then disconnects.  |       |                             |
|                      | 2. Start-Interim-Stop  |       |                             |
|                      | Accounting packets are transmitted by AP to AAA<br>server when a wireless station connects and then at<br>regular intervals of configured Interim Update<br>Interval and then when it disconnects. |       |                             |
|                      | 3. None  |       |                             |
|                      | Accounting mode will be disable.   |       |                             |
| Server Pool<br>Mode  | User can configure multiple Authorization and<br>Accounting servers. Based on number of wireless<br>stations, user can choose either Failover or Load<br>Balance mode.                             | -     | Load<br>Balance             |
|                      | 1. Load Balance  |       |                             |
|                      | AP communicates with multiple servers and ensures that authorization and accounting are equally shared across configured servers.  |       |                             |
|                      | 2. Failover  |       |                             |
|                      | AP selects the RADIUS server which is up and running based on the order of configuration.  |       |                             |
| NAS Identifier       | This is configurable parameter and is appended in RADIUS request packet.   | -     | Hostname/<br>System<br>Name |
|                      | 1. AP-ETHO-MAC:  |       |                             |
|                      | NAS identifier attribute will be ETH0 MAC address  |       |                             |
|                      | 2. AP-HOSTNAME   |       |                             |
|                      | NAS identifier attribute will be AP hostname   |       |                             |
|                      | 3. Custom:   |       |                             |
|                      | Any custom value   |       |                             |
| NAS IP               | NAS-IP attribute for use in RADIUS request packets.<br>Default is set to device IP and option to configure<br>custom IP address with the option <b>Custom.</b>                                     | -     | AP-IP                       |
| Called Station<br>ID | Following information can be communicated to RADIUS server:  |       | AP-MAC                      |
|                      | AP-MAC   |       |                             |
|                      | AP-MAC: SITE-NAME  |       |                             |
|                      | • AP-NAME  |       |                             |
|                      | AP-NAME: SITE-NAME   |       |                             |
|                      | • SITE-NAME  |       |                             |

| Parameters                    | Description   | Range           | Default  |
|-------------------------------|---|-----------------|----------|
|                               | CUSTOM  |                 |          |
| Interim<br>Update<br>Interval | This field is used when RADIUS accounting is enabled, and mode selected as Start-Interim-Stop.  | 10-65535        | 1800     |
| Dynamic<br>Authorization      | This option is required, where there is a CoA requests from AAA/RADIUS server.  | _               | Disabled |
| ACL                           |   |                 |          |
| Precedence                    | Provision to configure index of ACL rule. Packets are validated and processed based on precedence value configured.   | 1-256           | 1        |
| Policy                        | Provision to configure whether to permit or deny traffic.   | Deny/Perm<br>it | Deny     |
| Direction                     | Provision to apply the ACLs rules configured either in any direction or specific direction.   | _               | In       |
| Туре                          | <ul> <li>cnPilot devices support three layers of ACLs. A rule can be configured as below:</li> <li>IP</li> <li>IPv6</li> <li>MAC</li> <li>Proto</li> <li>Protov6</li> </ul>                               | _               | IP       |
| Source<br>IP/Mask             | This option is available when ACL type is configured to<br>an IP address. This field helps user to configure if rule<br>needs to be applied for a single IP address or range of<br>IP addresses.          | -               | _        |
| Destination<br>IP/Mask        | This option is available when ACL type is configured to<br>an IP address. This field helps user to configure if rule<br>needs to be applied for a single IP address or range of<br>IP addresses.          | -               | -        |
| Source<br>MAC/Mask            | This option is available when ACL type is configured to<br>a MAC address. This field helps user to configure if rule<br>needs to be applied for a single device MAC address or<br>range of MAC addresses. | -               | -        |
| Destination<br>MAC/Mask       | This option is available when ACL type is configured to<br>MAC address. This field helps user to configure if rule<br>needs to be applied for a single device MAC address or<br>range of MAC addresses.   | -               | -        |

| Parameters          | Description  | Range | Default |  |  |
|---------------------|--|-------|---------|--|--|
| Protocol            | This option is available when user selects ACL type as proto. User can select following protocols: | _     | ТСР     |  |  |
|                     | • TCP  |       |         |  |  |
|                     | • UDP  |       |         |  |  |
|                     | ICMP   |       |         |  |  |
|                     | • Any  |       |         |  |  |
| Source Port         | Provision to apply ACL with combination of protocol and port.                                      | _     | _       |  |  |
| Destination<br>Port | Provision to apply ACL with combination of protocol and port.                                      | _     | _       |  |  |
| Description         | To make administrator easy to understand, a text string can be added for each ACL rule.            | _     | _       |  |  |

To configure the above parameter, navigate to the **Configure > Network > Ethernet Ports** tab and provide the details as given below:

- 1. Select Access Single VLAN or Trunk Multiple VLANs from the ETH1 drop-down list.
- 2. Enter Access Mode in the textbox.
- 3. Select **Port Speed** from the drop-down list.
- 4. Select **Port Duplex** from the drop-down list.
- 5. Click Save.

To Configure MAC Authentication:

- 1. Enable MAC Authentication checkbox
- 2. Click Save.

To configure Radius Server:

- 1. Enter the RADIUS Authentication server details such as Hostname/Shared Secret/Port Number/ Realm in the **Authentication Server 1** textbox.
- 2. Enter the time in seconds of each request attempt in **Timeout** textbox.
- 3. Enter the number of attempts before a request is given up in the Attempts textbox.
- 4. Select the configuring Accounting Mode from the drop-down list.
- 5. Enable Load Balance/Failover in the Server Pool Mode checkbox.
- 6. Enter the Interim Update Interval parameter value in the textbox.
- 7. Enable **Dynamic Authorization** checkbox to configure dynamic authorization for wireless clients.
- 8. Click Save.

To configure ACL:

- 1. Select **Precedence** from the drop-down list.
- 2. Select type of **Policy** from the drop-down list.
- 3. Select **Direction** from the drop-down list.

- 4. Select **Type** from the drop-down list.
- 5. Enter IP address of source in the **Source IP/Mask** textbox.
- 6. Enter IP address of destination in the **Destination IP/Mask** textbox.
- 7. Enter **Description** in the textbox.
- 8. Click Save.

| ETH1                         | Trunk Multiple VLANs  | ~                            |   |                             |
|------------------------------|-----------------------|------------------------------|---|-----------------------------|
| Trunk Mode                   | Native VLAN 1         | Tagged                       |   |                             |
|                              | Allowed VLANs 1,10    | 010,1020 Eg: 1-3 or 4        | 4,10,22   |                             |
| Port Speed                   | Auto                  | ~                            |   |                             |
| Port Duplex                  | Full Duplex           | ~                            |   |                             |
|                              |                       | Save Cancel                  |   |                             |
| MAC Authentication           |                       |                              |   |                             |
| MAC Authentication           | Enable MAC authentica | tion                         |   |                             |
|                              |                       | Save Cancel                  |   |                             |
| Radius Casuer                |                       |                              |   |                             |
| Radius Server                | Hest                  | Pagest                       | Post  |                             |
| Authentication Server 1      | Host                  | Secret                       | Port 1812   |                             |
| 2                            | Host                  | Secret                       | Port  |                             |
|                              |                       |                              | 1812  |                             |
| 3                            | Host                  | Secret                       | Port  |                             |
|                              |                       |                              | 1812  |                             |
| Timeout                      | 3                     | Timeout in seconds of each   |   |                             |
| Attempts                     | 1                     | Number of attempts before    | giving up (1-3)   |                             |
| Accounting Server 1          | Host                  | Secret                       | Port 1813   |                             |
| 2                            | Host                  | Secret                       | Port  |                             |
| 2                            | HUSL                  | Secret                       | 1813  |                             |
| 3                            | Host                  | Secret                       | Port  |                             |
|                              |                       |                              | 1813  |                             |
| Timeout                      | 3                     | Timeout in seconds of each   | h request attempt (1-30)  |                             |
| Attempts                     | 1                     | Number of attempts before    | giving up (1-3)   |                             |
| Accounting Mode              | None ~                | Configure accounting mo      | de  |                             |
| Server Pool Mode             |                       | alance requests among the co |   |                             |
|                              |                       |                              | servers only when one is down)<br>fier attribute for use in Request |                             |
| NAS Identifier               | AP-HOSTNAME           | NAS-Identil<br>name          | ier aunoaie ior ase in riegaesi                                     | packota. Doradita to system |
| NAS IP                       | AP-IP                 | ✓ NAS-IP attr                | ibute for use in Request packe                                      | ts. Defaults to Device IP   |
| Called Station ID            | AP-MAC                | ✓ Configure A                | NP-MAC as Called-Station-Id in                                      | the RADIUS packet           |
| Interim Update Interval      | 1800                  | Interval for RADIUS Interin  | n-Accounting updates (10-6553                                       | 5 Seconds)                  |
| Dynamic Authorization        | Enable RADIUS dynamic | ic authorization (COA, DM me | ssages)   |                             |
|                              |                       | Save Cancel                  |   |                             |
| ACL                          |                       |                              |   |                             |
| Precedence                   | Policy                |                              | Direction   |                             |
| 1 ~                          | Deny                  | ~                            | In  | ~                           |
| Туре                         | Source IP/I           | Mask                         | Destinatio  | on IP/Mask                  |
| IP v                         |                       |                              |   |                             |
| Description                  |                       |                              |   | Save                        |
| Precedenc.:: Policy ~ Direct | tion ~ Type ~ R       | ule                          | <ul> <li>Descript</li> </ul>  | ion ~ Action ~              |
|                              |                       |                              |   | *                           |
|                              | No                    | Rules availab                |   |                             |
|                              | INO                   | i vuics availab              |   |                             |
|                              |                       |                              |   |                             |
|                              |                       |                              |   |                             |
|                              |                       |                              |   |                             |

## **Figure 41** Configure: Network > Ethernet Ports parameters

# Security

| Parameters        | Description   | Range | Default  |
|-------------------|---|-------|----------|
| DoS<br>Protection | cnPilot devices has inbuilt capability of detecting DoS<br>attacks on wired network. Following are the attacks that<br>are detected by cnPilot devices:   | -     | Disabled |
|                   | IP Spoof  |       |          |
|                   | Smurf Attack  |       |          |
|                   | IP Spoof Log  |       |          |
|                   | ICMP Fragment   |       |          |
| Rogue AP          |   |       |          |
| Detection         | cnPilot devices in association with cnMaestro has<br>capability of detecting Rogue APs. On enabling this all<br>neighbor information is shared to cnMaestro and reports<br>Rogue APs in the networks. |       | Disabled |

#### Table 40 Configure: Network > Security parameters

To configure the above parameter, navigate to the **Configure > Network > Security** tab and provide the details as given below:

- 1. Select any of the following from **DoS Protection** checkbox
  - a. IP Spoof
  - b. Smurf Attack
  - c. IP Spoof Log
  - d. ICMP Fragment
- 2. Enable **Detection** checkbox.
- 3. Click Save.

| VLAN | Routes   | Ethernet Ports | Security | DHCP | Tunnel | PPPoE | VLAN Pool |  |
|------|--|----------------|----------|------|--------|-------|-----------|--|
|      | DoS Protection  IP Spoof Enable IP spoof attack protection(Checks whether spoofed IP address is reachable before accept) Smurf Attack Enable SMURF attack protection(Do not respond to broadcast ICMP) IP Spoof Log Enable IP spoof log messages(Log unroutable source addresses) ICMP Fragment Enable fragmented ping attack protection(Drop fragmented ICMP packets) |                |          |      |        |       |           |  |
| F    | Rogue AP       Detection       Enable rogue AP detection   |                |          |      |        |       |           |  |
|      | Save Cancel  |                |          |      |        |       |           |  |

# Figure 42 Configure: Network > Security parameters

# DHCP

| Table 41 | Configure: | Network > | DHCP | parameters |
|----------|------------|-----------|------|------------|
|----------|------------|-----------|------|------------|

| Parameters       | Description   | Range | Default |
|------------------|---|-------|---------|
| Edit             | Provision to select DHCP Pool if multiple Pools are defined on cnPilot device.  | _     | _       |
| Address<br>Range | User can configure start and end addresses for a DHCP Pool selected from the drop-down box.   | _     | _       |
| Default Router   | Provision to configure next hop for a DHCP pool selected from drop-down box.  | _     | _       |
| Domain Name      | Provision to configure domain name for a DHCP pool selected from drop-down box.   | _     | -       |
| DNS Address      | Provision to configure DNS server for a DHCP pool selected from drop-down box.  | _     | _       |
| Network          | Provision to configure Network ID for a DHCP pool selected from drop-down box.  | _     | _       |
| Lease            | Provision to configure lease for a DHCP pool selected from drop-down box.   | _     | -       |
| Add Bind List    |   |       |         |
|                  | For every DHCP pool configured, user can bind MAC and<br>IP from the address pool defined, so that wireless station<br>gets same IP address every time they connect. Following<br>parameters are required to bind IP address: |       | _       |

| Parameters | Description | Range | Default |
|------------|-------------|-------|---------|
|            | MAC Address |       |         |
|            | IP Address  |       |         |

To configure the above parameter, navigate to the **Configure > Network > DHCP** tab and provide the details as given below:

- 1. Select DHCP pool from the **Edit** drop-down list.
- 2. Enter start and end IP addresses for a DHCP Pool selected from the **Address Range** textbox.
- 3. Enter **Default Router** IP address in the textbox.
- 4. Enter **Domain Name** for a DHCP pool selected in the textbox.
- 5. Enter **DNS Address** for a DHCP pool selected in the textbox.
- 6. Enter **Network** ID for a DHCP pool selected in the textbox.
- 7. Enter **Lease** for a DHCP pool selected in the textbox.
- 8. Click Save.

To configure Add Bind List:

- 1. Enter **MAC Address** for a DHCP pool selected in the textbox.
- 2. Enter **IP Address** for a DHCP pool selected in the textbox.
- 3. Click Save.

| Edit           | •    | Delete this | s Pool     |                   |         |  |            |           |          |                                |      | Create Po |
|----------------|------|-------------|------------|-------------------|---------|--|------------|-----------|----------|--------------------------------|------|-----------|
| Address Ra     | nge  | Start       |            | End               |         | IP add                                       | lress rang | e to be a | assigned | to clien                       | ts   |           |
| Default Router |      |             |            | Default router IP |         |  |            |           |          |                                |      |           |
| Domain N       | ame  |             |            | Domain Nar        | me      |  |            |           |          |                                |      |           |
| DNS Address    |      | Primary     |            | Secondary         |         | Domain name for the client                   |            |           |          |                                |      |           |
| Netv           | vork | IP          |            | Mask              |         | Subnet number and mask of the DHCP address p |            |           |          | ool                            |      |           |
| Lease          |      | 1           |            | Hours             |         | Minu   | ites       |           | Leas     | ease time (days:hours:minutes) |      |           |
|                |      | Save        | Cancel     |                   |         |  |            |           |          |                                |      |           |
| Add Bind List  |      | Jave        |            | IP Addres         | S       |  |            |           |          |                                | Save |           |
|                |      | Save        |            | IP Addres         |         |  |            |           |          |                                | Save |           |
| MAC Address    |      | v           | IP Address | XXX.XXX.          |         | ~  | Action     |           |          |                                | Save |           |
| MAC Address    |      |             | IP Address | XXX.XXX.          | XXX.XXX |  | Action     |           |          |                                | Save |           |

Figure 43 Configure: Network > DHCP parameters
# Tunnel

| Parameters              | Description   | Range    | Default |
|-------------------------|---|----------|---------|
| Tunnel<br>Encapsulation | Provision to enable tunnel type. Following tunnel types are supported by cnPilot devices:   | _        | OFF     |
|                         | • L2TP  |          |         |
|                         | • L2GRE   |          |         |
|                         | • OFF   |          |         |
| L2TP                    |   |          |         |
| Remote Host             | Configure L2TP end point. Either IP or hostname of endpoint is supported.   | _        | _       |
| Authentication<br>Info  | Provision to configure credentials required for L2TP authentication.  | _        | -       |
| Auth Type               | <ul> <li>Provision to select the PPP authentication method.</li> <li>Following are the options available:</li> <li>DEFAULT</li> <li>CHAP</li> <li>MS-CHAP</li> <li>MS-CHAP v2</li> <li>PAP</li> </ul> | _        | Default |
| TCP MSS                 | Provision to configure TCP Maximum Segment Size.  | 422-1410 | 1400    |
| PMTU<br>Discovery       | Provision to enable to discover PMTU in network.  | _        | Enabled |
| L2GRE                   |   |          |         |
| Remote Host             | Configure L2GRE end point. Either IPv4/IPv6 address or hostname of endpoint is supported.   | _        | -       |
| DSCP                    | User can configure priority of GRE packets.   | _        | 0       |
| TCP MSS                 | Provision to configure TCP MSS value.   | 472-1460 | 1402    |
| PMTU<br>Discovery       | Provision to enable to discover PMTU in network.  | _        | Enabled |
| MTU                     | Maximum Transmission Unit.  | 850-1460 | 1460    |

## Table 42 Configure: Network > Tunnel parameters

| Parameters  | Description   | Range | Default  |
|-------------|---|-------|----------|
| Cambium GRE | It's a proprietary GRE protocol designed using RFC 8086<br>to establish tunnel between cnMaestro c4000 Controller<br>and cnPilot devices. | -     | Disabled |
| GRE in UDP  | GRE protocol designed to establish tunnel between any third-party vendor which complies RFC 8086.   | _     | Disabled |

To configure the above parameter, navigate to the **Configure > Network > Tunnel** tab and provide the details as given below:

1. Select Tunnel type from the Tunnel Encapsulation drop-down list.

To configure L2TP:

- 2. Enter IP address or domain name in the **Remote Host** textbox.
- 3. Enter credentials required for L2TP authentication in the Authentication Info textbox.
- 4. Select authentication type from the Auth Type drop-down list.
- 5. Enter TCP Maximum Segment Size in the TCP MSS textbox.
- 6. Enable PMTU Discovery checkbox.
- 7. Enter Maximum Transmission Unit in the MTU textbox.
- 8. Click Save.

To configure L2GRE:

- 9. Enter IP address or domain name in the Remote Host textbox.
- 10. Enter DSCP in the textbox.
- 11. Enter TCP Maximum Segment Size in the TCP MSS textbox.
- 12. Enable PMTU Discovery checkbox.
- 13. Enter Maximum Transmission Unit in the MTU textbox.
- 14. Enable Cambium GRE checkbox.
- 15. Enable GRE in UDP checkbox.
- 16. Click Save.

| L2TP                |  |       |   |                              |  |
|---------------------|--|-------|---|------------------------------|--|
|                     |  |       |   |                              |  |
| Remote Host         | 0.0.0.0  |       |   | IP address or domain         |  |
| Authentication Info | admin  | ••••• |   | Max 64 characters            |  |
| Auth Type           | DEFAULT  | •     | MS-CHAPv2                                       | 2, MS-CHAP, CHAP, PAP        |  |
| TCP MSS             | € 1400   |       | TCP Maxi<br>1410 byte                           | mum Segment Size (422-<br>s) |  |
| PMTU Discovery      | al de la companya de |       | Path MTU Discovery                              |                              |  |
| Remote Host         | 0.0.0.0  |       | IP address or domain                            |                              |  |
| DSCP                | 0  |       | Differentiated Service Code Point               |                              |  |
| TCP MSS             | ☑ 1402   |       | TCP Maximum Segment Size (472-<br>1460 bytes)   |                              |  |
| PMTU Discovery      |  |       | Path MTU Discovery                              |                              |  |
| MTU                 | 1460   |       | Configure MTU for L2GRE tunnel (850-1460 bytes) |                              |  |
| GRE                 |  | •     |   |                              |  |

## Figure 44 Configure: Network > Tunnel parameters

# PPPoE

| Parameters   | Description   | Range | Default |
|--------------|---|-------|---------|
| Enable       | Provision to enable PPPoE client.                                       | _     | Disable |
| VLAN         | User can configure VLAN ID where PPPoE client should obtain IP address. | _     | -       |
| Service Name | Configure PPPoE service name  | _     | _       |

## Table 43 Configure: Network > PPPoE parameters

| Parameters             | Description  | Range    | Default  |
|------------------------|--|----------|----------|
| Authentication<br>Info | Provision to configure credentials required for PPPoE authentication.      | _        | -        |
| MTU                    | Maximum Transmission Unit.   | 500-1492 | 1430     |
| TCP MSS<br>Clamping    | Configure PPPoE end point. Either IP or hostname of endpoint is supported. | _        | Enabled  |
| Management<br>Access   | If enabled, user can access device either using UI or SSH with PPPoE IP.   | _        | Disabled |

To configure the above parameter, navigate to the **Configure > Network > PPPoE** tab and provide the details as given below:

- 1. Select **Enable** checkbox to enable PPPoE functionality.
- 2. Enter the VLAN ID assigned to the PPPoE in the VLAN textbox.
- 3. Enter **Service Name** in the textbox.
- 4. Enter the username and password for the device in the Authentication Info textbox.
- 5. Enter the MTU value PPPoE connection in the **MTU** textbox.
- 6. Enable the TCP MSS clamping for the PPPoE connection.
- 7. Enable Management Access.
- 8. Click Save.

#### Figure 45 Configure: Network > PPPoE parameters

| VLAN | Routes  | Ethernet Ports | Security                     | DHCP        | Tunnel        | PPPoE                                   | VLAN Pool   |                   |  |  |
|------|---|----------------|------------------------------|-------------|---------------|---|---|-------------------|--|--|
|      |   |                |                              |             |               |   |   |                   |  |  |
|      |   | Enable         |                              |             |               |   |   |                   |  |  |
|      | VLAN  |                |                              |             |               | Vlan ID assigned to PPPoE               |   |                   |  |  |
|      | Service Name  |                |                              |             |               | Configure pppoe service-name parameters |   |                   |  |  |
|      | Authentication Info   |                | admin                        |             |               | •••••                                   |   | Max 64 characters |  |  |
|      | MTU   |                |                              | 1430        |               |   | Configure mtu for pppoe connection (500-1492 bytes) |                   |  |  |
|      | TCP   | -MSS Clamping  | <ul> <li>Enable t</li> </ul> | cp mss clam | ping for pppo | e connection                            |   |                   |  |  |
|      | Management Access Enable CLI/GUI/SNMP access via this interface |                |                              |             |               |   |   |                   |  |  |
|      | Save  |                |                              |             |               |   |   |                   |  |  |

# VLAN Pool

#### Table 44 Configure: Network > VLAN Pool parameters

| Parameters        | Description   | Range | Default |
|-------------------|---|-------|---------|
| VLAN Pool<br>Name | Provision to configure user friendly name to a list of VLANs.   | _     | _       |
| VLAN ID List      | List of VLAN IDs for each VLAN Pool name. User can<br>configure either single VLAN ID or multiple VLAN ID.<br>Multiple VLAN IDs can be configured either separated by<br>comma or hyphen. | _     | -       |

To configure the above parameter, navigate to the **Configure > Network > VLAN Pool** tab and provide the details as given below:

- 1. Enter the name of the VLAN pool in the **VLAN Pool Name** textbox.
- 2. Enter the VLAN ID in the **VLAN ID List** textbox.
- 3. Click Save.

| VLAN | Routes       | Ethernet Ports | Security | DHCP   | Tunnel     | PPPoE        | VLAN    | Pool   |
|------|--------------|----------------|----------|--------|------------|--------------|---------|--------|
|      | V            | LAN Pool Name  |          |        |            | Vlan Pool Na | me      |        |
|      | VLAN ID List |                |          |        |            | 1-4094       |         |        |
|      |              |                | VLAN Poo | l Name | ~ V        | LAN ID List  | ~       | A      |
|      |              |                |          |        |            |              |         |        |
|      |              |                |          | No     | o list a   | vailable     | 9       |        |
|      |              |                |          |        |            |              |         |        |
|      |              |                |          |        |            |              |         |        |
|      |              |                |          |        |            |              |         |        |
|      |              |                |          |        |            |              |         |        |
|      |              |                |          | 4      | <u>/</u> 1 | ▶ 10         | ▼ items | per pa |
|      |              |                |          |        | Save       | Cancel       |         |        |

## Figure 46 Configure: Network > VLAN Pool parameters

# WWAN



Note

This feature is supported in cnPilot e600 platform only.

## Table 45 Configure: Network > WWAN

| Parameters     | Description   | Range                 | Default |
|----------------|---|-----------------------|---------|
| WWAN           | Provision to enable wireless WAN using a USB cellular dongle for internet access.   | -                     | _       |
| Failover Only  | <ul> <li>Failover only can be configured in two modes:</li> <li>Checked: <ul> <li>Ethernet will be the primary connection and</li> <li>WWAN will be backup.</li> </ul> </li> <li>Unchecked. <ul> <li>3G/4G (WWAN) will be the only working connection.</li> </ul> </li> <li>Note: Cellular link can be configured as backup only to Ethernet connection.</li> </ul> | Checked/<br>Unchecked | _       |
| APN            | Provision to configure network provider APN address.  | -                     | -       |
| Authentication | Provision to configure credentials required for WWAN authentication.  | _                     | _       |
| Monitor Host   | Running a check in the background that constantly<br>monitors a user configured IP address (Ex: 8.8.8.8) for<br>reachability through ping.  | IPv4 address          | _       |

To configure the above parameter, navigate to the **Configure > Network > WWAN** tab and provide the details as given below:

- 1. Enable **WWAN** checkbox to enable this functionality.
- 2. Check/Uncheck Failover Only to enable/disable.
- 3. Enter the APN address in the textbox.
- 4. Enter the authentication credentials.
- 5. Enter any IPv4 address to monitor.
- 6. Click Save.

| VLAN  | Routes | Ethernet Ports | Security             | DHCP | Tunnel | PPPoE   | VLAN Pool | WWAN                                   |  |
|---|--------|----------------|----------------------|------|--------|---|-----------|--|--|
|   |        | WWAN           | 🗌 Enable Wi          |      |        |   | f         |  |  |
| WWAN       Enable Wireless WAN using a USB cellular dongle for Internet access         Failover Only       Use WWAN as backhaul only when failover is triggered |        |                |                      |      |        |   |           |  |  |
| APN Configure network provider APN address  |        |                |                      |      |        |   |           |  |  |
| Authentication  |        | Authentication | username max 32 char |      | ar     | pubbword max oz onar                              |           | Configure authentication<br>parameters |  |
| Monitor Host  |        |                |                      |      | Н      | Host to monitor in order to trigger WWAN failover |           |  |  |

## Figure 47 Configure: Network > WWAN parameters

# Chapter 10: Configuration - Services

This chapter describes the following topics:

- Overview
- Configuring Services

## Overview

This chapter gives an overview of cnPilot configurable parameters related to LDAP, NAT Logging, Location API, Speed Test and DHCP Option 82.

# Configuring Services

This section provides information on how to configure the following services on cnPilot AP.

- LDAP
- NAT Logging
- Location API
- Speed Test
- DHCP Option 82

# LDAP

Table 40 lists the fields that are displayed in the Configuration > Services > LDAP tab:

Table 46 Configure: Services > LDAP parameters

| Parameters  | Description  | Range | Default |
|-------------|--|-------|---------|
| Server Host | Provision to configure IP/Hostname of LDAP server.           | _     | -       |
| Server Port | Provision to configure custom port number for LDAP services. | -     | -       |

To configure the above parameter, navigate to the **Configure > Services > LDAP** tab and provide the details as given below:

- 1. Enter the IP address of the LDAP server in the **Server Host** textbox.
- 2. Enter the Port address of the LDAP server in the **Server Port** textbox.
- 3. Click Save.

## Figure 48 Configure: Services > LDAP parameters

| LDAP |             | <br>                               |
|------|-------------|------------------------------------|
|      | Server Host | Configure LDAP server IP address   |
|      | Server Port | Configure LDAP server port address |
|      |             |                                    |

# **APIs**

cnPilot devices does support APIs w.r.t to Wi-Fi client presence, NAT information and BT client presence.

# NAT Logging

NAT logging is same as the internet access log that is generated when NAT is enabled on AP. Each internet access log PDU consists of one or more internet access log data in TLV format. The packet format for the internet access log PDU is defined as below:

## Table 47 PDU type code: 0x82

| Туре | Mandatory | Length   | Default Value                                     |
|------|-----------|----------|---|
| 0x01 | N         | 32 Bytes | Includes IPv4 internet access log data structure. |

Type 0x01 TLV includes the internet access log data structure as below:

#### Table 48 NAT Logging Packet Structure

| Length  | Description  |  |
|---------|--|--|
| 4 Bytes | NAT records UNIX time stamp which generates time in seconds from 1970-01-01 (00:00:00 GMT until now).        |  |
| 6 Bytes | The MAC address of the client.   |  |
| 1 Bytes | Reserved for future use.   |  |
| 1 Bytes | <ul> <li>The protocol type. The supported protocol types are:</li> <li>0x06 TCP</li> <li>0x11 UDP</li> </ul> |  |
| 2 Bytes | The VLAN ID where the client is connected. If there is no VLAN ID, the value will be 0.                      |  |
| 4 Bytes | The client internal or the private IP address.   |  |
| 2 Bytes | The internal port of the client.   |  |
| 4 Bytes | The Internet IP address which is translated by NAT.  |  |
| 2 Bytes | The Internet port which is translated by NAT.  |  |

| Length  | Description                             |
|---------|---|
| 4 Bytes | The IP address of the visited server.   |
| 2 Bytes | The port address of the visited server. |

Table 43 lists the fields that are displayed in Configuration > Services > NAT Logging tab:

#### Table 49 Configure: Services > NAT Logging parameters

| Parameters  | Description   | Range  | Default |
|-------------|---|--------|---------|
| Enable      | Provision to enable/disable NAT logging services.                   | _      | _       |
| Server IP   | Provision to configure IP/Hostname of NAT logging server.           | _      | _       |
| Server Port | Provision to configure custom port number for NAT Logging services. | _      | _       |
| Interval    | Provision to configure frequency of logging.                        | 5-3600 | -       |

To configure the above parameter, navigate to the **Configure > Services > NAT Logging** tab and provide the details as given below:

- 1. Select the **Enable** checkbox to enable NAT Logging.
- 2. Enter the IP address of the server for NAT Logging in the Server IP textbox.
- 3. Enter the IP address of the server port for NAT Logging in the **Server Port** textbox.
- 4. Enter the interval for NAT Logging in the **Interval** textbox.
- 5. Click Save.

#### Figure 49 Configure: Services > NAT Logging parameters

| NAT Logging |   |   |
|-------------|---|---|
| Enable      | 0 |   |
| Server IP   |   | Configure NAT Logging server IP address         |
| Server Port |   | Configure NAT Logging server port address       |
| Interval    |   | Configure NAT Logging interval (5-3600) seconds |
|             |   |   |

## Location API

Location API is a method to send the discovered (Probed) clients list to a specified server address. The reports are sent as HTTP Post to the HTTP server every interval. The discovered client entries are deleted from the list if the entry is aged out. The client aging timeout is 2 times of location API interval configured. If there are no new probe requests from the client within 2xlocation API interval time, then the client entry will be removed from the list.

Table 44 lists the fields that are displayed in Configuration > Services > Location API tab:

| Parameters           | Description   | Range   | Default |
|----------------------|---|---------|---------|
| Enable               | Provision to enable/disable Location API services.                                    | -       | -       |
| Server               | Provision to configure HTTP/HTTPs server to send report with the pot number.          | 0-65535 | _       |
| Interval             | Provision to configure custom frequency of information to be shared to server.        | 2-3600  | _       |
| MAC<br>Anonymization | Provision to detect fake clients and avoid populating it in Location API client list. | _       | _       |

| Table 50 Configure: Services > Location API paran |
|---|
|---|

To configure the above parameter, navigate to the **Configure > Services > Location API** tab and provide the details as given below:

- 1. Select the **Enable** checkbox to enable Location API.
- 2. Enter the HTTP/HTTPs server and port number in the **Server** textbox.
- 3. Enter the interval for Location API in the Interval textbox.
- 4. Enable MAC Anonymization checkbox.
- 5. Click Save.

#### Figure 50 Configure: Services > Location API parameters

| — Location API —  |                                      |  |
|-------------------|--------------------------------------|--|
| Loouton / T       |                                      |  |
| Enable            |                                      |  |
| Server            | Eg: http:// <domain>.com:80</domain> | Configure HTTP/HTTPS server with the port number (0-65535) |
| Interval          |                                      | Configure Location API interval (2-3600) seconds           |
| MAC Anonymization | Ignore Anonymized MACs ()            |  |
|                   |                                      |  |



## Note

For further details about this feature and sample reference output, go to <u>https://support.cambiumnetworks.com/files/cnpilot-tech-ref/</u> and download Wireless client Presence and Locationing API document.

# BT Location API

## **Bluetooth Scanning**

cnPilot Aps with an integrated Bluetooth Low Energy (BLE) radio can detect and locate nearby Bluetooth Low Energy devices. This data is then provided via API to third-party applications. Examples of such devices include smartwatches, battery-based beacons, Apple iBeacons, fitness monitors, and remote sensors.

Organization can create use cases for indoor wayfinding and mapping, asset tracking, and more.

Below table lists the fields that are required for configuring BT Location API.

| Parameters                       | Description  | Range  | Default |
|----------------------------------|--|--------|---------|
| Location-bt-api<br>server        | Provision to configure details of destined API server.   | -      | -       |
| Location-bt-api<br>interval      | Provision to configure the interval at which the BT information is updated to destined API server. | 2-3600 | 2       |
| Ignore-<br>anonymized-bt-<br>mac | Ignore client BT addresses that are anonymized.  | -      | -       |

## Table 51 Configuring BT Location API parameters

## Sending Report

After enabling BLE Scanning on AP it will start processing:

- 1. Convert the scanned data to a JSON array
- 2. Send that data in one single HTTP/HTTPS POST

## In the CLI

To configuring the BT Location-API:

| E500-BB164C(config | )# location-bt-api   |
|--------------------|--|
| ignore-anonymize   | d-bt-mac : Ignore MAC addresses that are anonymized        |
| interval           | : Configure reporting interval in secs                     |
| server             | : HTTP/HTTPS server to send report to with the port number |

#### To disable the BT Location-API:

E500-BB164C(config)# no location-bt-api

## BT Location API data elements

| Table 52 | ΒТ | Location | API | data | elements |
|----------|----|----------|-----|------|----------|
|          |    |          |     |      |          |

| Parameters  | Description                                     |
|-------------|---|
| арМас       | MAC address of the observing AP.                |
| API Version | API Version applied for particular data format. |
| AP Name     | Host name of the observing AP.                  |
| Timestamp   | Observation time in seconds seen by AP.         |
| BT MAC      | BLE device MAC seen by AP.                      |
| UUID        | BLE device UUID seen by AP.                     |
| RSSI        | BLE device RSSI as seen by AP.                  |

## HTTP POST Body Format:

u'ap\_mac': '00-04-56-A5-5A-EC',

```
{
```

}

{

```
'version': '2.2',
 'ap_name': 'E600-A55AEC',
 'ble discoverd clients':{Array of 0-250 devices}
Bluetooth API Data Format
bt rssi': u' -80 dBm ',
bt_mac': 14-8F-21-FD-37-18', u
'bt_uuids': Garmin International, Inc. (Oxfe1f)\n',
```

'bt\_timestamp': u' 1.811127'

}

# Speed Test

Wifiperf is a speed test service available on cnPilot devices. This tool is interoperable with open source zapwireless tool (https://code.google.com/archive/p/zapwireless/)

The wifiperf speed test can be triggered by using zapwireless tool between two cnPilot Aps or between cnPilot AP and with other third-party devices (or PC) that is having zapwireless endpoint running.

Refer https://code.google.com/archive/p/zapwireless/ to download the zapwireless tool to generate zapwireless endpoint for third party device (or PC) and zap CLI to perform the test.

In this case, wifiperf endpoint should be enabled in cnPillot AP through UI shown below.

Table 45 lists the fields that are displayed in the Configuration > Services > Speed Test tab:

#### Table 53 Configure: Services > Speed Test parameters

| Parameters | Description                                 | Range | Default  |
|------------|---|-------|----------|
| wifiperf   | Provision to enable wifiperf functionality. | _     | Disabled |

To configure the above parameter, navigate to the **Configure > Services > Speed Test** tab. Select **Wifiperf** checkbox to enable this functionality.

| - Speed Test |                             |
|--------------|-----------------------------|
| Wi-Fiperf    | Enable Wi-Fiperf Endpoint 🚯 |

# **DHCP Option 82**

Global parameter to configure DHCP Option 82 parameters that will be appended to DHCP packets when a device is connected either from wireless or wired to a cnPilot device. This parameter is given first precedence and overwrites any configuration defined in VLAN or WLAN profiles.

Table 46 lists the fields that are displayed in the Configuration > Services > DHCP Option 82 tab:

| Table 54 Configure | : Services > DHCP | Option 82 parameters |
|--------------------|-------------------|----------------------|
|--------------------|-------------------|----------------------|

| Parameters              | Parameters Description  |   |      |  |  |
|-------------------------|---|---|------|--|--|
| Enable                  | Provision to enable/disable DHCP Option 82 as global services.  | _ | -    |  |  |
| Option 82<br>Circuit ID | <ul> <li>When enabled, DHCP packets generated from wireless stations that are associated to APs are appended with Option 82 parameters. Option 82 provides provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID:</li> <li>None</li> <li>All</li> <li>Hostname</li> <li>APMAC</li> <li>SSID</li> <li>VLAN ID</li> <li>SITEID</li> </ul> | _ | None |  |  |
|                         | • Custom  |   |      |  |  |

| Parameters             | Description  | Range  | Default |
|------------------------|--|--------|---------|
| Option 82<br>Remote ID | <ul> <li>When enabled, DHCP packets generated from wireless stations that are associated to APs are appended with Option 82 parameters. Option 82 provides provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID:</li> <li>None</li> </ul> | _      | None    |
|                        | Hostname   |        |         |
|                        | • APMAC  |        |         |
|                        | • SSID   |        |         |
|                        | VLAN ID  |        |         |
|                        | • SITEID   |        |         |
|                        | • Custom   |        |         |
|                        | • All  |        |         |
| VLAN ID                | User can configure VLAN IDs where DHCP Option 82 must be enabled.  | 1-4094 | _       |

To configure the above parameter, navigate to the **Configure > Services** tab and select **DHCP Option 82** tab and provide the details as given below:

- 1. Select the **Enable** checkbox to enable DHCP Option 82.
- 2. Select **Option 82 Circuit ID** to enable DHCP Option-82 circuit ID information from the drop-down list.
- 3. Select **Option 82 Remote ID** to enable DHCP Option-82 remote ID information from the dropdown list.
- 4. Enter **VLAN ID** parameter to configure VLAN to have DHCP Option 82.
- 5. Click Save.

#### Figure 52 Configure: Services > DHCP Option 82 parameters

| Option 82 Circuit ID     None     Insert DHCP option 82 circuitID information       Option 82 Remote ID     None     Insert DHCP option-82 remoteID information       VLAN ID     Configure vlan to have DHCP Option-82 (1-4094) | Enable               | Insert DHCP Option 82 for all wireless a | nd guest enabled wired clients                 |
|--|----------------------|--|--|
| information  | Option 82 Circuit ID | None •                                   |  |
| VLAN ID Configure vlan to have DHCP Option-82 (1-4094)   | Option 82 Remote ID  | None •                                   |  |
|  | VLAN ID              |  | Configure vlan to have DHCP Option-82 (1-4094) |

# Chapter 11: Operations

This chapter describes the following topics:

- Overview
- Firmware update
- System
- Configuration

## Overview

This chapter gives an overview of cnPilot administrative functionalities such as Firmware update, System and Configuration.

## Firmware update

The running software on the cnPilot Enterprise AP can be upgraded to newer firmware. When upgrading from the UI the user can upload the firmware file from the browser. The same process can be followed to downgrade the AP to a previous firmware version if required. Configuration is maintained across the firmware upgrade process.



Note Once a firmware upgrade has been initiated, the AP should not be rebooted or power cycled until the process completes, as this might leave the AP inoperable.

 Table 47 lists the fields that are displayed in the Operations > Firmware update tab:

| Parameters          | Description  | Range | Default |
|---------------------|--|-------|---------|
| Choose File         | Provisions to select upgrade file.                   | _     | _       |
| Upgrade<br>Firmware | Provision to initiate upgrade once file is selected. | _     | _       |

**Table 55** Configure: Operations > Firmware update parameters

To configure the above parameter, navigate to **Operations > Firmware update** tab and provide the details as given below:

- 1. Click **Choose File** and select the downloaded image file to upgrade the firmware manually.
- 2. Click **Upgrade Firmware** and select the downloaded image file to upgrade the firmware automatically.

You can view the status of upgrade in the **Upgrade Status** field.

Firmware update
Choose File No file chosen
Upgrade Firmware
Upgrade Status :

Figure 53 Configure: Operations > Firmware update parameters

# System

This section provides multiple troubleshooting tools provided by cnPilot Enterprises.

Table 56 lists the fields that are displayed in the **Operations > System** tab:

 Table 56 Configure: Operations > System parameters

| Parameters   | Description  | Range | Default |
|--|--|-------|---------|
| Reboot   | User will be prompted with Reboot pop-up requesting for reboot. If Yes, device will go for reboot.   | _     | -       |
| Download<br>Tech Support   | User will be prompted with permission to download tech-<br>support from AP. If yes, file will be saved in your default<br>download path configured on your system. | -     | -       |
| Disconnect All<br>Clients  | All clients connected to both the radios will be<br>terminated by sending de-authentication packet to each<br>client connected to radios.                          | -     | -       |
| Flash LEDs on the device will toggle for configured time period. |  | 1-120 | 10      |
| Factory<br>Default   | A pop-up window appears requesting confirmation for factory defaults. If yes, device will delete all configuration to factory reset and reboots.                   | -     | -       |

To configure the above parameter, navigate to **Operations > System** tab and provide the details as given below:

- 1. Click **Reboot** for rebooting the device.
- 2. Click **Download Tech Support** to generate a techsupport from the device and save it locally.
- 3. Click Disconnect All Clients to disconnect all wireless clients.
- 4. Select **Flash LEDs** value from the drop-down list to flash LEDs for the given duration of time.
- 5. Click Factory Default to delete all configuration on the device.

# System Reboot Download Tech Support Disconnect All Clients Flash LEDs 10 Flash LED (1-120) seconds Factory Default Factory Default

## Figure 54 Configure: Operations > System parameters

# Configuration

The device configuration can either be exported from the device as a text file or imported into the device from a previous backup. Ensure that when a configuration file is imported onto the device, a reboot is necessary to activate that new configuration.

Table 57 lists the fields that are displayed in the **Operations > Configuration** tab:

Table 57 Configure: Operations > Configuration parameters

| Parameters | Description  | Range | Default |
|------------|--|-------|---------|
| Export     | Provision to export configuration of device to default download path configured on system. | _     | -       |
| Import     | Provision to import configuration of device.   | _     | _       |

To configure the above parameter, navigate to **Operations > Configuration** tab and provide the details as given below:

- 1. Click **Export** to export device configuration and save locally to the device.
- 2. Click **Import** to import device configuration to the device.

#### Figure 55 Configure: Operations > Configuration parameters

| _ ( | Configura | ation — | <br> | <br> |
|-----|-----------|---------|------|------|
|     | Export    | Import  |      |      |
|     |           |         |      |      |

# Chapter 12: Troubleshoot

This section provides detailed information about troubleshooting methods supported by cnPilot enterprise devices. Troubleshooting methods supported by cnPilot devices are categorized as below:

- Logging
  - o Events
  - o Debug Logs
- RF
  - Wi-Fi Analyzer
  - Spectrum Analyzer
  - o Unconnected Clients
- Packet Capture
- Performance
  - o Wi-Fi Perf Speed Test
  - o Connectivity

# Logging

cnPilot devices supports multi-level logging, which will ease to debug issues.

## Events

cnPilot devices generates events that are necessary for troubleshooting across various modules. Below is the list of modules, cnPilot device generates events for troubleshooting.

- Wireless station
  - Connectivity
- Configuration updates
- LDAP
  - o Authentication
- RADIUS
  - o Authentication
  - o Accounting
  - o CoA
- Mesh
- Roaming
  - Enhanced roaming
- Auto-RF
  - o Channel change
- Tunnel state

- Reboot
- Guest Access
- Autopilot

Events are available at **Troubleshoot > Logs > Events**.

Figure 56 Troubleshoot > Logs > Events

|                      | Troubleshoot / Logs |                              |                              |  |                        |
|----------------------|---------------------|------------------------------|------------------------------|--|------------------------|
| Dashboard            |                     |                              |                              |  |                        |
| a Monitor 🗸          | Events Debug Logs   |                              |                              |  |                        |
| Configure -          |                     |                              |                              | -  | Refresh                |
|                      | Date                | <ul> <li>Severity</li> </ul> | <ul> <li>Mnemonic</li> </ul> | <ul> <li>Message</li> <li>Filter:</li> </ul>   | ~                      |
| Operations           | Apr 23 07:47:12     | Notice                       | NETWORK-RENEW-INTERFACE-IP   | Renewed the interface IP on ethernet link [eth0] status move to up and running state |                        |
|                      | Apr 23 07:47:02     | Notice                       | SYSTEM-CONFIG-APPLIED        | System configuration change applied  |                        |
| F Troubleshoot       | Apr 23 07:45:50     | Notice                       | NETWORK-RENEW-INTERFACE-IP   | Renewed the interface IP on ethernet link [eth0] status move to up and running state |                        |
| WiFi Analyzer        | Apr 23 07:45:40     | Notice                       | SYSTEM-CONFIG-APPLIED        | System configuration change applied  |                        |
| a wiri Analyzer      | Apr 23 07:45:40     | Notice                       | NETWORK-RENEW-INTERFACE-IP   | Renewed the interface IP on ethernet link [eth0] status move to up and running state |                        |
| M Spectrum Analyzer  | Apr 23 07:45:28     | Notice                       | SYSTEM-CONFIG-APPLIED        | System configuration change applied  |                        |
|                      | Apr 23 07:44:43     | Notice                       | NETWORK-RENEW-INTERFACE-IP   | Renewed the interface IP on ethernet link [eth0] status move to up and running state |                        |
| WiFi Perf Speed Test | Apr 23 07:44:32     | Notice                       | SYSTEM-CONFIG-APPLIED        | System configuration change applied  |                        |
| Connectivity         | Anr 23 07:44:19     | Notice                       | SYSTEM-CONFIG-APPLIED        | System configuration change applied  | ·                      |
|                      | 1 ; 16 of 16 items  |                              |                              |  | ▶1 25 ▼ items per page |
| II Packet Capture    |                     |                              |                              |  |                        |
| I Logs               |                     |                              |                              |  |                        |

## Debug Logs

cnPilot provisions enhanced debugging of each module as events generated by system and scope of debugging is limited. Debug logs can be triggered when user click **Start Logs** and can be terminated when clicked on **Stop Logs**. By default, debug logs auto terminate after 1 minute when clicked on **Start Logs**.

Debug logs are available at **Troubleshoot > Logs > Debug Logs**.

#### Figure 57 Troubleshoot > Logs > Debug Logs

| Cambium Networks      | xiPilot E400 - E400-AFA308  | C Reboot | 🕞 Logou |
|-----------------------|---|----------|---------|
| M Dashboard           | Troubleshoot / Logs   |          |         |
| 🕰 Monitor 👻           | Events Debug Logn   |          |         |
| Configure •           | Step Logs   |          |         |
| Operations            | Logs<br>Apr 24 07-89:35: wild : dynamic-power (00), current power (-1110) (cache.c=2655)<br>Apr 24 07-89:35: wild : Meighbor stor (0) 00-04-56-F3-33 Zor sai (00) [ast-active 4 (cache.c=2667)<br>2015-04-24 07-93:55 S25 common.c3Mftr. Hills: Received LLD peacht   |          | Î       |
| F Troubleshoot -      | 2019.04.28 07:45:05 592 commons.c176/LIDP: CC E1:T-6 47E:00<br>2019.04.28 07:45:37 592 device agents.c371:dia_allws_ch<br>Apr 24:07:69:45:wildi anothy may type CMB_MOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c2735)  |          |         |
| al WiFi Analyzer      | Apr 24 07:64:54: will i: Existing neighbor 10.44:56:F3:32:32 bas 00.04:56:F8:34:0000.04:56:F8:39:80 power 15/18 rssi 00 #clients 0/1<br>Apr 24 07:69:50: will id: error ucing neighbor indi (main.c:1424)<br>201504:24:07:69:55: 55:04:0-agent.c:55:28:PMIS DATA: lene=28:msg [PPId]: "592", "PULoss": "0"]   |          |         |
| M Spectrum Analyzer   | Apr 24 07:45:39. wild: dynamic power (100), current power (-1118) (cachac-28:55)<br>2019-04:24 07:52:38 29:00.cac2019:tatt  |          |         |
| WiFi Perf Speed Test  | Apr 24 07:64:52, wild: Heighbor stol (0) 00.04:55F.03.13.67 ensi (00) last.active 4 (cache.c:2667)<br>2019:04:24 07:69:50 552 will:c:1208:500 fcgi request 0<br>2019:04:24 07:69:59 S2 will:c:1208:500 fcgi request 0   |          |         |
| Connectivity          | 2019 04 24 07:49:50 592 will.cr1208:Got log1 regunst 0<br>Apr 24 07:49:59: scmd : Exec recv complete closing 31 (actions.cr37)  |          |         |
| Packet Capture        | Apr 24 07:59:00: wild : notify mag type CMB, MOTEY, MSG, TVPE, MEIGH, Apr 2, DATA[21] neosherd (tachts::2735)<br>Apr 24 07:59:00: wild : Existing mightor 00-45:67-83-32 60 bas 00-45:67-83-34 000-04:56:78-33-80 power 15/18 rssi 00 #clients 0/1<br>201504/24 07:59:04 532 common:::MTrs:: Idle: Received LLDP packet   |          |         |
| 📾 Logs                | 2019-04-24 97:56:04 552 common.cs/876:LLDP: CC_E1-7F-84-7E-00<br>Apr 24 07:59:05 wild1: errortx'ing neighbor info (main:cs/84)  |          |         |
| % Unconnected Clients | 2015.04.24 07:52.25 552 Up.2.2073.tatt, cms, logging. Send bg history (10 lines)<br>Apr 24 07:50:05; wild: 5-heghtors: content power (1716) (coche2555)<br>Apr 24 07:50:05; wild: 5-heghtors: adv 00,00.45:4F-83.32 for sil (00) last active 4 (cache2667)<br>2015.04.24 07:50:05 52:04; wild: statts timer at 155500B54 (lasts202)<br>Apr 24 07:55:05; wild: and the statts timer at 155500B54 (lasts202)<br>Apr 24 07:55:05; wild: and the statts timer at 155500B54 (lasts202)<br>Apr 24 07:55:05; wild: a control time type Color Direct Proc. PRICE, AP_DATA[21] received (cache2735)<br>Apr 24 07:55:05; wild: a control time type to 00:45:06; Ap.25; bas 00:04:05:4F-83:4:0000-04:56:F-83:4:000; out 56:F-83:4:00; out 56:F-8 |          | ÷       |

# Radio Frequency

## Wi-Fi Analyzer

This tool provisions customer to scan the channels supported as per regulatory domain and provides information related to AP's presence in each channel. Wi-Fi analyzer graphs are available in two modes:

• Interference

This tool shares more information of each channel as below:

- o Noise
- Interference measured in RSSI
- List of top 64 neighbor APs
- Number of APs

This tool shares more information of each channel as below:

- o Noise
- Number of neighbor APs
- List of top 64 neighbor APs

Channel analyzer is available at **Troubleshoot > Wi-Fi Analyzer > Interference Mode**.



Figure 58 Troubleshoot > Wi-Fi Analyzer > Interference Mode

Channel analyzer is available at Troubleshoot > Wi-Fi Analyzer > Number of APs Mode:





## Spectrum analyzer

Due to heavy commercialization of Wi-Fi devices and wide range of non-Wi-Fi devices operating in the ISM band, interference in the ISM bands is unavoidable and imminent. The Wi-Fi performance can quickly degrade with the presence of these wide range of devices in the vicinity. The Wi-Fi network deployment is in need of more robust tools for RF spectrum analysis for determining potential Wi-Fi (and non-Wi-Fi) interferers for efficient planning of the network deployment.

Given the wide range deployment of high capacity Wi-Fi networks, it is inevitable that the devices come ready with automatic interference detection and mitigation. The spectral scan feature on cnPilot is the first step towards achieving the same.

Spectral analyzer is triggered on demand. Following options are required to trigger spectrum analyzer:

• Band

This feature is available on both 2.4GHz and 5GHz. At an instance, any one band can be selected

• Continuous scan

If user is looking for continuous scan until stopped, this field has to be enabled.

• Scanning

Option to start and stop the scan process.

Spectrum analyzer is available at **Troubleshoot > Spectrum Analyzer**.

| Cambium Networks       | cnPilot E400 - E400-AFA308   | 🖒 Reboot | G Logout |
|------------------------|--|----------|----------|
| Lul Dashboard          | Troubleshoot / Spectrum Analyzer   |          |          |
| 🚳 Monitor 👻            | Band © 2.4GHz 🔹 5GHz   |          |          |
| Configure -            | Continuous Scan<br>Scanning Start  |          |          |
|                        |  |          |          |
| F Troubleshoot -       |  |          |          |
| Il WiFi Analyzer       | 33   |          |          |
| Lat. Spectrum Analyzer |  |          |          |
| WiFi Perf Speed Test   |  |          |          |
| C Connectivity         |  |          |          |
| E Packet Capture       | 3180 5200 5220 5240 5280 5300 5320 5140 5560 5800 5400 5440 5460 5460 5500 5520 5540 5580 5600 5620 5640 5660 5680 5700 5720 5740 5780 5800 5820 5840 5860 |          |          |
| E Logs                 |  |          |          |
| 13 Unconnected Clients |  |          |          |

## Figure 60 Troubleshoot > Spectrum Analyzer

## Unconnected clients

Unconnected clients provides a list of clients that could not connect properly due to various reasons with the Aps. Currently the following failures are tracked:

- Invalid pre-shared key
- EAP authentication failure
- Denied due to MAC ACL
- Client disconnected by enhanced-roaming

## Figure 61 Unconnected clients

| Cambium Networks <sup>— C</sup> | nPilot E600 - E600-96620C         |          |                         |             |                       | C Reboot | C Logout |
|---------------------------------|-----------------------------------|----------|-------------------------|-------------|-----------------------|----------|----------|
| Lett Dashboard                  | Troubleshoot / Unconnected Client | is .     |                         |             |                       |          |          |
|                                 | MAC                               | Vendor ~ | \$SID ~                 | Last Seen 🗸 | Message               | ~        |          |
| 🚳 Monitor 👻                     | 3C-A9-F4-B1-11-44                 | Intel    | Test_NWCI_IGA_DF_VLAN_1 | 00:03:10    | Denied due to MAC ACL |          | ^        |
| & Configure -                   |                                   |          |                         |             |                       |          |          |
| 莘 Operations                    |                                   |          |                         |             |                       |          |          |
| 🗲 Troubleshoot -                |                                   |          |                         |             |                       |          |          |
| J WiFi Analyzer                 |                                   |          |                         |             |                       |          |          |
| Lat Spectrum Analyzer           |                                   |          |                         |             |                       |          |          |
| WiFi Perf Speed Test            |                                   |          |                         |             |                       |          |          |
| Connectivity                    |                                   |          |                         |             |                       |          | ÷        |
| Packet Capture                  | Refresh                           |          |                         |             |                       |          |          |
| E Logs                          |                                   |          |                         |             |                       |          |          |
| S Unconnected Clients           |                                   |          |                         |             |                       |          |          |

# Packet capture

Allows the administrator to capture all packets on a specified interface. A decode of the packet indicating the network addresses, protocol types etc is displayed. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, port number etc. The number of packets that are captured can also be capped, so the console or system is not overwhelmed. Packets captured on the ETH interfaces are packets that are being transmitted or received on the physical interface of the device.

cnPilot device allows packet capture on following interfaces:

- WLAN
- Ethernet
- VLAN
- SSID

Multiple options of filtering are provided and is available **Troubleshoot > Packet Capture page**:

| Cambium Networks      | cnPi | ilot E400 - E400-AFA308       |                          |   |  | C Reboot | 🕞 Logout |
|-----------------------|------|-------------------------------|--------------------------|---|--|----------|----------|
| Lul Dashboard         |      | Troubleshoot / Packet Capture |                          |   |  |          |          |
| 🚳 Monitor 👻           |      | Interface :                   | Ethernet                 | • | Ex : 1   |          |          |
|                       | _    | Source IP & Destination IP:   | Source IP                |   | Destination IP   |          |          |
| 🌣 Configure 👻         |      | Source MAC & Destination MAC: | Source MAC               |   | Destination MAC  |          |          |
|                       |      | Direction :                   | Both                     | ٣ |  |          |          |
| ≢ Operations          |      | Count :                       | Ex: 100                  |   |  |          |          |
| 🗲 Troubleshoot -      |      | Filter :                      | Ex : icmp[icmptype] == 8 |   | NOTE: Packet capture is aborted after 60 seconds, if the count has not reached.<br>Summary will not be available when aborted. |          |          |
| I WiFi Analyzer       |      |                               | Start Capture            |   |  |          |          |
| Le Spectrum Analyzer  |      | Packet Capture Result         |                          |   |  |          |          |
| WiFi Perf Speed Test  |      |                               |                          |   |  |          |          |
| Connectivity          |      |                               |                          |   |  |          |          |
| Packet Capture        |      |                               |                          |   |  |          |          |
| Logs                  |      |                               |                          |   |  |          |          |
| S Unconnected Clients |      |                               |                          |   |  |          |          |

#### Figure 62 Troubleshoot > Packet Capture page

# Performance

## Wi-Fi Perf speed test

The Wi-Fi Perf Speed Test feature helps to measure the bandwidth from AP to an end point. You can measure both TCP and UDP with variable payloads. To configure this feature:

- 1. Navigate to **Troubleshoot > Wi-Fi Perf Speed Test** page in the UI.
- 2. Provide the following details:
  - Select the duration from the **Duration** drop-down list.
  - Select the Protocol as UDP or TCP.
  - Enter the length of the payload in the Payload Length textbox.
  - Enter the IP of the payload length in the Wi-FiPerf Endpoint textbox.
  - Select **Downlink** or **Uplink** Radio button.

3. Click on Start Test.

| Cambium Networks       | cnPilot E400 | 0 - E400-AFA308       |                        |   |
|------------------------|--------------|-----------------------|------------------------|---|
| LIII Dashboard         | Trout        | bleshoot / Speed Test |                        |   |
| 🚯 Monitor 🗸            |              | Duration:             | 10 sec                 | ٣ |
|                        |              | Protocol:             | TCP                    | ٣ |
| 🔅 Configure 🗸          |              | Payload Length:       | optional (64 to 65505) |   |
| t On continue          |              | WiFiPerf Endpoint:    | Please select          | ٣ |
| ≢ Operations           |              | Downlink:             | •                      |   |
| 🖋 Troubleshoot 🗸       |              | Uplink:               | 0                      |   |
| Larger and some        |              |                       | Start Test             |   |
| WiFi Analyzer          | - 1          | Test Result           |                        |   |
| Lill Spectrum Analyzer |              |                       |                        |   |
| WiFi Perf Speed Test   |              |                       |                        |   |
| Connectivity           |              |                       |                        |   |
| Packet Capture         |              |                       |                        |   |
| Logs                   |              |                       |                        |   |
| S Unconnected Clients  |              |                       |                        |   |

Figure 63 Troubleshoot > Wi-Fi Perf Speed Test

## Speedtest on Access Point

Speedtest can be used to measure speed across the WAN to Cambium hosted servers. The CLI output displays uplink and downlink speed in Mbps. You can also host your own server in your data center and measure bandwidth to it using ETSI option and specifying the URL. The server software can be obtained from the LibreSpeed project <a href="https://github.com/librespeed/speedtest">https://github.com/librespeed/speedtest</a>.

#### Configuration:

Syntax:

```
cnPilot-E400-202(config)# speedtest etsi
  <server url> <download MB> <upload MB>
  cnPilot-E400-202(config)# speedtest etsi
```

Example 1:

```
cnPilot-E400-202(config)# speedtest etsi 10.110.211.19:9000 200 200
Your IP is 10.110.240.202 - private IPv4 access
Latency: 14.5ms Jitter: 1.3ms
Download: 169.53Mbps Upload: 93.93Mbps
```

Example 2:

```
E400-AE27D2(config)# speedtest
Your IP is 115.110.71.66
Test server located in Singapore, Singapore
Latency: 57.4ms Jitter: 2.0ms
Download: 26.48Mbps Upload: 26.00Mbps
```



Cambium hosted server is chosen automatically

# Connectivity

Note

## IPv4

This tool helps to check the accessibility of remote hosts from cnPilot device. Three types of tools are supported under this category:

- Ping
- DNS Lookup
- Traceroute

## Table 58 Troubleshoot: Connectivity

| Parameters                | Description  | Range   | Default   |  |  |  |
|---------------------------|--|---------|-----------|--|--|--|
| Ping                      | Ping   |         |           |  |  |  |
| IP Address or<br>Hostname | Provide IPv4 address or Hostname to validate the reachability of the destined Host.                                  | -       | -         |  |  |  |
| Number of<br>Packets      | Provide number of request packets that are required to be transmitted to validate the reachability of destined Host. | 1-10    | 3         |  |  |  |
| Buffer Size               | Configure ICMP packet size.  | 1-65507 | 56        |  |  |  |
| Ping Result               | Displays the ICMP results.   | -       | -         |  |  |  |
| DNS Lookup                |  |         |           |  |  |  |
| Host Name                 | Provide Hostname whose IPv4 must be resolved.  | -       | -         |  |  |  |
| DNS Test<br>Result        | Displays the IP's that are associated with configured Hostname.  | -       | -         |  |  |  |
| Traceroute                |  |         |           |  |  |  |
| IP Address or<br>Hostname | Provide IPv4 address or Hostname to validate the reachability of the destined Host.                                  | -       | -         |  |  |  |
| Fragmentation             | Provision to allow or deny fragment packets.   | -       | Off       |  |  |  |
| Trace Method              | Provision to configure payload mechanism to check the reachability of destined IPv4 Hostname.                        | -       | ICMP Echo |  |  |  |
| Display TTL               | Provision to customize TTL display.  | -       | On        |  |  |  |
| Verbose                   | Provision to display the output of traceroute.   | -       | On        |  |  |  |

| Parameters           | Description                                | Range | Default |
|----------------------|--|-------|---------|
| Traceroute<br>Result | Displays the output of traceroute command. | -     | -       |

To configure the above parameter, navigate to the **Troubleshoot > Connectivity** tab and provide the details as given below:

To configure **Ping**:

- 1. Select **Test type** from the drop-down list.
- 2. Enter IPv4 address or Hostname in the textbox.
- 3. Enter the **Number of packets** in the textbox.
- 4. Select **Buffer Size** value from the drop-down list.
- 5. Start Ping.

To configure **DNS Lookup:** 

- 1. Enter the **Hostname** in the textbox.
- 2. Click DNS Test.

To configure **Traceroute**:

- 1. Enter IPv4 address or Hostname in the textbox.
- 2. Click Fragmentation to ON/Off.
- 3. Select Trace Method to either ICMP Echo/UDP.
- 4. Click **Display TTL** to **ON/Off.**
- 5. Click Verbose to ON/Off.
- 6. Click Start Traceroute.

| Test Type :   | Ping  | ¥                    |  |
|---|---|----------------------|--|
| IP Address or Hostname :  | www.google.com  |                      |  |
| Number of Packets :   | 3   | Min = 1, Max = 10    |  |
| Buffer Size :   | 56  | Min = 1, Max = 65507 |  |
| Ping Result<br>PING www.google.com (216.5<br>64 bytes from 216.58.197.68: s<br>64 bytes from 216.58.197.68: s<br>64 bytes from 216.58.197.68: s | eq=0 ttl=56 time=7.428 ms<br>seq=1 ttl=56 time=7.131 ms |                      |  |

| Figure 64 Troubleshoot > Connectivity > Pin | ng |
|---|----|
|---|----|



| ubleshoot / Connectivity |  |  |  |  |
|--------------------------|--|--|--|--|
| Test Type :              | DNS Lookup 🔻   |  |  |  |
| Host Name:               | www.google.com DNS Test  |  |  |  |
| DNS Test Result          |  |  |  |  |
| Name:www.google.com Addr | ess:2404:6800:4007:800::2004 Name:www.google.com Address:216.58.197.68 |  |  |  |
|                          |  |  |  |  |
|                          |  |  |  |  |
|                          |  |  |  |  |

| Test Type :  | Traceroute  |
|--|---|
| IP Address or Hostname :   | 8.8.8.8   |
| Fragmentation :  | ⊛ Off ⊜ On  |
| Trace Method :   | ICMP Echo      UDP  |
| Display TTL :  | ⊙ Off ⊛ On  |
| Verbose :  | ⊙ Off ⊛ On  |
|  | Stop Traceroute   |
|  |   |
| Traceroute Result  |   |
|  | 30 hone may 32 huta nackate   |
| traceroute to 8.8.8.8 (8.8.8.8),   | , 30 hops max, 38 byte packets<br>2541 3.128 ms (255) 5.707 ms (255) 4.423 ms (255) |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 * * *   | , 30 hops max, 38 byte packets<br>254) 3.128 ms (255) 5.707 ms (255) 4.423 ms (255) |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.  |   |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 ***<br>3 ***<br>4 ***                                     |   |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 * * *<br>3 * * *<br>4 * * *<br>5 * * *                    |   |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 ***<br>3 ***<br>4 ***<br>5 ***<br>6 ***                   |   |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 ***<br>3 ***<br>4 ***<br>5 ***<br>6 ***<br>7 ***          |   |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 ***<br>3 ***<br>4 ***<br>5 ***<br>6 ***<br>7 ***<br>8 *** |   |
| traceroute to 8.8.8.8 (8.8.8.8),<br>1 10.110.219.254 (10.110.219.<br>2 ***<br>3 ***<br>4 ***<br>5 ***<br>6 ***<br>7 ***          |   |

Figure 66 Troubleshoot: Connectivity > Traceroute

## IPv6

This tool helps to check the accessibility of remote hosts from cnPilot device. Three types of tools are supported under this category:

- Ping6
- DNS Lookup6
- Traceroute6

Table 59 Troubleshoot: Connectivity

| Parameters                | Description  | Range   | Default |
|---------------------------|--|---------|---------|
| Ping                      |  | L       |         |
| IP Address or<br>Hostname | Provide IPv6 address or Hostname to validate the reachability of the destined Host.                                  | -       | -       |
| Number of<br>Packets      | Provide number of request packets that are required to be transmitted to validate the reachability of destined Host. | 1-10    | 3       |
| Buffer Size               | Configure ICMP packet size.  | 1-65507 | 56      |
| Ping Result               | Displays the ICMP results.   | -       | -       |
| DNS Lookup                |  |         |         |

| Parameters                | Description   | Range                       | Default   |
|---------------------------|---|-----------------------------|-----------|
| Host Name                 | Provide Hostname whose IPv6 must be resolved.   | -                           | -         |
| DNS Test<br>Result        | Displays the IP's that are associated with configured Hostname.                               | -                           | -         |
| Traceroute                |   |                             |           |
| IP Address or<br>Hostname | Provide IPv6 address or Hostname to validate the reachability of the destined Host.           | -                           | -         |
| Fragmentation             | n Provision to allow or deny fragment packets Of  |                             | Off       |
| Trace Method              | Provision to configure payload mechanism to check the reachability of destined IPv6/Hostname. | -                           | ICMP Echo |
| Display TTL               | Provision to customize TTL display.   | to customize TTL display On |           |
| Verbose                   | Provision to display the output of traceroute C   |                             | On        |
| Traceroute<br>Result      | Displays the output of traceroute command.  |                             |           |

To configure the above parameter, navigate to the **Troubleshoot > Connectivity** tab and provide the details as given below:

To configure Ping6:

- 6. Select **Test type** from the drop-down list.
- 7. Enter IPv6 address or Hostname in the textbox.
- 8. Enter the Number of packets in the textbox.
- 9. Select **Buffer Size** value from the drop-down list.
- 10. Start Ping6.

To configure **DNS Lookup6**:

- 3. Enter the **Hostname** in the textbox.
- 4. Click DNS Test.

To configure Traceroute6:

- 7. Enter IPv6 address or Hostname in the textbox.
- 8. Click Fragmentation to ON/Off.
- 9. Select Trace Method to either ICMP Echo/UDP.
- 10. Click Display TTL to ON/Off.
- 11. Click Verbose to ON/Off.
- 12. Click Start Traceroute.

| Test Type :   | Ping6 ~  |                      |  |
|---|--|----------------------|--|
| IPv6 Address or Hostname :  | 2018:1:2:400:6502:efa5:a978:2e8f   |                      |  |
| Number of Packets :   | 3  | Min = 1, Max = 10    |  |
| Buffer Size :   | 56   | Min = 1, Max = 65507 |  |
|   |  |                      |  |
| 64 bytes from 2018:1:2:400:65<br>64 bytes from 2018:1:2:400:65<br>64 bytes from 2018:1:2:400:65 | a978:2e8f (2018:1:2:400:6502:efa5:a978:2e8f<br>502:efa5:a978:2e8f: seq=0 ttl=63 time=0.810<br>502:efa5:a978:2e8f: seq=1 ttl=63 time=0.671<br>502:efa5:a978:2e8f: seq=2 ttl=63 time=0.644 | ns                   |  |
| PING 2018:1:2:400:6502:efa5:<br>64 bytes from 2018:1:2:400:65<br>64 bytes from 2018:1:2:400:65  | 02:efa5:a978:2e8f: seq=0 ttl=63 time=0.810<br>02:efa5:a978:2e8f: seq=1 ttl=63 time=0.611<br>02:efa5:a978:2e8f: seq=2 ttl=63 time=0.644<br>8:2e8f ping statistics                         | ns                   |  |

Figure 67 Troubleshoot > Connectivity > Ping6



| Troubleshoot / Connectivity                   |  |
|---|--|
| Test Type :                                   | DNS Lookup6  |
| Host Name:                                    | google.com DNS Test  |
| DNS Test Result<br>Name:google.com Address:24 | 04:6800:4007:80e::200e Name:google.com Address:172.217.163.142 |

| Troubleshoot / Connectivity    |   |
|--------------------------------|---|
| Toubleshool / Connectivity     |   |
| Test Type :                    | Traceroute6   |
| IPv6 Address or Hostname :     | 2018:1:2:400:6502:efa5:a978:2e8f  |
| Fragmentation :                | ● Off ○ On  |
| Trace Method :                 | ICMP Echo UDP   |
| Display TTL :                  | ⊖ Off ● On  |
| Verbose :                      | ○ Off   |
|                                | Start Traceroute  |
| 1 2018:1:2:100::1 (2018:1:2:10 | 02:efa5:a978:2e8f (2018:1:2:400:6502:efa5:a978:2e8f), 30 hops max, 64 byte packets<br>)0::1) 2.723 ms 2.531 ms 2.185 ms<br>8:2e8f (2018:1:2:400:6502:efa5:a978:2e8f) 0.409 ms 0.427 ms 0.343 ms |

## Figure 69 Troubleshoot: Connectivity > Traceroute6

# Chapter 13: Management Access

This chapter describes different methods of authenticating users to access device UI. Following are the authentication methods supported by cnPilot devices:

- Local authentication
- SSH-Key authentication
- RADIUS authentication

## Local authentication

This is the default authentication mode enabled on device. Only one username is supported which is "admin". Default password for "admin" username is "admin". User has provision to configure/update password.

## Device configuration

Figure 67 shows how to configure/update default password of admin user.

- 1. Under Management, enter Admin Password.
- 2. Click Save.

Figure 70 configure/update default password of admin user

| Cambium Networks Cr | Pilot E400 - E400-AFA308 |   |   | C Reboot | C Logout |
|---------------------|--------------------------|---|---|----------|----------|
| III Dashboard       | Configure / System       |   |   |          |          |
| 🚳 Monitor 🗸         | System                   |   |   |          |          |
|                     | Nam                      | e E400-AFA308   | Hostname of the device (max 64 characters)                    |          |          |
| 🜣 Configure 👻       | Locatio                  | 1   | Location where this device is placed (max 64 characters)      |          |          |
| 🖵 System            | Contac                   | t   | Contact information for the device (max 64 characters)        |          |          |
| + Radio             | Country-Cod              | India •   | For appropriate regulatory configuration                      |          |          |
| 🗢 WLAN              | Placemen                 |   |   |          |          |
| A Network           | LE                       |   |   |          |          |
|                     | LLD                      | Whether the AP should transmit LLDP packets             |   |          |          |
| Services            | - Management             |   |   |          |          |
| 幸 Operations        | management               |   |   |          |          |
|                     | Admin Passwor            |   | Configure password for authentication of GUI and CLI sessions |          |          |
| 🖋 Troubleshoot -    | Autopile                 | t Default •   | Autopilot Management of APs                                   |          |          |
|                     | Teine                    | t Enable Telnet access to the device CLI                |   |          |          |
|                     | SS                       | <ul> <li>Enable SSH access to the device CLI</li> </ul> |   |          |          |
|                     | SSH Ke                   | /   | Use SSH keys instead of password for authentication           |          |          |
|                     | нтт                      | Enable HTTP access to the device GUI                    |   |          |          |
|                     | HTTP Po                  | t 80  | Port No for HTTP access to the device GUI(1-65535)            |          |          |

# SSH-Key authentication

SSH keys are also used to connect remote machines securely. They are based on the SSH cryptographic network protocol, which is responsible for the encryption of the information stream between two machines. Ultimately, using SSH keys user can connect to remote devices without even entering a password and much more securely too. SSH works based on "public-key cryptography". For simplicity, let us consider that SSH keys come in pairs. There is a **private key**, that is safely stored to the home

machine of the user and a **public key**, which is stored to any remote machine (AP) the user wants to connect. So, whenever a user initiates an SSH connection with a remote machine, SSH first checks if the user has a private key that matches any of the public keys in the remote machine and if not, it prompts the user for password.

## Device configuration

SSH Key based access method can be configured on device using standalone AP or from cnMaestro. Navigate to **System > Management** and configure the following:

- 1. Enable **SSH** checkbox.
- 2. Provide Public key generated from steps described in SSH Key Generation section.

| Cambium Networks CnPi | lot E400 - E400-AFA308 |   |   | 🖒 Reboot | C Logout |
|-----------------------|------------------------|---|---|----------|----------|
| Lee Dashboard         | Configure / System     |   |   |          |          |
|                       | System                 |   |   |          |          |
| 🔁 Monitor 👻           | System                 |   |   |          |          |
| Configure -           | Name                   | E400-AFA308   | Hostname of the device (max 64 characters)                    |          |          |
|                       | Location               |   | Location where this device is placed (max 64 characters)      |          |          |
| 🖵 System              | Contact                |   | Contact information for the device (max 64 characters)        |          |          |
| 9 Radio               | Country-Code           | India 🔻   | For appropriate regulatory configuration                      |          |          |
| ♥ WLAN                | Placement              | Indoor      Outdoor Configure the AP placement details  |   |          |          |
|                       | LED                    | ✓ Whether the device LEDs should be ON during operation |   |          |          |
| A Network             | LLDP                   | Whether the AP should transmit LLDP packets             |   |          |          |
| Services              |                        |   |   |          |          |
|                       | Management             |   |   |          |          |
|                       | Admin Password         |   | Configure password for authentication of GUI and CLI sessions |          |          |
| 🖋 Troubleshoot 🗸      | Autopilot              | Default <b>v</b>  | Autopilot Management of APs                                   |          |          |
|                       | Teinet                 | Enable Teinet access to the device CLI                  |   |          |          |
|                       | SSH                    | Enable SSH access to the device CLI                     |   |          |          |
|                       | SSH Key                |   | Use SSH keys instead of password for authentication           |          |          |
|                       | нттр                   | Enable HTTP access to the device GUI                    |   |          |          |
|                       | HTTP Port              | 80  | Port No for HTTP access to the device GUI(1-65535)            |          |          |
|                       | HTTPS                  | Enable HTTPS access to the device GUI                   |   |          |          |
|                       | HTTPS Port             | 443   | Port No for HTTPS access to the device GUI(1-65535)           |          |          |

#### Figure 71 System > Management

## SSH Key Generation

#### Windows

PUTTY tool can be used to generate both Public and Private Key. Below is a sample demonstration of configuring cnPilot device and logging using SSH Key via UI.

1. Generate a key pair in PUTTY Key Generator (Figure 72) and save private and public key as shown in Figure 73.

| 🚰 PuTTY Key Generator   | ? ×              | 😴 PuTTY Key Generator   | ?                        |
|---|------------------|---|--------------------------|
| ile <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp                       |                  | <u>F</u> ile <u>K</u> ey Con <u>v</u> ersions <u>H</u> elp              |                          |
| Key<br>No key.  |                  | Key<br>Please generate some randomness by moving the mouse over         | the blank area.          |
|   |                  |   |                          |
| Actions<br>Generate a public/private key pair                           | Generate         | Actions<br>Generate a public/private key pair                           | <u>G</u> enerate         |
|   | <u>G</u> enerate |   | <u>G</u> enerate<br>Load |
| Generate a public/private key pair                                      | Load             | Generate a public/private key pair                                      | <br>Load                 |
| Generate a public/private key pair<br>Load an existing private key file | Load             | Generate a public/private key pair<br>Load an existing private key file | <br>Load                 |

2. Save the Public key and Private key once key pair is generated as shown in Figure 73.

| PuTTY             | ' Key Generat          | tor             |                |                  | ?   | >    |
|-------------------|------------------------|-----------------|----------------|------------------|---|------|
| le <u>K</u> ey    | Conversion             | ns <u>H</u> elp |                |                  |   |      |
| Key               |                        |                 |                |                  |   |      |
| Public ke         | y for pasting in       | nto Open SS     | H authorized_  | keys file:       |   |      |
| oVsxtA2<br>+gLG4C | J8d6AÓ9tICFs<br>/N2P/G | i7uMldAyD2      | ZPFzL0CYZat    | 0rM+e96XRhSF     | vjxwFbvUZeL1D2caL<br>xt&eC<br>2uQU5BOsSREsVAM |      |
| Key finge         | erprint:               | ssh-rsa 204     | 48 02:9e:02:ba | af3:9b:74:b1:5d: | dc:93:c0:d2:d2:33:0b                          |      |
| Key <u>c</u> om   | ment:                  | rsa-key-20      | 170405         |                  |   |      |
| Key p <u>a</u> ss | phrase:                |                 |                |                  |   |      |
| Confirm p         | assphrase:             |                 |                |                  |   |      |
| Actions           |                        |                 |                |                  |   |      |
| Generate          | e a public/priva       | ate key pair    |                |                  | <u>G</u> enerate                              |      |
| Load an           | existing private       | e key file      |                |                  | <u>L</u> oad                                  |      |
| Save the          | generated ke           | y               |                | Save public key  | <u>S</u> ave private k                        | ey   |
| Paramete          | ers                    |                 |                |                  |   |      |
| Type of k         | key to generat         |                 | OECDSA         | O ED255          | 519 🔿 SSH-1 (F                                | (SA) |
|                   | 0.                     | -               | _              | _                | 2048  |      |

#### Figure 73 Public and Private Key

- 3. Save the Public key generated in step above as described in **Device configuration** section.
- 4. Login to device using Private key generated above with username as "admin".

## Linux

If using a Linux PC and SSH from the Linux host, then you can generate the keys with the following steps:

1. Generate key pair executing below command on Linux console as shown in **Figure 74**.



- 2. The Public key is now located in PATH mentioned in Figure 71.
  - PATH = "Enter the file to which to save the key"
- 3. The private key (identification) is now saved in PATH as mentioned in Figure 75.
  - PATH = "Your identification has saved in <>"

#### Figure 75 Private Key saved path

| tatdell@saidell-vostro-15-3568:-\$<br>saidell@saidell-vostro-15-3568:-\$<br>ssh-rsa AAAAB3NzaCiycZEAAAADAQABAAABAQDg/1dscyP4rFOKHBUnyjHgCHGzLll4quxd2ak2oQ4Us+qGRQLQNBlUDBJh6Zh9pESHcJTaBxlGZg0oN33b1HpUlnEtxKY9pvC77ccQYn8u<br>sLClLq157svTnBbXYn-7BgQ7+AUKG+WFuCDMRh05LucHJJPSXAtcwwlQBpXHzsTyOJ2EXhKBEVOB+rFnAt/DJFDdzfp6pLcO8LnotZQ3h/FtHUDxLtH0xX3gB7vHQQLhy6WTnzYZLT2PHv<br>1906ASyMvVd1qW01hoss57Z7hecxs+fqddfTfH+19uphXHzVDcLInBFHxATBfKXRrQq4WxRMxIM43n3v+zhWYH saidell@saidell-vostro-15-3568 |
|---|
| IYOGASMWVGIMDSES/Z/NDEXSF/EQDSTTIN+IYEUDNXFWZVDECKIZNBFFWSAI8TKCXKFQQ4WXKNWIM43m3V+ZNWYH Saldell@Saldell-VOSTFO-15-3508<br>saidell@saidell-VOstro-15-3568:-\$   |

- 4. Save the Public key generated in step above as described in Device configuration section.
- 5. Login to device using Private key generated above with username as "admin".

# **RADIUS** authentication

Device management access using RADIUS authentication allows multiple users to access using unique credentials and is secured.

## Device configuration

Management access using RADIUS authentication method can be configured on device using standalone AP or from cnMaestro. Navigate to **System > Management** and configure the following:

- 1. Enable **RADIUS Mgmt Auth** checkbox.
- 2. Configure RADIUS IPv4/IPv6/Hostname and shared secret in **RADIUS Server** and **RADIUS** Secret parameters respectively.
#### 3. Click Save.

| Cambium Networks" Cr | Pilot E400 - E400-AFA308          |  |   | 🖒 Reboot | € Logout |
|----------------------|-----------------------------------|--|---|----------|----------|
| Lal Dashboard        | Configure / System                |  |   |          |          |
|                      | System                            |  |   |          |          |
| 🙆 Monitor 👻          | Name                              | E400-AFA308  | Hostname of the device (max 64 characters)  |          |          |
| Configure •          | Location                          | E400-AFA306  | Location where this device is placed (max 64 characters)                                    |          |          |
| 🖵 System             | Contact                           |  | Contact information for the device (max 64 charactera)                                      |          |          |
| * Radio              | Country-Code                      | India 🔻  | For appropriate regulatory configuration  |          |          |
| ♥ WLAN               | Placement                         | Indoor      Outdoor Configure the AP placement details |   |          |          |
|                      | LED                               | Whether the device LEDs should be ON during operation  |   |          |          |
| A Network            | LLDP                              | Whether the AP should transmit LLDP packets            |   |          |          |
| Services             | Management                        |  |   |          |          |
| 幸 Operations         |                                   |  |   |          |          |
| F Troubleshoot -     | Admin Password Autopilot          |  | Configure password for authentication of GUI and CLI assions<br>Autopilot Management of APs |          |          |
| F Houbleshool        | Telnet                            | Default  | Handpinon managannam sa Pin a   |          |          |
|                      | SSH                               | Enable SSH access to the device CLI                    |   |          |          |
|                      | SSH Key                           |  | Use SSH keys instead of password for authentication   |          |          |
|                      | HTTP                              | Enable HTTP access to the device GUI                   |   |          |          |
|                      | HTTP Port                         | 80   | Part No for HTTP access to the device GUI(1-65535)  |          |          |
|                      | HTTPS                             | Enable HTTPS access to the device GUI                  |   |          |          |
|                      | HTTPS Port                        | 443  | Port No for HTTPS access to the device GUI(1-65535)   |          |          |
|                      | RADIUS Mgmt Auth<br>RADIUS Server | Enable RADIUS authentication of GUI/CLI sessions       | R&DIUS server IP/Hostname   |          |          |
|                      |                                   |  | RADIUS server shared secret   |          |          |
|                      | RADIUS Secret                     |  | RADIUS server shared secret   |          |          |

Figure 76 System > Management: RADIUS Server and RADIUS Secret parameters

4. Login to device using appropriate credentials as shown in Figure 77.

Figure 77 UI Login page

| Login |      |
|-------|------|
| -     | bob  |
|       | •••• |
| Sig   | n In |

# Chapter 14: Mesh

cnPilot Enterprise series Wi-Fi Aps support wireless mesh allowing the user to easily extend the range of their network and to cover areas where a cable run might be hard to do. Mesh support was added in software version 2.0.

cnPilot devices support mesh connections between radios. Mesh links can form between radios which are operating in the same band. Given the larger set of available channels and typically cleaner RF environment Cambium recommend using the 5GHz radio for mesh backhaul.

For a stable mesh link to be established, cnPilot mesh operates in three modes of operation:

#### 1. Mesh Base (MB)

cnPilot device that operates in MB mode is the key to Mesh topology. MB is usually connected to the wired network. The radio setup for MB will select a channel and start transmitting beacons as soon as the AP comes up.

#### 2. Mesh Client (MC)

cnPilot device that operates in MC mode, scans all available channels supported as per regulatory domain and establishes a link with MB.

#### 3. Mesh Recovery (MR)

This mode when enabled helps to maintain mesh link if there is a disruption in backhaul link established with MB and MC. Mesh link disruption can cause due to PSK mismatch or due to asynchronous configurations on MB and MC. This mode needs to be exclusively enabled on MB device.

This mode can also help in Zero Touch Configuration of cnPilot device.

### Mesh configurable parameters

Table 60 lists the configurable parameters that are exclusive to mesh:

| Parameters | Description  | Range | Default |  |  |  |  |
|------------|--|-------|---------|--|--|--|--|
| Enable     | Option to enable a WLAN profile. Once enabled, a Beacon – –<br>is broadcasted with SSID and respective configured<br>parameters in a WLAN profile.   |       |         |  |  |  |  |
| Mesh       | <ul> <li>This parameter is required when a WDS connection is established with cnPilot devices. Four options are available under this parameter:</li> <li><b>Base</b> <ul> <li>A WLAN profile configured with mesh-base will operate like a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients.</li> </ul> </li> <li><b>Client</b></li> </ul> | ł     | Off     |  |  |  |  |

| Parameters  | Description   | Range                        | Default  |
|-------------|---|------------------------------|----------|
|             | A WLAN profile configured with mesh-client will scan<br>all available channels on startup, looking for a mesh-<br>based AP to connect.  |                              |          |
|             | 3. Recovery   |                              |          |
|             | A WLAN profile configured as mesh-recovery will<br>broadcast pre-configured SSID upon detection of<br>mesh link failure after a successful connection. This<br>needs to be exclusively configured on mesh-base<br>device. Mesh-client will auto scan for mesh-recovery<br>SSID upon failure of mesh link. |                              |          |
|             | 4. Off  |                              |          |
|             | Mesh support disable on WLAN profile.   |                              |          |
| SSID        | SSID is the unique network name to which MC connects and establishes mesh link.   | _                            | -        |
| VLAN        | Management VLAN to access all devices in mesh topology.   | 1-4094                       | 1        |
| Security    | This parameter determines key values that is encrypted<br>based on selected algorithm. Following security methods<br>are supported by cnPilot devices:  | _                            | Open     |
|             | 1. Open   |                              |          |
|             | This method is preferred when Layer 2 authentication<br>is built in the network. With this configured on cnPilot<br>device, any mesh link can be established.   |                              |          |
|             | 2. WPA2-Pre-Shared Keys   |                              |          |
|             | This mode is supported with AES encryption.   |                              |          |
|             | 3. WPA2 Enterprise  |                              |          |
|             | This security type uses 802.1x authentication to associate mesh devices. This is a centralized system of authentication method.   |                              |          |
| Passphrase  | String that is a key value to generate keys based on security method configured.  | _                            | 12345678 |
| Radios      | Each SSID can be configured to be transmitted as per the deployment requirement. For a mesh WLAN profile, options available to configure band:  | _                            | 2.4GHz   |
|             | • 2.4GHz  |                              |          |
|             | • 5GHz  |                              |          |
| Max Clients | This specifies the maximum number of mesh clients that<br>can be associated to a mesh WLAN profile. This varies<br>based on cnPilot device model number. Refer <b>Table 16</b> for<br>more details.   | 1-512<br>(Refer<br>Table 16) | 128      |

| Parameters                      | Description  | Range | Default  |
|---------------------------------|--|-------|----------|
| Client Isolation                | This feature needs to be enabled when there is a need for<br>prohibition of inter mesh devices communication either<br>over the network or on an AP. Three options are available<br>to configure based on requirement:   | _     | Disabled |
|                                 | 1. Disable   |       |          |
|                                 | This option when selected disables client isolation feature. i.e. Inter Mesh client communication is allowed.  |       |          |
|                                 | 2. Local   |       |          |
|                                 | This options when selected enables client isolation feature. This option prevents inter mesh client communications connected to same device.   |       |          |
|                                 | 3. Network Wide  |       |          |
|                                 | This option when selected enables network wide<br>client isolation feature. It prevents mesh client<br>communications connected to different AP deployed<br>in same network.   |       |          |
| Hide SSID                       | This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.   | _     | Disabled |
| Mesh Vlan<br>Tagging            | Enable the VLAN tagging over mesh link. This is applicable only for Cambium mesh topology.   | _     | Enabled  |
| Mesh Auto<br>Detect<br>Backhaul | <ol> <li>Single Hop         MC is configured on MB with same WLAN parameters.<br/>When enabled, this feature triggers when a MB losses<br/>Ethernet connectivity. MB profile will get disabled and<br/>MC profile will get enable and establishes mesh link<br/>with nearest MB. For MB profile to get auto disabled,<br/>uncheck Mesh Multi Hop.     </li> <li>Multi Hop         MC is configured on MB with same WLAN parameters.<br/>When enabled, this feature triggers when a MB losses<br/>Ethernet connectivity. MB profile and MC profile will     </li> </ol> | _     | Disabled |
| Drop Multicast<br>Traffic       | get enable and establishes mesh link with nearest MB.<br>When enabled, will drop all multicast flowing in or out of<br>that WLAN.  | _     | Disabled |
| name                            |  |       |          |
| Insert DHCP<br>Option 82        | Enabling this option appends Option 82 in the DHCP packets. Following information is allowed to configure:   |       | Disabled |
|                                 | 1. DHCP Option 82 Circuit ID   |       |          |
|                                 | Configurable parameters under this option are as follows:  |       |          |
|                                 | Hostname   |       |          |

| Parameters                   | Description   | Range    | Default  |
|------------------------------|---|----------|----------|
|                              | <ul> <li>APMAC</li> <li>Site ID</li> <li>BSSID</li> <li>SSID</li> <li>Custom</li> </ul> 2. DHCP Option 82 Remote ID <ul> <li>Configurable parameters under this option are as follows:</li> <ul> <li>Hostname</li> <li>APMAC</li> <li>Site ID</li> <li>BSSID</li> <li>SSID</li> <li>Custom</li> </ul> </ul> |          |          |
| Tunnel Mode                  | This option is enabled when user traffic is tunneled to central network either using L2TP or L2GRE.   | _        | Disabled |
| Mesh<br>Monitored<br>Host    | This parameter is exclusive to MC device. Configure IP or<br>Hostname to check the link status.   | _        | -        |
| Mesh Monitor<br>Duration     | Configure the interval at which the ping is sent for the configured mesh monitored host.  | 5-60 Min | 30       |
| Mesh<br>Recovery<br>Interval | Configure the interval for the consecutive ping loss seen<br>after which the mesh link is considered to be down and a<br>reconnect is attempted. One can configure the duration<br>and interval both to be the same at which case the first<br>ping loss itself will result in triggering the reconnect.    | 5-30 Min | 30       |

To configure the above parameters, navigate to the **Configure > WLAN > Basic** tab and provide the details as given below:

- 1. Select the **Enable** checkbox to enable the operations of this WLAN.
- 2. Select the operating parameters Base/Client/Recovery from the Mesh drop-down list.
- 3. Enter a name that uniquely identifies a wireless network in the SSID textbox.
- 4. Enter the **VLAN** parameter value in the textbox.
- 5. Select **Security** type from the drop-down list.
- 6. Enter WPA2 Pre-shared security passphrase or key in the **Passphrase** textbox.
- 7. Select the radio type (2.4GHz, 5GHz) on which the WLAN should be supported from the **Radios** drop-down list.
- 8. Select Max Clients parameter value from the drop-down list.

- 9. Select the required **Client Isolation** parameter from the drop-down list.
- 10. Enable Hide SSID checkbox.
- 11. Enable Mesh Vlan Tagging checkbox.
- 12. Enable Mesh Auto Detect Backhaul checkbox.
- 13. Enable Drop Multicast Traffic checkbox.
- 14. Enable Insert DHCP Option 82 checkbox.
- 15. Select Tunnel Mode checkbox to enable tunnelling of WLAN traffic over configured tunnel.
- 16. Enter the IP or hostname name in the **Mesh Monitored Host** textbox.
- 17. Select the Mesh monitor duration time from the drop-down list.
- 18. Select the Mesh recovery interval time from the drop-down list.
- 19. Click Save.

#### Figure 78 Configure > Mesh > Base parameters

| Mesh                      | Base   | Mesh Base/Client/Recovery mode   |
|---------------------------|--|--|
| SSID                      | TEST_SMOKE_8                                 | The SSID of this WLAN (upto 32 characters)   |
| VLAN                      | 1  | Default VLAN assigned to clients on this WLAN. (1-4094)  |
| Security                  | WPA2 Pre-shared Keys                         | Set Authentication and encryption type   |
| Passphrase                |  | WPA2 Pre-shared Security passphrase or key   |
| Radios                    | 5GHz 🔻                                       | Define radio types (2.4GHz, 5GHz) on which this WLAN<br>should be supported  |
| Max Clients               | 5  | Default maximum Client assigned to this WLAN. (1-256)  |
| Client Isolation          | Disable •                                    | When selected, it allows wireless clients connected to the<br>same AP or different APs to communicate with each other i<br>the same VLAN |
| Hide SSID                 | Do not broadcast SSID in beacons             |  |
| Mesh Vlan Tagging         | Enable the vian tagging over mesh link       |  |
| Mesh Auto Detect Backhaul | Enable the ethernet link status detection an | d try to connect over mesh link  |
| Drop Multicast Traffic    | Drop the send/receive of multicast traffic   |  |
| Advanced                  |  |  |
| Insert DHCP Option 82     | Enable DHCP Option 82                        |  |
| Tunnel Mode               | Enable tunnelling of WLAN traffic over con   | igured tunnel  |

| Mesh                                    | Client               | ✓ Mesh Base/Client/Recovery mode   |
|---|----------------------|--|
| SSID                                    | TEST_SMOKE_8         | The SSID of this WLAN (upto 32 characters)   |
| VLAN                                    | 1                    | Default VLAN assigned to clients on this WLAN. (1-<br>4094)                                  |
| Security                                | WPA2 Pre-shared Keys | Set Authentication and encryption type   |
| Passphrase                              | *******              | WPA2 Pre-shared Security passphrase or key   |
|   |                      |  |
| Radios                                  | 5GHz                 | ▼ Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported                   |
| Radios<br>Mesh Vian Tagging             | 5GHz                 | WLAN should be supported   |
| Radios                                  |                      | WLAN should be supported   |
| Radios<br>Mesh Vian Tagging             |                      | WLAN should be supported   |
| Radios<br>Mesh Vlan Tagging<br>Advanced |                      | WLAN should be supported<br>nesh link<br>IP or hostname that if not reachable a mesh recover |

Figure 79 Configure > Mesh > Client parameters

### Mesh link

This section briefs about configuration of device to get mesh link established with different deployment scenarios.

### Order of Mesh profile configuration

If a device is configured as mesh base/client/recovery, recommended order of WLAN configuration should be as follows:

- WLAN profile 1: Mesh client
- WLAN profile 2: Mesh base
- WLAN profile 3: Mesh recovery

### VLAN 1 as management interface

Follow the below steps to establish mesh link with VLAN 1 as management interface:

- 1. On MB, configure MB and MR. Follow the below steps to configure MB:
  - a. WLAN profile

| La Dashboard     Configure : Wain       Ba Monitor -     Add wu,AA       Configure -     Edt WLAN       St St,WAAK     ISTS,WAAK  |        |
|---|--------|
| BalMonitor - Edit WLAN  |        |
|   |        |
|   |        |
| Ţ 5)stem  |        |
| Radio     Radio Server Quest Access Usage Limits Access   | Delete |
| ♥ MLM Basic   |        |
| A Network Enable #  |        |
| Benose     Meth     Base     Meth     Add Dass Clear Recovery mote  |        |
| SSID CAMBIUM_MESH_BASE The SSID of this VILAW (upto 32 chemotien)   |        |
| Ze Operations VLAN 1 Default VLAN segred to clent on the VLAN (14094)   |        |
| Security ppn + Oet Authentication and encryption type   |        |
| F Toubleshoot - Radios 2.40Hz United States 2.40Hz |        |
| Max Clients 128 Default maximum Client assigned to itin VLAV (1-250)  |        |
| Client Isolation Disable V When selected, if allows wreters client connected to the same AP or different APs to communicate with each other a VLAW  | e same |
| Hide SSID  D cont breadmant SSID in beacons   |        |
| Mesh Vaan Tagging 🌾 Enable the vian tagging over meah tink  |        |
| Mesh Auto Detect Backbaul 🔋 Enable the enterner link status detection and try to connect over mesh link   |        |
| Orego Multiceast Traffic 👘 Dray the sendirective of multiceast buffic   |        |
| Advanced  |        |
|   |        |
| Insert DHCP Option 82 0 Entatio CHCP Option 82  |        |
| Tunnet Mode  C Enable tunnelling of HLAN traffic over configured tunnel   |        |
| Save Cancel   |        |

Figure 80 Mesh Base configuration with native VLAN 1

b. Management VLAN interface

Figure 81 Mesh Base configuration > Management VLAN 1

| Cambium Networks | cnPilot E400 - E400-AFA308               |   |                  |   | ර් Reboot            | 🕞 Logou |
|------------------|--|---|------------------|---|----------------------|---------|
| de Dashboard     | Configure / Network                      |   |                  |   |                      |         |
| 🙆 Monitor 👻      | VLAN Routes Ethermet Ports Security DHCP | Tunnel PPPoE VLAN Pool                                      |                  |   |                      |         |
| Ocnfigure -      | Edit VLAN 1                              | Delete this interface                                       |                  |   | Add new L3 Interface |         |
| Garage System    | IP Address                               | DHCP  Static IP  Net  | twork Mask       |   |                      | - 11    |
| ∳ Radio          |  |   | CX.3007.3007.307 |   |                      |         |
| 🗢 WLAN           | NAT                                      | When NAT is enabled, IP addresses under this SVI are hidden |                  |   |                      |         |
| A Network        | Zeroconf IP                              | Support 169.254.x.x local IP address                        |                  |   |                      |         |
| Services         | Management Access                        | Allow from both Wired & Wireless                            | ٣                | CLI/GUI/SNMP access via this interface        |                      |         |
| Services         | DHCP Relay Agent                         | 3003.3007.3007.3003   |                  | Enables relay agent and assign DHCP server to | đ                    |         |
|                  | DHCP Option 82 Circuit ID                | None  | ٠                |   |                      |         |
|                  | DHCP Option 82 Remote ID                 | None  | ٣                |   |                      |         |
| 🗲 Troubleshoot 👻 | Request Option All                       | Use Gateway, DNS, Dhcp options received on this interface   |                  |   |                      |         |
|                  | Routing & DNS                            |   |                  |   |                      |         |
|                  | Default Gateway                          |   |                  | IP address of default gateway                 |                      |         |
|                  | Domain Name                              |   |                  | Domain name                                   |                      |         |
|                  | DNS Server 1                             |   |                  | Primary Domain Name Server                    |                      |         |
|                  | 2  |   |                  | Secondary Domain Name Server                  |                      |         |
|                  | DNS Proxy                                | DNS Proxy   |                  |   |                      |         |
|                  |  | Save  | ncel             |   |                      |         |

c. Ethernet interface

| Cambium Networks" | cnPilot E400 | - E400-AFA     | 308        |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            | Reboot         | 6 |
|-------------------|--------------|----------------|------------|----------------------------|---------|------|-----------|-----------|------------|------|----------------|--------|---------------------------------|---------------------|-----|----------------|----------------------------|----------------|---|
| M Dashboard       | Config       | gure / Network |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
| 🝘 Monitor 👻       | VLA          |                | Ethernet F | Ports Sec                  | urity I | OHCP | Tunnel    | PPPoE     | VLAN       | Pool |                |        |                                 |                     |     |                |                            |                |   |
| Ocnfigure -       | E            | lh1            |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
| - System          |              |                |            |                            |         |      | ETH1      |           | s Single V | /LAN |                | ٣      |                                 |                     |     |                |                            |                |   |
| + Radio           |              |                |            |                            |         | Acc  | ess Mode  | VLAN<br>1 |            |      |                |        |                                 |                     |     |                |                            |                |   |
| 🗢 WLAN            |              |                |            |                            |         |      |           |           |            |      | Save           | Cancel |                                 |                     |     |                |                            |                |   |
| A Network         |              | ACL            |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
| Services          |              | Precede        | nce        |                            |         |      |           |           |            |      | Policy         |        |                                 | Direction           |     |                |                            |                |   |
| 듚 Operations      |              | 1              |            |                            |         |      | ٠         |           |            |      | Deny           | ٣      |                                 | In                  |     |                | ٣                          |                |   |
| - operatione      |              | Type           |            |                            |         |      | *         |           |            |      | Source IP/Mask |        |                                 | Destination IP/Mask |     |                |                            |                |   |
| 🗲 Troubleshoot -  |              | Descript       | ion        |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            | Save           |   |
|                   |              |                |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
|                   |              | Preced         | Ince       | <ul> <li>Policy</li> </ul> |         | Ÿ    | Direction |           | ~ Тур      | 96   | ~ Rule         |        | <ul> <li>Description</li> </ul> | ion                 |     |                | <ul> <li>Action</li> </ul> | ~              |   |
|                   |              |                |            |                            |         |      |           |           |            |      | No Rules av    |        |                                 |                     |     |                |                            |                |   |
|                   |              |                |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
|                   |              |                |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
|                   |              |                |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            |                |   |
|                   |              |                |            |                            |         |      |           |           |            |      |                |        |                                 |                     |     |                |                            | -              |   |
|                   |              |                |            |                            |         |      |           |           |            |      |                |        |                                 |                     | 4 4 | /1 <b>&gt;</b> | ▶  10 ¥                    | items per page |   |

#### Figure 82 Mesh Base Ethernet configuration > Access VLAN 1

- 2. Configure MC as below:
  - a. WLAN profile

| Figure 83 | Mesh | Client | configuration | with | VLAN | 1 |
|-----------|------|--------|---------------|------|------|---|
|-----------|------|--------|---------------|------|------|---|

| Cambium Networks" | cnPilot E400 - E400-AFA308 |  | 01  | Reboot 🖙 Lo | ogout |
|-------------------|----------------------------|--|---|-------------|-------|
| Left Dashboard    | Configure / Wlan           |  |   |             |       |
| 🖀 Monitor 🗸       | Add WLAN Edit WLAN         |  |   |             |       |
| 🌣 Configure 👻     | !!STSK_WLAN                |  |   |             |       |
| - System          |                            |  |   | Delete      |       |
| ₱ Radio           | Basic                      |  |   | Delete      | 9     |
| 🗢 WLAN            | Basic                      |  |   |             |       |
| A Network         | Enable                     | *                                      |   |             |       |
| Services          | Mesh                       | Client                                 | Mesh Base/Client/Recovery mode The SSID of this WLAN (upto 32 characters)                             |             |       |
| 幸 Operations      | SSID                       | CAMBIUM_MESH_BASE                      | Default VLAN assigned to clients on this WLAN. (1-4094)   |             |       |
|                   | Security                   | r<br>open T                            |   |             |       |
| 🗲 Troubleshoot -  | Radios                     | 5GHz •                                 | Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported                              |             |       |
|                   | Mesh Vlan Tagging          | Enable the vian tagging over mesh link |   |             |       |
|                   | Advanced                   |  |   |             |       |
|                   | Mesh Monitored Host        |  | IP or hostname that if not reachable a mesh recovery is attempted                                     |             |       |
|                   | Mesh monitor duration      | 30                                     | Duration in minutes (5-60)  |             |       |
|                   | Mesh recovery interval     | 30                                     | Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30) |             |       |
|                   |                            |  |   |             |       |
|                   |                            | Save Cancel                            |   |             |       |

b. Management interface

| Cambium Networks cr | Pilot E400 - E400-AFA308                              |   |  | ් Reboot 🕞 Log       |  |  |
|---------------------|---|---|--|----------------------|--|--|
| 📶 Dashboard         | Configure / Network                                   |   |  |                      |  |  |
| 🙆 Monitor 🗸         | VLAN Routes Ethernet Ports Security DHCP T            | unnel PPPoE VLAN Pool   |  |                      |  |  |
| Configure -         | Edit VLAN 1 V   |   |  | Add new L3 Interface |  |  |
| G System            | IP Address  | Delete this interface<br>© DHCP   |  | Add new L3 interface |  |  |
| ∲ Radio             |   | Static IP         Network M           x000,000,0000         x000,000  |  |                      |  |  |
| 🗢 WLAN              | NAT<br>Zeroconf IP                                    | <ul> <li>When NAT is enabled, IP addresses under this SVI are hidden</li> <li>Support 169.254.x.x local IP address</li> </ul> |  |                      |  |  |
| a Network           | Management Access                                     | Allow from both Wirel & Wireless  | <ul> <li>CL//GU//SNMP access via this interface</li> </ul> |                      |  |  |
| Services            | DHCP Relay Agent                                      | X06.3006.3006   | Enables relay agent and assign DHCP server to it           |                      |  |  |
| 茎 Operations        | DHCP Option 82 Circuit ID<br>DHCP Option 82 Remote ID | None *  |  |                      |  |  |
| F Troubleshoot -    | Request Option All                                    | None  Use Gateway, DNS, Dhcp options received on this interface   | ·  |                      |  |  |
|                     | Routing & DNS   |   |  |                      |  |  |
|                     | Default Gateway                                       |   | IP address of default gateway                              |                      |  |  |
|                     | Domain Name   |   | Domain name  |                      |  |  |
|                     | DNS Server 1  |   | Primary Domain Name Server<br>Secondary Domain Name Server |                      |  |  |
|                     | 2<br>DNS Proxy  | DNS Proxy   | Secondery Lorreen Nathe Server                             |                      |  |  |
|                     |   | Save Cancel   |  |                      |  |  |

#### Figure 84 Mesh Client configuration > Management VLAN 1

c. Ethernet interface

Figure 85 Mesh Client Ethernet configuration > Access VLAN 1

| Configure : Network      Configure :      Configure -      System      Rado      VLAN      KNetwork      KNetwork      Security      Configure :      Conf      |                     |
|--|---------------------|
|  |                     |
| nfigure -<br>ten  ten  ten  cen  cen  cen  cen  cen  |                     |
| tem ETH Access Single VLAN • Access Single VLAN Access Mode VLAN I Access Mode |                     |
| Access Mode VLAN<br>1<br>Access Mode Cancel<br>ACL   |                     |
| AAN Example Center   |                     |
| ACL  |                     |
|  |                     |
| Services Brandstore Balloy   |                     |
|  | Direction           |
| perations  | In 🔻                |
| Type Source IPMask   | Destination IP/Mask |
| roubleshoot - Description  | Save                |
|  |                     |
| Precedence v Policy v Direction v Type v Rule v Descr  | ription ~ Action ~  |

- 3. Configure MR on MB device as follows on any WLAN profile:
  - a. WLAN profile

| Cambium Networks | cnPilot E400 - E400-AFA308                     | C Reboot | C+ Logout |
|------------------|--|----------|-----------|
| 🔟 Dashboard      | Configure / Wan                                |          |           |
| 🚳 Monitor 🗸      | Add WLAN Edit WLAN                             |          |           |
| 🌣 Configure 🗸    | IISTSK_WLAN                                    |          |           |
| System           |  |          | Delete    |
| Radio            | Base Access                                    |          | Delete    |
| 🗢 WLAN           | Basic  |          |           |
| A Network        | Enable 8                                       |          |           |
| Services         | Mesh Recovery   Mesh Base/Client/Recovery mode |          |           |
| 至 Operations     | Save Cance                                     |          |           |
| 🗲 Troubleshoot - |  |          |           |

#### Figure 86 Configure > WLAN > Mesh Recovery

### Non-VLAN 1 as management interface

Follow the below steps to establish mesh link with Non-VLAN 1 as management interface:

- 1. On MB, configure MB and MR. Following are the steps to configure MB:
  - a. WLAN profile

| Cambium Networks                   | cnPilot E400 - E400-AFA308  | © Reboot i≆ Logout  |
|------------------------------------|---|---|
| al Dashboard                       | Configure / Wlan  |   |
| 🖀 Monitor 👻                        | Add WLAN  |   |
| 🕏 Configure 👻                      | IIST SK_WLAN  |   |
| System                             | Basic Radius Server Quest Access Usage Limits Access  | Deinto  |
| † Radio                            | Caller Francis Certre Celevi Pocess College Links Pocess                                    | - Marine  |
| ♥ WLAN                             | Basic   |   |
| A Network                          | Enable <sup>10</sup>  |   |
| Services                           | Mesh Base   | Mesh Base/Client/Recovery mode  |
|                                    | SSID CAMBIUM_MESH_BASE  | The SSID of this WLAN (upto 32 characters)  |
| ≆ Operations                       | VLAN 1  | Default VLAN assigned to clients on this WLAN. (1-4094)   |
| F Troubleshoot -                   | Security open   | Set Authentication and encryption type  |
| <ul> <li>Troubleshoot •</li> </ul> | Radios 2.4GHz   | <ul> <li>Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported</li> </ul>  |
|                                    | Max Clients 128   | Default maximum Client assigned to this WLAN. (1-256)   |
|                                    | Client isolation Disable  | When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN |
|                                    | Hide \$\$ID Do not broadcast SSID in beacons  |   |
|                                    | Mesh Vian Tagging Reader the vian tagging over mesh link                                    |   |
|                                    | Mesh Auto Detect Backhaul Enable the ethernet link status detection and try to connect over | r medh link   |
|                                    | Drop Multicast Traffic Drop the send/receive of multicast traffic                           |   |
|                                    | Advanced  |   |
|                                    | Insert DHCP Option 82 Enable DHCP Option 82   |   |
|                                    | Tunnel Mode Enable tunneling of WLAV traffic over configured tunnel                         |   |
|                                    |   | Cancel  |

#### Figure 87 Mesh Base configuration with non-VLAN1

b. Management VLAN interface

| Cambium Networks" | cnPilot E400 - E400-AFA308   | 🗘 Reboot 🛭 😁 Logo   |
|-------------------|--|---|
| 🔟 Dashboard       | Configure / Network  |   |
| 🙆 Monitor 🗸       | VLAN Routes Ethermet Ports Security DHCP Tunnel PPPoE VLAN Pool              |   |
| Configure -       | VLAN<br>Edit VLAN 1 V Delete tibis interface                                 | Add new L3 Interface                                      |
| System            | IP Address @ DHCP<br>© Static IP   | Network Mask  |
| ₱ Radio           | 2000/200X<br>2000/200X   | NOR JOIC ZOCI JOX   |
| 🗢 WLAN            | NAT When NAT is enabled, IP addresses under this SVI are in                  | sre hidden  |
| A Network         | Zeroconf IP Support 169.254.x.x local IP address                             |   |
| Services          | Management Access Allow from both Wireless                                   | <ul> <li>CL//GU/SMMP access via this interface</li> </ul> |
| Convices          | DHCP Relay Agent SOCK SOCK SOCK SOCK   | Enables relay agent and assign DHCP server to it          |
|                   | DHCP Option 82 Circuit ID None   | ¥   |
|                   | DHCP Option 82 Remote ID None  | ¥   |
| F Troubleshoot -  | Request Option All 🛛 Vise Gateway, DNS, Dhcp options received on this interf | terface   |
|                   | Routing & DNS  |   |
|                   | Default Gateway  | IP address of default gateway                             |
|                   | Domain Name  | Domain name   |
|                   | DNS Server 1   | Primary Domain Name Server                                |
|                   | 2  | Secondary Domain Name Server                              |
|                   | DNS Proxy DNS Proxy  |   |
|                   |  | Seve Cancel   |

Figure 88 Mesh Base configuration > Management non-VLAN 1

c. Ethernet interface

Figure 89 Mesh Base Ethernet configuration > Access non-VLAN 1

| Precedence v Policy v Direction v Type v Rule v Description v Action v   | Cambium Networks | cnPilot E400 | 0 - E <b>4</b> 0 | 0-AFA308    |             |          |      |           |       |               |        |             |   |          |     |      |      |         | O Reboot      | 🕞 Log |
|--|------------------|--------------|------------------|-------------|-------------|----------|------|-----------|-------|---------------|--------|-------------|---|----------|-----|------|------|---------|---------------|-------|
| Almandor -     Configure -     System     Radio     VLAN     National     Almandor -     Services   Procedence   Procedence  <   | 📶 Dashboard      | Config       | igure / 1        | letwork     |             |          |      |           |       |               |        |             |   |          |     |      |      |         |               |       |
| © Configure -<br>⇒ System  | 🗃 Monitor 👻      | VLA          | N R              | outes Ether | met Ports S | lecurity | DHCP | Tunnel    | PPPoE | VLAN Pool     |        |             |   |          |     |      |      |         |               |       |
| > year Radic   | Configure -      | E            | Bh 1             |             |             |          |      |           |       |               |        |             |   |          |     |      |      |         |               |       |
| Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar<br>Ackar | System           |              |                  |             |             |          |      |           |       | s Single VLAN |        |             | ٣ |          |     |      |      |         |               |       |
| Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Altaine<br>Alt   | Radio            |              |                  |             |             |          | Ac   | cess Mode |       |               |        |             |   |          |     |      |      |         |               |       |
| Benoces Benoc  | ♥ WLAN           |              |                  |             |             |          |      |           |       |               |        | Save Cancel |   |          |     |      |      |         |               |       |
| te Operations  | 📥 Network        |              | _ A              | CL          |             |          |      |           |       |               |        |             |   |          |     |      |      |         |               |       |
| E Operations  Type Source IPMask IP Outbleshood  Type Oestination IPMask IP Oestination IPMask III O O O O O O O O O O O O O O O O O   | Services         |              |                  |             |             |          |      |           |       |               |        |             |   |          |     |      |      |         |               |       |
| F Troubleshoot -     Proceedence      V Policy     V Direction     V Type     V Rule     V Direction     V Type     V Rule     V Direction     V Direction     V Type     V Rule     V Direction   | E Operations     |              |                  |             |             |          |      |           |       |               |        | ,           | Ŧ |          |     |      |      | ٣       |               |       |
| Precedence v Policy v Direction v Type v Rule v Description v Action v   | F Troubleshoot - |              |                  | IP          |             |          |      | •         |       |               |        |             |   |          |     |      |      |         |               |       |
|  |                  |              |                  | escription  |             |          |      |           |       |               |        |             |   |          |     |      |      |         | Save          |       |
|  |                  |              |                  | recedence   | ~ Poli      | су       | Ý    | Direction | 1     | ~ Туре        | ~ Rule |             | Ý | Descript | ion |      | Ý    | Action  | ¥             |       |
|  |                  |              |                  |             |             |          |      |           |       |               | No F   |             |   |          |     |      |      |         | *             |       |
|  |                  |              |                  |             |             |          |      |           |       |               |        |             |   |          |     |      |      |         |               |       |
|  |                  |              |                  |             |             |          |      |           |       |               |        |             |   |          |     |      |      |         | -             |       |
| If a 1 (a ) If a parameter source of the second sec   |                  |              |                  |             |             |          |      |           |       |               |        |             |   |          |     | 14 4 | 1 11 | ▶  10 ¥ | tems per page |       |

- 2. Configure MC as below:
  - a. WLAN profile

| Cambium Networks" | nPilot E400 - E400-AFA308 |  | c   | b Reboot | 🕞 Logout |
|-------------------|---------------------------|--|---|----------|----------|
| 📶 Dashboard       | Configure / Wlan          |  |   |          |          |
| 🙆 Monitor 👻       | Add WLAN                  |  |   |          |          |
| 🕏 Configure 👻     | !!\$TSK_WLAN              |  |   |          |          |
| 🖵 System          | _                         |  |   |          |          |
| † Radio           | Basic                     |  |   |          | Delete   |
| ♥ WLAN            | Basic                     |  |   |          |          |
| 📥 Network         | Enable                    | 8                                      |   |          |          |
| Services          | Mesh                      |  | Mesh Base/Client/Recovery mode  |          |          |
|                   | SSID                      | II\$TSK_WLAN_Free\$!!                  | The SSID of this WLAN (upto 32 characters)  |          |          |
|                   | VLAN                      | 10                                     | Default VLAN assigned to clients on this WLAN. (1-4094)   |          |          |
| 🗲 Troubleshoot -  | Security                  | open                                   | Set Authentication and encryption type  |          |          |
| Troubleshoot •    | Radios                    | 5GHz                                   | <ul> <li>Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported</li> </ul>          |          |          |
|                   | Mesh Vlan Tagging         | Enable the vian tagging over mesh link |   |          |          |
|                   | Advanced                  |  |   |          |          |
|                   | Mesh Monitored Host       |  | IP or hostname that if not reachable a mesh recovery is attempted                                     |          |          |
|                   | Mesh monitor duration     | 30                                     | Duration in minutes (5-60)  |          |          |
|                   | Mesh recovery interval    | 30                                     | Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30) |          |          |
|                   |                           | Save Cancel                            |   |          |          |

### Figure 90 Mesh Client configuration with non-VLAN 1

b. Management interface

Figure 91 Mesh Client configuration > Management non-VLAN 1

| Cambium Networks CN | ilot E400 - E400-AFA308                  |   |                 |  |           | C Reboot             | 🕞 Logout |
|---------------------|--|---|-----------------|--|-----------|----------------------|----------|
| 🔟 Dashboard         | Configure / Network                      |   |                 |  |           |                      |          |
| & Monitor ◄         | VLAN Routes Ethernet Ports Security DHCP | Tunnel PPPoE VLAN Pool                                      |                 |  |           |                      |          |
| 🌣 Configure 👻       | Edit VLAN 10 V                           | Delete this interface                                       |                 |  |           | Add new L3 Interface |          |
| C System            | IP Address                               | DHCP     Static IP  | Network Mask    |  |           |                      |          |
| ₱ Radio             |  | XXX.XXX.XXX.XXX   | 303.303.303.303 | x                                      |           |                      |          |
| 🗢 WLAN              | NAT                                      | When NAT is enabled, IP addresses under this SVI are hidden |                 |  |           |                      |          |
| 1 Marcal            | Zeroconf IP                              | Support 169.254.x.x local IP address                        |                 |  |           |                      |          |
| A Network           | Management Access                        | Allow from both Wired & Wireless                            | ٣               | CLI/GUI/SNMP access via this interface |           |                      |          |
| Services            | DHCP Relay Agent                         | XXX.XXX.XXX   |                 | Enables relay agent and assign DHCP se | ver to it |                      |          |
| 至 Operations        | DHCP Option 82 Circuit ID                | None  | ٣               |  |           |                      |          |
|                     | DHCP Option 82 Remote ID                 | None  |                 |  |           |                      |          |
| 🗲 Troubleshoot -    | Request Option All                       | Use Gateway, DNS, Dhcp options received on this interface   |                 |  |           |                      |          |
|                     | Routing & DNS                            |   |                 |  |           |                      |          |
|                     | Default Gateway                          |   |                 | IP address of default gateway          |           |                      |          |
|                     | Domain Name                              |   |                 | Domain name                            |           |                      |          |
|                     | DNS Server 1                             |   |                 | Primary Domain Name Server             |           |                      |          |
|                     | 2  |   |                 | Secondary Domain Name Server           |           |                      |          |
|                     | DNS Proxy                                | DNS Proxy   |                 |  |           |                      |          |
|                     |  |   |                 |  |           |                      |          |

c. Ethernet interface

| Configure -   System   Sado   WLAN   Network   Sentices   Operations     Configure -     Diff     Access Single VLAN     Access Single VLAN     Access Single VLAN     Access Single VLAN     Sentices     Operations     Diff     Access Single VLAN     Operations     Diff     Operations     Diff     Diff     Diff     Diff     Diff  | Cambium Networks" | cnPilot E400 | - E400-#    | FA308      |          |          |      |                               |        |               |        |        |                                 |          | C Reboo                            |
|---|-------------------|--------------|-------------|------------|----------|----------|------|-------------------------------|--------|---------------|--------|--------|---------------------------------|----------|------------------------------------|
| Montor - Configure  | Dashboard         | Confi        | gure / Netv | rorik      |          |          |      |                               |        |               |        |        |                                 |          |                                    |
| Configure -<br>3 Optimume<br>Radio<br>Monore<br>Services<br>Troubleshoot -<br>Troubleshoot -<br>Configure - | Monitor -         | VLA          | N Route     | is Etherne | at Ports | Security | DHCP | Tunnel                        | PPPoE  | VLAN Pool     |        |        |                                 |          |                                    |
| System         ETH         Access Single VLN         Image: Cancel           ado         VLN         Image: Cancel  | Configure -       | E            | th 1        |            |          |          |      |                               |        |               |        |        |                                 |          |                                    |
| ado IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII  |                   |              |             |            |          |          |      | ETH                           | Access | s Single VLAN |        | ٣      |                                 |          |                                    |
| AcL     Direction       Services     Procedence     Direction       1     •     Direction       Troubleshoot -     Image: Comparison of the compa   | ladio             |              |             |            |          |          | Α    | ccess Mode                    |        |               |        |        |                                 |          |                                    |
| Sendad     Predence     Policy     Direction       Operations     1     0     0     in     •       Trubleshoat -     0     0     0     0     0  | WLAN              |              |             |            |          |          |      |                               |        |               | Save   | Cancel |                                 |          |                                    |
| Precision     Precision       Operations     1     •     0     in     •       Type     Source PMask     Destination PMask     •     •       Troubleshoot -     0     •     •     •     •  | Network           |              | ACL         |            |          |          |      |                               |        |               |        |        |                                 |          |                                    |
| Operations     Type     Source (PMask     Destination (PMask       IP     v     P     P     P       Description     P     P     P     P   | Services          |              |             | Idence     |          |          |      |                               |        |               |        |        |                                 |          |                                    |
| Troubleshoot - Description  | Operations        |              |             |            |          |          |      |                               |        |               |        | •      |                                 |          |                                    |
|   | Troubleshoot -    |              |             | ription    |          |          |      | ,                             | r      |               |        |        |                                 |          | Sava                               |
| Precedence v Policy v Direction v Type v Rule v Description v Action v Action v   |                   |              |             |            |          |          |      |                               |        |               |        |        |                                 |          |                                    |
|   |                   |              | Prei        | .edence    | ~ Pol    | licy     |      | <ul> <li>Direction</li> </ul> | n      | ~ Туре        | V Rule |        | <ul> <li>Description</li> </ul> | ~ Action | ~                                  |
|   |                   |              |             |            |          |          |      |                               |        |               |        |        |                                 |          |                                    |
| No Rules available  |                   |              |             |            |          |          |      |                               |        |               |        |        |                                 |          |                                    |
|   |                   |              |             |            |          |          |      |                               |        |               |        |        |                                 |          |                                    |
|   |                   |              |             |            |          |          |      |                               |        |               |        |        |                                 |          | -                                  |
|   |                   |              |             |            |          |          |      |                               |        |               |        |        |                                 |          | <ul> <li>items per page</li> </ul> |

#### Figure 92 Mesh Client Ethernet configuration > Access non-VLAN 1

- 3. Configure MR on MB device on any WLAN profile as follows:
  - a. WLAN profile

#### Figure 93 Configure > WLAN > Mesh Recovery

| Cambium Networks G | Pilot E400 - E400-AFA308                       | C Reboot | l Logout |
|--------------------|--|----------|----------|
| M Dashboard        | Configure / Wan                                |          |          |
| 🚳 Monitor 👻        | Edit WLAN                                      |          |          |
| & Configure -      | HSTSK_VILAN                                    |          |          |
| G System           |  |          | Pelete   |
| 🕈 Radio            | Benc Access                                    | C        | elete    |
| ♥ WLAN             | Basic  |          |          |
| A Network          | Enable 🕅                                       |          |          |
| Services           | Mesh Recovery v Mesh Base Client Recovery mode |          |          |
| 호 Operations       | Saw Cancel                                     |          |          |
| 🗲 Troubleshoot 🗸   |  |          |          |

# Chapter 15: Autopilot

Autopilot is a feature on Cambium Enterprise Wi-Fi APs that allows one AP to be a controller of other APs in a network to manage:

- Configuration and Onboarding
- Manage Autopilot
- Dashboard
- Insight

### Configuration and Onboarding

This section provides required information to:

- Configure member AP to Autopilot master
- Configuring WLAN in default WLAN Group
- Configuring WLANs with user created WLAN Group
- WLAN group override
- Configuring WPA2-Enterprise WLAN
- Onboard member APs to Autopilot master
- Connect clients to the WLANs and check statistics

### Configure member AP to Autopilot master

To configure member APs to a Master:

Note

1. Open a web browser and browse the IP address of an AP in the network and access the AP's UI page.



The AP needs to be upgraded with autopilot firmware.

2. Go to **Configure > System > Management > Autopilot** and select the AP as Master.

| Cambium Networks CnP | ilot E500 - E500-B99DDC |   |   | C Reboot | 🕞 Logout |
|----------------------|-------------------------|---|---|----------|----------|
| 🔟 Dashboard          | Configure / System      |   |   |          |          |
| 🍘 Monitor 🗸          | System                  |   |   |          |          |
|                      | Name                    | E500-B99DDC   | Hostname of the device (max 64 characters)                          |          |          |
| 🌣 Configure 👻        | Location                | Cambium_Lab   | Location where this device is placed (max 64 characters)            |          |          |
| 🖵 System             | Contact                 | Automation_Team                                       | Contact information for the device (max 64 characters)              |          |          |
| Radio                | Country-Code            | India v   | For appropriate regulatory configuration                            |          |          |
| ♥ WLAN               | Placement               | ● Indoor ○ Outdoor Configure the AP placement details |   |          |          |
| ♥ WLAN               | PoE Output              | • no  | Enable Power-over-Ethernet to an auxiliary device connected to ETH2 |          |          |
| A Network            | LED                     | Whether the device LEDs should be ON during operation |   |          |          |
| Services             | LLDP                    | Whether the AP should transmit LLDP packets           |   |          |          |
| 幸 Operations         |                         |   |   |          |          |
|                      | Management              |   |   |          |          |
| 🗲 Troubleshoot 🗸     | Admin Password          |   | Configure password for authentication of GUI and CLI sessions       |          |          |
|                      | Autopilot               | Default   | Autopilot Management of APs   |          |          |
|                      | Teinet                  | Default<br>Master                                     |   |          |          |
|                      | SSH                     | Disabled<br>Enable SSH access to the device CLI       |   |          |          |

#### Figure 94 Configure > System > Management > Autopilot

- 3. Click Save.
- 4. Refresh the web page and AP brings up the Autopilot UI.

The configured Master AP can perform the following:

- Act as a controller and manage other member APs
- Configure approved APs
- Upgrade firmware
- Display combined statistics and events

Cambium Enterprise AP can be configured the following ways:

- Configuring an AP with Internal DHCP server
- Configuring an AP with External DHCP Server

### Configuring an AP with Internal DHCP server

#### Network Topology

The initial network for installments with external NAT device and VLAN segregation (having two VLANs for the network) is shown in Figure 95.



### Configure an AP with default WLAN group

To configure an AP with default WLAN group:

- 1. Connect all the APs to the native VLAN; for example, VLAN 1 as shown above.
- 2. Configure all the ports of the switch as trunk with the native VLAN 1 where,
  - a. Allowed VLAN: 10, 20
  - b. Native VLAN: 1

To configure the Master AP:

1. Go to **CONFIGURE > System** and configure **Country Code** and **NTP Servers**.

#### Figure 96 Configure > Systems

| Cambium Networks"           | DASHBOARD | 🍕 INSIGHT     |        | ☞ MANAGE                             |   | ₽ LOGOUT    |
|-----------------------------|-----------|---------------|--------|--------------------------------------|---|-------------|
| Configuration               |           |               |        |                                      |   |             |
| Configuration               |           | System        |        |                                      |   |             |
| System                      |           | BASIC CONFIGU | RATION |                                      |   |             |
| Management<br>Wireless LANs |           | Admin Passwor | "d     |                                      | ۲ |             |
| Radios                      |           | Country Code  |        | India                                | • |             |
| MASTER-AP CONFIG            |           | PoE Output    |        | Off                                  | • |             |
| IP Settings<br>Networks     |           | LED           |        | Turn on device LEDs during operation |   |             |
| NETWORK                     |           | LLDP          |        | Turn on LLDP transmission            |   |             |
| Ethernet Ports              |           | TIME SETTINGS |        |                                      |   |             |
| Firewall                    |           | NTP Server 1  |        | time1.google.com                     |   |             |
| OVERRIDES                   |           | NTP Server 2  |        | time2.google.com                     |   |             |
| Access Point Setting        | ţs        | Timezone      |        | Asia/Bengaluru                       | • |             |
| CLI Overrides               |           |               |        |                                      |   |             |
| CLI Overrides               |           |               |        |                                      |   | Cancel Save |

| Cambium Networks 🛛 🖵 DASHE | ioard 🌂 insight | CONFIGURE | S MANAGE               | ₽ Log  |
|----------------------------|-----------------|-----------|------------------------|--------|
| Configuration              |                 |           |                        |        |
| Configuration              | Ethernet Por    | :5        |                        |        |
| System<br>Management       | PORT CONFIGU    | RATION    |                        |        |
| Wireless LANs              | ETH 1           | ETH 2     |                        |        |
| Radios                     | Port Mode       |           | Trunk - Multiple VLANs |        |
| MASTER-AP CONFIG           | Native VLAN     |           | 1                      |        |
| IP Settings<br>Networks    | Allowed VLAN:   |           | 1,15,25,50             |        |
| NETWORK                    | Native Tagged   | l         | Native VLAN tagged     |        |
| Ethernet Ports             | Port Speed      |           | Auto 🔹                 |        |
| Firewall<br>Tunnels        | Port Duplex     |           | Full Duplex •          |        |
| OVERRIDES                  |                 |           |                        |        |
| Access Point Settings      |                 |           |                        | Cancel |
| CLI Overrides              |                 |           |                        |        |

#### Figure 97 Configure > Ethernet Ports

- 2. Go to CONFIGURE > MASTER AP CONFIG > Networks and configure the Static IP Address and the DHCP Server for VLAN1 (native VLAN).
- 3. Enable DHCP Server and provide range of IP addresses. For example, when starting address range is give as 10.10.10.20 to 10.10.10.200, IP addresses can be assigned from 10.10.10.20 to 10.10.10.200 range.

| Camblum Networks DASHBOARD | 🔍 🦄 INSIGHT 🌩 CONFIGURI   | e 🞯 Manage  | Ť   | LOGOUT |
|----------------------------|---------------------------|---|---|--------|
| Configuration              | Edit Interface - VLAN 50  |   |   |        |
| System<br>Management       | IP CONFIGURATION          |   |   |        |
| Wireless LANs              | VLAN ID                   | 10  |   |        |
| Radios                     | Address Mode              | Static  |   |        |
| MASTER-AP CONFIG           | Available in member APs   | Enable this VLAN on all member Access Points                |   |        |
| IP Settings                | Static IP Address         | 10.10.10.10   |   |        |
| Networks                   | Network Mask              | 255.255.255.0   |   |        |
| NETWORK                    | Enable Nat                | When NAT is enabled, IP addresses under this SVI are hidden |   |        |
| Ethernet Ports<br>Firewall | Enable DHCP Server        | Enable DHCP server for this interface     Ena               | ble this option to configure DHCP                           |        |
| Tunnels                    |                           |   |   |        |
| OVERRIDES                  | DHCP SERVER CONFIGURATION |   |   |        |
| Access Point Settings      | Starting Address Range    | 10.10.10.20   |   |        |
| CLI Overrides              | Ending Address Range      | 10.10.10.200  |   |        |
|                            | Network IP Address        | 10.10.10.0  |   |        |
|                            | Network Mask              | 255.255.255.0   |   |        |
|                            | ROUTING AND DNS           |   |   |        |
|                            | Default gateway           | 10.10.10.1  | This should be the IP address of NAT device in your network |        |
|                            | Domain Name               | CAMNWK  |   |        |
|                            | Primary DNS server        | 208.69.38.205   | Edit these fields as per the DNS server of ISP              |        |
|                            | secondary DNS server      | 4.2.2.2   | -   |        |
|                            |                           |   |   |        |
|                            |                           |   | Cancel  | Save   |

#### Figure 98 Configure > Networks

- **4.** DHCP pool is used to provide IP addresses to all devices on VLAN 1. Add L3 interface of VLAN 10 and 20 under **CONFIGURE > Networks**.
  - a. Enable **NAT** in this L3 interface.
  - b. Enable **DHCP server** for this VLAN L3 interface.
  - c. Default gateway needs to be Static IP Address of the L3 interface.

| Cambium Networks DASHBOARD | 🔍 🦄 INSIGHT 🔹 C        | CONFIGURE | ☞ MANAGE  | ₽ LOGOUT                |
|----------------------------|------------------------|-----------|---|-------------------------|
| Configuration              | Edit Interface - VLAN  | N 50      |   |                         |
| System<br>Management       | IP CONFIGURATION       |           |   |                         |
| Wireless LANs              | VLAN ID                |           | 10  |                         |
| Radios                     | Address Mode           |           | Static •  |                         |
| MASTER-AP CONFIG           | Available in member AF | NPs       | Enable this VLAN on all member Access Points                |                         |
| IP Settings                | Static IP Address      |           | 192.168.10.1  |                         |
| Networks                   | Network Mask           |           | 255.255.2   |                         |
| NETWORK<br>Ethernet Ports  | Enable Nat             | æ         | When NAT is enabled, IP addresses under this SVI are hidden | NAT                     |
| Firewall                   | Enable DHCP Server     |           | Enable DHCP server for this interface                       | DHCP Server             |
| Tunnels                    | DHCP SERVER CONFIGU    |           |   |                         |
| OVERRIDES                  | Starting Address Range |           | 198.168.10.10   |                         |
| Access Point Settings      | Ending Address Range   |           | 192.168.10.240  |                         |
| CLI Overrides              | Network IP Address     |           | 192.168.10.0  |                         |
|                            | Network Mask           |           | 255.255.255.0   |                         |
|                            | ROUTING AND DNS        |           | 200,200,200,0   |                         |
|                            | Default gateway        |           | 192.168.10.1 Static IF                                      | Address of L3 interface |
|                            | Domain Name            |           | CAMNWK  |                         |
|                            | Primary DNS server     |           | 208.69.38.205   | address provided by ISP |
|                            | secondary DNS server   |           | 10.10.10.1  | nuless provided by ISP  |
|                            |                        |           |   |                         |
|                            |                        |           |   | Cancel Save             |

Figure 99 Configure > Networks > VLAN 10

5. Add L3 interface of VLAN 20 and enable DHCP server and NAT as shown in Figure 100.

| Cambium Networks* DASHBOARD            | 💐 INSIGHT         |              | ♥ MANAGE  | P LOGOL     | υτ |
|--|-------------------|--------------|---|-------------|----|
| Configuration                          | Edit Interface -  |              |   |             |    |
| System                                 | Eur menace -      | VLAN 50      |   |             |    |
| Management                             | IP CONFIGURATI    | ON           |   |             |    |
| Wireless LANs                          | VLAN ID           |              | 20  |             |    |
| Radios                                 | Address Mode      |              | Static •  |             |    |
| MASTER-AP CONFIG                       | Available in mer  | nber APs     | Enable this VLAN on all member Access Points                |             |    |
| IP Settings                            | Static IP Address | 5            | 192.168.20.1  |             |    |
| Networks                               | Network Mask      |              | 255.255.255.0   |             |    |
| NETWORK                                | Enable Nat        |              | When NAT is enabled, IP addresses under this SVI are hidden |             |    |
| Ethernet Ports                         |                   |              |   |             |    |
| Firewall                               | Enable DHCP Se    | rver a       | Enable DHCP server for this interface                       |             |    |
| Tunnels                                | DHCP SERVER CO    | ONFIGURATION |   |             |    |
| OVERRIDES                              | Starting Address  | s Range      | 198.168.20.10   |             |    |
| Access Point Settings<br>CLI Overrides | Ending Address    | Range        | 192.168.20.200  |             |    |
|  | Network IP Addr   | ress         | 192.168.20.0  |             |    |
|  | Network Mask      |              | 255.255.255.0   |             |    |
|  | ROUTING AND D     | INS          |   |             |    |
|  | Default gateway   |              | 192.168.20.1  |             |    |
|  | Domain Name       |              | CAMNWK  |             |    |
|  | Primary DNS ser   | rver         | 208.69.38.205   |             |    |
|  | secondary DNS     | server       | 4.2.2.2   |             |    |
|  |                   |              |   |             |    |
|  |                   |              |   | Cancel Save |    |

#### Figure 100 Configure > Networks > VLAN 20

### Configuring an AP with External DHCP Server

#### Network Topology

Initial network installments with external DHCP server and NAT box. The complete network is connected to VLAN 1.



Figure 101 Configuring an AP with External DHCP server

All the member APs are connected to ports of Switch. All the ports are mapped to VLAN 1.

To configure Master AP:

1. Configure country code, ntp server in master AP under System.

#### Figure 102 Configure > Systems

| Cambium Networks" DASHBOAR  | d 🍕 insight   |         | S MANAGE   |     | Digout   |
|-----------------------------|---------------|---------|--|-----|----------|
| 🌣 Configuration             |               |         |  |     |          |
| Configuration               | System        |         |  |     |          |
| System                      | BASIC CONFIGU | JRATION |  |     |          |
| Management<br>Wireless LANs | Admin Passwo  | rd      |  | Ð   |          |
| Radios                      | Country Code  |         | India  | •   |          |
| MASTER-AP CONFIG            | PoE Output    |         | Off  | •   |          |
| IP Settings<br>Networks     | LED           |         | <ul> <li>Turn on device LEDs during operation</li> </ul> |     |          |
| NETWORK                     | LLDP          |         | Turn on LLDP transmission                                |     |          |
| Ethernet Ports              | TIME SETTINGS |         |  |     |          |
| Firewall                    | NTP Server 1  |         | time1.ntp.com  |     |          |
| Tunnels                     | NTP Server 2  |         | time2.ntp.com  |     |          |
| Access Point Settings       | Timezone      |         | Asia/Bengaluru   | •   |          |
| CLI Overrides               |               |         |  |     | _        |
|                             |               |         |  | Can | cel Save |

2. Configure static IP on Master.

| Cambium Networks                                | DASHBOARD | 🍕 INSIGHT        |         | S MANAGE  |  | 🖡 LOGOUT |
|---|-----------|------------------|---------|---|--|----------|
| Configuration                                   |           |                  |         |   |  |          |
| Configuration                                   |           | Master IP Sett   | ings    |   |  |          |
| System<br>Management<br>Wireless LANs<br>Radios |           | i                |         | Please note when the IP address or mode is ch               | <b>de change</b><br>nanged, you may lose connectivity to this session.<br>gin if you decide to change mode / IP address. |          |
| MASTER-AP CONFIG                                |           | Address Mode     |         | Static  |  |          |
| IP Settings                                     |           | Static IP Addres | s       | 10.10.0.20  |  |          |
| Networks  |           | Network Mask     |         | 255.255.255.0   |  |          |
| NETWORK   |           |                  |         |   |  |          |
| Ethernet Ports                                  |           | Default Gatewa   | у       | 10.10.0.1   |  |          |
| Firewall  |           | Domain Name      |         | CAMNWK  |  |          |
| Tunnels   |           | DNS Server 1     |         | 10.110.12.110   |  |          |
| OVERRIDES                                       |           | DNS Server 2     |         | 10.110.12.111   |  |          |
| Access Point Settin                             | gs        |                  |         |   |  |          |
| CLI Overrides                                   |           | Enable Nat       | 6       | When NAT is enabled, IP addresses under this SVI are hidden |  |          |
|   |           | Enable DHCP Se   | erver E | Enable DHCP server for this interface                       |  |          |

#### Figure 103 Configure > IP Settings

3. Refresh the page after saving with newly configured Ip address. In this example, open URL in browser http://10.10.10.25.

### Configuring WLAN in default WLAN Group

To configure WLAN in default WLAN group:

1. Add a Wireless LAN.

| Cambium Networks*    | DASHBOARD | 🂐 INSIGHT          |               | S MANAGE        |       |      | 🗗 LOGOU                |
|----------------------|-----------|--------------------|---------------|-----------------|-------|------|------------------------|
| Configuration        |           |                    |               |                 |       |      |                        |
| Configuration        |           | Wireless LANs      | 5             |                 |       |      | WLAN Group Default 🔹 📋 |
| System               |           | SSID/NAME          |               | SECURITY        | GUEST | VLAN | ACTIONS                |
| Management           |           | Auto_pilot_8       |               | open            | ✓     | 1    | 🖉 EDIT 📋 DELETE        |
| Wireless LANs        |           | Auto_pilot_4       |               | open            | ×     | 50   | 🖉 EDIT 📋 DELETE        |
| Radios               |           | Auto_pilot_1       |               | wpa2-enterprise | ×     | 1    | 🖉 EDIT 📋 DELETE        |
| MASTER-AP CONFIG     |           | of 16 Wireless LAN | Is configured |                 |       |      | + Add Wireless LAN     |
| IP Settings          |           |                    |               |                 |       |      |                        |
| Networks             |           |                    |               |                 |       |      |                        |
| NETWORK              |           |                    |               |                 |       |      |                        |
| Ethernet Ports       |           |                    |               |                 |       |      |                        |
| Firewall             |           |                    |               |                 |       |      |                        |
| Tunnels              |           |                    |               |                 |       |      |                        |
| OVERRIDES            |           |                    |               |                 |       |      |                        |
| Access Point Setting | ţs        |                    |               |                 |       |      |                        |
|                      |           |                    |               |                 |       |      |                        |

#### Figure 104 Configure > Wireless LANs

2. Enter **SSID** and password in respective fields.

3. Configure VLAN as 10 and click Save.

| 🜔 Cam | bium Networks"      | DASHBOARD | 💐 INSIGHT     |                   | 👁 MANAGE                    |                  |   |
|-------|---------------------|-----------|---------------|-------------------|-----------------------------|------------------|---|
| X Co  | onfiguration        |           |               |                   |                             |                  |   |
| Co    | onfiguration        |           | Wireless LAN  | s                 |                             |                  |   |
|       | ystem<br>lanagement |           | EDIT WIRELESS | LAN - AUTO_PILOT_ | _8                          |                  |   |
|       | /ireless LANs       |           | Basic         | Guest Access      | Usage Limits Access Control | Scheduled Access |   |
| Ra    | adios               |           | Name / SSID   |                   | member-10                   |                  |   |
| M     | ASTER-AP CONFIG     |           | Enable        |                   | Enable this Wireless LAN    |                  |   |
|       | Settings            |           | Band          |                   | 2.4GHz & 5GHz               |                  | • |
|       | etworks             |           | Security      |                   | WPA2 Pre-shared Key         |                  | ٠ |
|       | ETWORK              |           | Passphrase    |                   |                             |                  | ٩ |
| Fi    | rewall              |           | VLAN          |                   | 10                          |                  |   |
| τι    | unnels              |           | Guest Access  |                   | ✓ Use WLAN for guest access |                  |   |
| 0\    | VERRIDES            |           | ADVANCED SE   | ETTINGS ③         |                             |                  |   |
|       | ccess Point Setting | gs        |               |                   |                             |                  |   |
| CL    | LI Overrides        |           |               |                   |                             |                  |   |

Figure 105 Configure > Wireless LANs > VLAN 10

- 4. Add another WLAN with VLAN 20. Enter **SSID** and password as required.
- 5. Configure VLAN as 20 and click **Save**.

| Cambium Networks"           | DASHBOARD | 💐 INSIGHT       |                  | © MANAGE                                     | LOGOUT  |
|-----------------------------|-----------|-----------------|------------------|--|---------|
| Configuration               |           |                 |                  |  |         |
| Configuration               |           | Wireless LANs   |                  |  |         |
| System                      |           | EDIT WIRELESS I | AN - AUTO_PILOT_ | 8  |         |
| Management<br>Wireless LANs |           | Basic           | Guest Access     | Usage Limits Access Control Scheduled Access |         |
| Radios                      |           | Name / SSID     |                  | member-20                                    |         |
| MASTER-AP CONFIG            |           | Enable          |                  | C Enable this Wireless LAN                   |         |
| IP Settings<br>Networks     |           | Band            |                  | 2.4GHz & 5GHz •                              |         |
| NETWORK                     |           | Security        |                  | WPA2 Pre-shared Key                          |         |
| Ethernet Ports              |           | Passphrase      |                  |  |         |
| Firewall                    |           | VLAN            |                  | 20   |         |
| Tunnels                     |           | Guest Access    |                  | Use WLAN for guest access                    |         |
| OVERRIDES                   |           | ADVANCED SE     | TTINGS 🕥         |  |         |
| Access Point Setting        | s         |                 |                  |  |         |
| CLI Overrides               |           |                 |                  | Cance  | el Save |

6. Check the configured WLANs.

| Cambium Networks 🛛 📮 DASH                              | HBOARD 🍕 INSIGHT 🔅        | CONFIGURE S MANAGE |       |          | ₽ LOGOUT                |
|--|---------------------------|--------------------|-------|----------|-------------------------|
| Configuration  |                           |                    |       |          |                         |
| Configuration  | Wireless LANs             |                    |       | WLAN G   | roup member_grp • + 🖉 📋 |
| System   | SSID/NAME                 | SECURITY           | GUEST | VLAN     | ACTIONS                 |
| Management   | member-10                 | wpa2-psk           | ×     | 10       | 🖉 EDIT 🗎 DELETE         |
| Wireless LANs  | member-20                 | wpa2-psk           | ×     | 20       | 🖉 EDIT 📋 DELETE         |
|  | 2 of 16 Wireless LANs cor | nfigured           |       |          | + Add Wireless LAN      |
| MASTER-AP CONFIG<br>IP Settings<br>Networks<br>NETWORK |                           |                    |       | ×        |                         |
| IP Settings<br>Networks<br>NETWORK<br>Ethernet Ports   |                           |                    |       | alitica. |                         |
| IP Settings<br>Networks<br>NETWORK                     |                           |                    |       |          |                         |

Figure 107 Configure > Wireless LANs > VLAN 10 and 20

7. Connect member APs to the Switch. The connected member APs receive IP from IP address from Master AP on VLAN 1. Once the member APs connect to the Master AP and they are approved, the configured WLANs are pushed to all the approved member APs and Master AP.

Figure 108 Dashboard

| OVERVIEW      | (+) ACCESS POINTS    |  |  |                            |                                     |               |  |                              |   |
|---------------|----------------------|--|--|----------------------------|-------------------------------------|---------------|--|------------------------------|---|
| LIENTS        | 4GHz — 5GHz — Total  |  |  | THROUGHPUT                 | TX — RX                             |               | SITE INFORMATION   |                              |   |
| 30            | -4GH2 - 5GH2 - 10tal |  | BO MI  |                            |                                     |               | 6<br>APS CONFIGURED  | 3<br>APS ONLINE              | 30<br>CLIENTS   |
| 10            |                      |  | 20 M   |                            |                                     |               | DISCOVERED DEVICES   | approve here                 | Approve Al  |
| 0             |                      |  |  | bos                        |                                     |               | NAME   | IP 🔨                         | ACTIONS   |
| 2:24:30 12:25 | 12:25:30             | 12:26 12:26                                  |  | 12:24:30 12:25             | 12:25:30 12:26 1.                   | 2:26:30 12:27 | E400-B5AD58  | 10.10.10.169                 | APPROVI   |
|               |                      |  |  |                            |                                     |               |  |                              |   |
|               |                      |  |  |                            |                                     |               | mesh-client1-E410-93F18A   | 10.10.10.130                 | V APPROV  |
| OP APS        | Clients Tra          | affic TOP CLIE                               | ENTS   |                            | CLIENTS BY RADIO TYPE               | Band Radio    | mesh-client1-E410-93F18A<br>mesh-base1-E410-93F185                                     | 10.10.10.130<br>10.10.10.137 |   |
| DP APS        | L'andre La           |  | ENTS<br>16-00-00-04                                      | 1 Mbps                     | CLIENTS BY RADIO TYPE               | Band Radio    |  |                              | V APPROV  |
| 1             | L'andre La           | 02-00-4                                      | 1  | 1 Mbps                     |                                     | Band Radio    | mesh-base1-E410-93F185   | 10.10.10.137                 | V APPROVI   |
| 1             | L'andre La           | 02-00-41<br>02-00-41                         | 6-00-00-04   |                            | CLIENTS BY RADIO TYPE<br>RADIO TYPE | Band Radio    | mesh-base1-E410-93F185<br>mesh-client2-E410-93F19F<br>EVENTS                           | 10.10.10.137                 | APPROVI     APPROVI     APPROVI     APPROVI     Filter Ever     |
| E400-B5B05A 0 | L'andre La           | 02-00-41<br>02-00-41<br>02-00-41             | 16-00-00-04  | 1 Mbps                     |                                     | Band Radio    | mesh-base1-E410-93F185<br>mesh-client2-E410-93F19F<br>EVENTS                           | 10.10.10.137                 | <ul><li>✓ APPROVI</li><li>✓ APPROVI</li><li>✓ APPROVI</li></ul> |
| E500-917722   | L'andre La           | 02-00-41<br>02-00-41<br>02-00-41<br>02-00-41 | 16-00-00-04<br>16-00-00-18                               | 1 Mbps<br>1 Mbps           |                                     |               | mesh-base1-E410-93F185<br>mesh-client2-E410-93F19F<br>EVENTS                           | 10.10.10.137                 | <ul><li>✓ APPROV</li><li>✓ APPROV</li></ul>                     |
| E500-917722   | 3                    | 02-00-41<br>02-00-41<br>02-00-41<br>02-00-41 | 16-00-00-04<br>16-00-00-18<br>16-00-00-00<br>16-00-00-02 | 1 Mbps<br>1 Mbps<br>1 Mbps | RADIO TYPE                          |               | mesh-base1-E410-93F185<br>mesh-client2-E410-93F19F<br>EVENTS<br>O AUTOPILOT-AP-CONNECT | 10.10.10.137                 | APPROVI     APPROVI     Filter Even                             |

### Configuring WLANs with user created WLAN Group

User can group one or multiple WLANs under a WLAN group and push the configuration to specific APs. WLAN group is used to push specific WLANs to specific selected APs.

1. Create a WLAN group.

| Cambium Networks" | DASHBOARD | 💐 INSIGHT          | CONFIGURE    | ♥ MANAGE |            |                    | Logou                    |
|-------------------|-----------|--------------------|--------------|----------|------------|--------------------|--------------------------|
| Configuration     |           |                    |              |          | click here | e to create new Wl | an group                 |
| Configuration     |           | Wireless LANs      |              |          |            |                    | WLAN Group Default 🔻 🕂 📋 |
| System            |           | SSID/NAME          |              | SECURITY | GUEST      | VLAN               | Default<br>ACTIONS       |
| Management        |           | wlan_release123    |              | wpa2-psk | ×          | 1                  |                          |
| Wireless LANs     |           | wlan4              |              | wpa2-psk | ×          | 1                  | 🖉 EDIT 📋 DELETE          |
| Radios            | 2         | of 16 Wireless LAN | s configured |          |            |                    |                          |
| MASTER-AP CONFIG  |           |                    |              |          |            |                    | + Add Wireless LAN       |
| IP Settings       |           |                    |              |          |            |                    |                          |
| Networks          |           |                    |              |          |            |                    |                          |
| NETWORK           |           |                    |              |          |            |                    |                          |
| Ethernet Ports    |           |                    |              |          |            |                    |                          |
| Tunnels           |           |                    |              |          |            |                    |                          |
| OVERRIDES         |           |                    |              |          |            |                    |                          |
|                   | s         |                    |              |          |            |                    |                          |

#### Figure 109 Create a WLAN group

2. Configure a new WLAN Group.

| Figure 110 Configure a new | WLAN Group |
|----------------------------|------------|
|----------------------------|------------|

| Cambium Networks*           | DASHBOARD | 💐 INSIGHT    | CONFIGURE | MANAGE |  |  | 🕞 LOGOUT      |
|-----------------------------|-----------|--------------|-----------|--------|--|--|---------------|
| Configuration               | 1         |              |           |        |  |  |               |
| Configuration               |           | WLAN Group   |           |        |  |  |               |
| System                      |           | ADD WLAN GRO | UP        |        |  |  |               |
| Management<br>Wireless LANs |           | Group Name   |           | group1 |  |  |               |
| Radios                      |           |              | 7         |        |  |  |               |
| MASTER-AP CONFIG            | configur  | e group na   | ime       |        |  |  | Cancel Save   |
| IP Settings                 |           | 0 0          |           |        |  |  | 1             |
| Networks                    |           |              |           |        |  |  |               |
| NETWORK                     |           |              |           |        |  |  | click on save |
| Ethernet Ports              |           |              |           |        |  |  |               |
| Tunnels                     |           |              |           |        |  |  |               |
| OVERRIDES                   |           |              |           |        |  |  |               |
| Access Point Setti          | ngs       |              |           |        |  |  |               |
| CLI Overrides               |           |              |           |        |  |  |               |

3. Configure WLAN under the newly created WLAN Group.

| Cambium Networks" DASHBOAI | RD 💐 INSIGHT 🌻 CONFIGURE 🚱 MANAGE  |                 |       |      | 🔁 LOG                   |
|----------------------------|------------------------------------|-----------------|-------|------|-------------------------|
| Configuration              |                                    |                 |       |      |                         |
| Configuration              | Wireless LANs                      |                 |       |      | WLAN Group group1 🔻 + 🖉 |
| System                     | SSID/NAME                          | SECURITY        | GUEST | VLAN | ACTIONS                 |
| Management                 | new-wlan                           | wpa2-enterprise | ×     | 1    | 🖉 EDIT 📋 DELETE         |
| Wireless LANs              | 1 of 16 Wireless LANs configured   |                 |       |      |                         |
| Radios                     | T of TO WILEIESS LIVINS CONTIGUIED |                 |       |      | + Add Wireless L        |
| MASTER-AP CONFIG           |                                    |                 |       |      |                         |
| P Settings                 |                                    |                 |       |      |                         |
| ietworks                   |                                    |                 |       |      |                         |
| IETWORK                    |                                    |                 |       |      |                         |
| thernet Ports              |                                    |                 |       |      |                         |
| lunnels                    |                                    |                 |       |      |                         |
| DVERRIDES                  |                                    |                 |       |      |                         |
| Access Point Settings      |                                    |                 |       |      |                         |
| CLI Overrides              |                                    |                 |       |      |                         |
|                            |                                    |                 |       |      |                         |
|                            |                                    |                 |       |      |                         |
|                            |                                    |                 |       |      |                         |
|                            |                                    |                 |       |      |                         |
|                            |                                    |                 |       |      |                         |

#### Figure 111 Configure WLAN under the newly created WLAN Group

### WLAN group override

This section is to describe how user can select device and configure user configured WLAN-group. By selecting device and overriding their WLAN-group, specific WLANs can be pushed to selected devices.

1. Select the device and click **Edit** button.

#### Figure 112 Configure > Access Point settings

| Cambium Networks 🛛 📮 DASH | BOARD 🌂 INSIGHT | CONFIGURE | S MANAGE          |            | P LOGO          |
|---------------------------|-----------------|-----------|-------------------|------------|-----------------|
| Configuration             |                 |           |                   |            |                 |
| Configuration             | Access Point    | Settings  |                   |            | Filter          |
| System                    | NAME            |           | MAC               | IP         | ACTIONS         |
| Management                | E500-9F33F0 🍲   |           | 00-04-56-9F-33-F0 | 10.10.0.20 | Ø EDIT          |
| Wireless LANs             | E400-B16F48     |           | 00-04-56-B1-6F-48 | 10.10.0.4  | 🖉 EDIT 📋 DELETE |
| Radios                    | E400-B16F48     |           | 00-04-56-B1-6F-48 | 10.10.0.4  | 🖉 EDIT 📋 DELETE |
| MASTER-AP CONFIG          | E400-B558D2     |           | 00+04+56+B5+58-D2 | 10.10.0.5  | 🖉 EDIT 📋 DELETE |
| IP Settings               |                 |           |                   |            |                 |
| Networks                  |                 |           |                   |            |                 |
| NETWORK                   |                 |           |                   |            |                 |
| Ethernet Ports            |                 |           |                   |            |                 |
| Firewall                  |                 |           |                   |            |                 |
| Tunnels                   |                 |           |                   |            |                 |
| OVERRIDES                 |                 |           |                   |            |                 |
| Access Point Settings     |                 |           |                   |            |                 |
| CLI Overrides             |                 |           |                   |            |                 |

2. Choose the WLAN-group you had configured from the drop-down list and click **Save** button. This will push the WLANs configured under **group1** to the selected AP.

| Cambium Networks            | DASHBOARD | 🂐 INSIGHT      |                    | ☞ MANAGE            |        | 🖟 logo |
|-----------------------------|-----------|----------------|--------------------|---------------------|--------|--------|
| Configuration               |           |                |                    |                     |        |        |
| Configuration               |           | Access Point S | Settings - 00-04-5 | 6-9F-33-F0          |        |        |
| System                      |           | BASIC CONFIGU  | -                  |                     |        |        |
| Management<br>Wireless LANs |           | Name           |                    | member2-E600-96616C |        |        |
| Radios                      |           | Location       |                    | Location            |        |        |
| MASTER-AP CONFIG            |           | WLAN Group     |                    | Default             |        |        |
| IP Settings<br>Networks     |           | RADIO CONFIGU  | JRATION            | group1              | •      |        |
| NETWORK                     |           | 2.4GHz Channe  | 4                  | Don't Override      | •      |        |
| Ethernet Ports              |           | 2.4GHz Power   |                    | Don't Override      | •      |        |
| Firewall                    |           | 5GHz Channel   |                    | Don't Override      |        |        |
| OVERRIDES                   |           | 5GHz Power     |                    | Don't Override      |        |        |
| Access Point Settings       |           |                |                    |                     |        |        |
| CLI Overrides               |           |                |                    |                     | Cancel | Sav    |

Figure 113 Configure > Access Point settings > WLAN Group

### Configuring WPA2-Enterprise WLAN

Follow the below steps to create a WLAN with Enterprise security under user created WLAN Group.

| <ul> <li>Configuration</li> <li>Configuration</li> <li>System</li> <li>System</li> <li>SSDMAME</li> <li>SECURITY</li> <li>GUEST</li> <li>VLAN</li> <li>ACTIONS</li> </ul> |
|---|
| System SSID/NAME SECURITY GUEST VLAN ACTIONS Management Wireless LANs   |
| Management Wireless LANs  |
| Wireless LANs   |
| Wineless LMIs   |
| 1 of 16 Wreless LAks configured   |
| T AUD WIERESS DAW   |
| NACES AF COURS  |
| P Settings  |
| Networks  |
| NETHORK   |
| Ethernet Ports  |
| Tunnels   |
| O GRADES  |
| Access Point Settings   |
| CU Divendes   |
|   |
|   |
|   |
|   |

Figure 114 Configure > Access Point settings > user created WLAN Group

1. Enter details in the WLAN page.

- 2. Select **Security** as **WPA2-Enterprise** from the drop-down list.
- 3. Keep VLAN as 1.
- 4. Do not press **Save** button before configuring Radius configurations for authentication.

| ٢ | Cambium Networks"    | DASHBOARD | 🍕 INSIGHT     | CONFIGURE         | 𝚱 MANAGE                            | ₽ LOGOUT |
|---|----------------------|-----------|---------------|-------------------|-------------------------------------|----------|
| ٥ | Configuration        |           |               |                   |                                     |          |
|   | Configuration        |           | Wireless LANs | 5                 |                                     |          |
|   | System               |           |               |                   |                                     |          |
|   | Management           |           | EDIT WIRELESS | LAN - AUTO_PILOT_ | 8                                   |          |
| 1 | Wireless LANs        |           | Basic         | Usage Limits      | Access Control Scheduled Access     |          |
|   | Radios               |           | Name / SSID   |                   | Auto_pilot_8                        |          |
|   | MASTER-AP CONFIG     |           | Enable        | 6                 | Enable this Wireless LAN            |          |
|   | IP Settings          |           |               |                   | 2 46H7 & 56H7                       |          |
|   | Networks             |           | Band          |                   | 2.4GHz & 5GHz                       |          |
|   | NETWORK              |           | Security      |                   | Open ·                              |          |
|   | Ethernet Ports       |           | VLAN          |                   | WPA2 Pre-shared Key WPA2 Enterprise |          |
|   | Firewall             |           | Guest Access  | (                 | Use WLAN for guest access           |          |
|   | Tunnels              |           | ADVANCED SE   | TTINGS ③          |                                     |          |
|   | OVERRIDES            |           |               |                   |                                     |          |
|   | Access Point Setting | s         |               |                   | Canc                                | el Save  |
|   | CLI Overrides        |           |               |                   |                                     |          |

Figure 115 Configure > Wireless LANs > Security

5. Configure **Radius Server** details for Authentication and for Accounting if applicable. Authentication server details has to be filled before saving the WLAN configuration.

| ¢ | Cambium Networks"    | DASHBOARD  | 💐 INSIGHT       |                 | S MANAGE                  |                          |              |              |  | ₽ LOGOUT    |
|---|----------------------|------------|-----------------|-----------------|---------------------------|--------------------------|--------------|--------------|--|-------------|
| ¢ | Configuration        |            |                 |                 |                           |                          |              |              |  |             |
|   | Configuration        |            | Wireless LANs   |                 |                           |                          |              |              |  |             |
|   | System<br>Management |            | EDIT WIRELESS I | AN - AUTO_PILOT | _8                        |                          |              |              |  |             |
|   | Wireless LANs        |            | Basic           | Guest Access    | Radius Server Usag        | e Limits Access C        | ontrol Sched | luled Access |  |             |
|   | Radios               |            | Authentication  | Server          | IP address / Domain       | Secret                   | Port         | Realm        |  |             |
|   | MASTER-AP CONFIG     |            |                 |                 | 1. 10.10.10.145           |                          | 1812         | Realm        |  |             |
|   | IP Settings          |            |                 |                 | 2. IP address / Domain    | Secret                   | 1812         | Realm        |  |             |
|   | Networks             |            |                 |                 | 3. IP address / Domain    | Secret                   | 1812         | Realm        |  |             |
|   | NETWORK              |            |                 |                 | IP address / Domain       | Secret                   | Port         |              |  |             |
|   | Ethernet Ports       |            | Accounting Serv |                 | 1. 10.10.10.145           | Secret                   | 1813         |              |  |             |
|   | Firewall             |            |                 |                 | 2. IP address / Domain    | Secret                   | 1813         |              |  |             |
|   | Tunnels              |            |                 |                 | 3. IP address / Domain    | Secret                   | 1813         |              |  |             |
|   | OVERRIDES            |            |                 |                 |                           |                          |              |              |  |             |
|   | Access Point Setting | <u>g</u> s | ADVANCED SET    | rtings ⊙        |                           |                          |              |              |  |             |
|   | CLI Overrides        |            | NAS Identifier  |                 | NAS-ID for use in request | packets. Defaults to sy  | stem name    |              |  |             |
|   |                      |            | Accounting Atte | mpts            | 1                         |                          |              |              |  |             |
|   |                      |            | Interim Update  | Interval        | 1800                      |                          |              |              |  |             |
|   |                      |            | Accounting Mod  | le              | start-interim-stop        |                          | •            |              |  |             |
|   |                      |            | Server Pool Moo | ie              | Load Balance              |                          | •            |              |  |             |
|   |                      |            | Dynamic Author  | ization         | Enable RADIUS dynamic     | authorization (COA, DM n | nessages)    |              |  |             |
|   |                      |            | Dynamic VLAN    |                 | Enable RADIUS assigned    | VLANs                    |              |              |  |             |
|   |                      |            |                 |                 |                           |                          |              |              |  | Cancel Save |

#### Figure 116 Configure > Wireless LANs > Radius Server

### Onboard member APs to Autopilot master

To onboard other member APs to Autopilot Master:

- 1. Access the Autopilot Master AP via web browser.
- 2. Login with the below credentials:
  - Username: admin
  - Password: admin

| Figure | 117 | Login | page |
|--------|-----|-------|------|
|--------|-----|-------|------|

| Sign in to your account |
|-------------------------|
| admin                   |
| · ·····                 |
| Sign in 🚽               |
| Signin 1                |

3. Go to the **DASHBOARD** tab of the Master AP which displays the list of member APs those have discovered the Master AP.



4. Click **APPROVE** to approve and manage the desired member AP or click **APPROVE ALL** to approve and manage all the listed APs.

| Cambium Networks"   | DASHBOARD           | 4 INSIGHT O CONFIGUR                  | e 🥪 MANAGE       |                       |                |                          |  | ₽ LOGOUT                            |
|---------------------|---------------------|---------------------------------------|------------------|-----------------------|----------------|--------------------------|--|-------------------------------------|
| Ø OVERVIEW          | ACCESS POINTS       | WIRELESS CLIENTS                      |                  |                       |                |                          |  |                                     |
| CLIENTS             |                     |                                       | THROUGHPUT       |                       |                | SITE INFORMATION         |  |                                     |
| 30                  | AGHz — 5GHz — Total |                                       | 30 Mbps          |                       |                | 6<br>APS CONFIGURED      | 3<br>APS ONLINE  | 30<br>CLIENTS                       |
| 10                  |                     |                                       | 20 Mbps          |                       |                | DISCOVERED DEVICES       | approve here   | Approve All                         |
| 0                   |                     |                                       | 0 bps            |                       |                | NAME                     | 19 🔨   | ACTIONS                             |
| 12:24:30 12:25      | 12:25:30            | 12:26 12:26:30 12:2                   |                  | 12:25:30 12:26        | 12:26:30 12:27 | E400-85AD58              | 10.10.10.169   | APPROVE                             |
|                     |                     |                                       |                  |                       |                | mesh-client1-E410-93F18A | 10.10.10.130   | ✓ APPROVE                           |
| TOP APS             | Clients Tra         | ffic TOP CLIENTS                      |                  | CLIENTS BY RADIO TYPE | Band Radio     | mesh-base1-E410-93F185   | 10.10.137  | V APPROVE                           |
| E500-917722         | 3                   | 0 02-00-46-00-00-04 02-00-46-00-00-18 | 1 Mbps           |                       |                | mesh-client2-E410-93F19F | 10.10.136  | APPROVE                             |
| E400-85805A 0       |                     | 02-00-46-00-00-00                     | 1 Mbps           | RADIO 1               | TYPE           | EVENTS                   | wents  | Filter Events                       |
| E410-93F1AD 0       |                     | 02-00-46-00-00-02                     | 1 Mbps<br>1 Mbps | ■ A ■ B ■ G           | N AC           |                          | wents  |                                     |
| -                   |                     | -                                     |                  |                       |                |                          | ED: Access Point [E500-917722] N<br>ected to Autopilot Master-AP | AC Jun 28, 12:27:35<br>E500-917722  |
| CHANNEL DISTRIBUTIC | N                   |                                       |                  |                       |                |                          | ED: Access Point [E400-B5AEFC] N<br>ected to Autopilot Master-AP | MAC Jun 28, 12:27:29<br>E500-917722 |

#### Figure 118 Dashboard > Overview

5. The approved member APs are listed under **DASHBOARD** > **ACCESS POINTS** tab.

#### Figure 119 Dashboard > Access points

| Cambium Networks     | I DASHBOARD 🦄 INSIGHT 🔹 CO    | ONFIGURE 🧇 MANAGE |              |         |            |         | LOGOUT   |
|----------------------|-------------------------------|-------------------|--------------|---------|------------|---------|----------|
| @ OVERVIEW (*) AC    | CESS POINTS 🗇 WIRELESS CLIENT | rs.               |              |         |            |         |          |
| Overview Performance | System RF Stats               | Approved APs are  | listed here. |         |            |         | Search 🛛 |
| IAME                 | MAC                           | IP ADDRESS        | MODEL        | CLIENTS | POWER      | CHANNEL | STATE    |
| 400-B5AD58           | 00-04-56-B5-AD-58             | 10.10.169         | cnPilot E400 | 0       | 25, 20 dBm | 1, 100  | ON, ON   |
| 400-AF0782           | 00-04-56-AF-07-82             | 10.10.141         | cnPilot E400 | 0       | 25, 24 dBm | 1, 144  | ON, ON   |
| 500-917722           | 00-04-56-91-77-22             | 10.10.165         | cnPilot ES00 | 2       | 29, 24 dBm | 1, 48   | ON, ON   |
| 400-B5B05A           | 00-04-56-85-80-5A             | 10.10.166         | cnPilot E400 | 0       | 25, 14 dBm | 1, 44   | ON, ON   |
| 400-B5AD58 🍲         | 00-04-56-B1-6C-D0             | 10.10.10.41       | cnPilot E400 | 0       | 25, 24 dBm | 1, 100  | ON, DFS  |
| 400-B5AEFC           | 00-04-56-B5-AE-FC             | 10.10.167         | cnPilot E400 | 0       | 25, 14 dBm | 6, 48   | ON, ON   |
| 410-93F1AD           | 00-04-56-93-F1-AD             | 10.10.138         | cnPilot E410 | 0       | dBm        |         | 2        |

### Connect clients to the WLANs and check statistics

#### 1. Go to DASHBOARD > WIRELESS CLIENTS.

2. Connect the listed clients to the configured WLANs and check statistics.

#### Figure 120 Dashboard > Wireless clients

| Cambiun 🌔      | n Networks 💭 DASHBOARD         | 🔨 🤻 INSIGHT 📢  | 🕽 CONFIGURE 🛛 😚 MA | NAGE     |          |             |           | LOGOUT                    |
|----------------|--------------------------------|----------------|--------------------|----------|----------|-------------|-----------|---------------------------|
| OVER           | RVIEW (••) ACCESS POINTS       | 奈 WIRELESS CLI | IENTS SWIRELESS    | LANS     |          |             |           |                           |
| Overview       | RF Stats                       |                |                    |          |          |             | Search    | Y                         |
| NAME           | MAC                            | IP             | AP                 | VENDOR   | USERNAME | DEVICE TYPE | WLAN      | VLAN                      |
| android-777    | 78-7B-8A-9A-9E-77              | 192.168.10.10  | E400-AF0782        | Apple    |          | Motorola    | member-10 | 10                        |
| ipad-766       | 80-00-6E-2E-59-3F              | 192.168.20.10  | E400-AF0782        | Motorola |          | iphone      | member-20 | 20                        |
| Displaying 1-1 | of 1 items. Items per page: 25 | ×              |                    |          |          |             |           | <ul> <li>← 1 →</li> </ul> |

## Manage Autopilot

The Manage tab of Autopilot UI manages firmware upgrades, configuration file updates, and technical assistance of the master and member APs. Data is distributed in the following sub-sections:

- Firmware
- System
- Tools

Figure 121 Manage > Firmware

| Cambium Networks | DASHBOARD     | 🂐 INSIGHT | 🛇 MANAGE | 🕞 LOGOUT |
|------------------|---------------|-----------|----------|----------|
| -l≁ FIRMWARE     | の SYSTEM 🔧 TO | OLS       |          |          |

### Firmware

This section supports uploading required firmware to master AP, and from master AP to the member APs.

To configure firmware:

- 1. Go to Manage > Firmware tab.
- 2. Click the **Browse** button to browse the firmware file.

Figure 122 Manage > Upload Firmware

| Cambium Net | vorks" 📮 DASHE   | BOARD    | 🤻 INSIGHT  |             | S MANAGE       |          |         |        |                 | 🕞 LOGOL | UT |
|-------------|------------------|----------|------------|-------------|----------------|----------|---------|--------|-----------------|---------|----|
| J≁ FIRMWARE | € SYSTEM         | 🔧 тоо    | LS         |             |                |          |         |        |                 |         |    |
|             | Upload Firmwar   | e        |            |             |                |          |         |        |                 |         |    |
|             |                  |          |            | Choose File | lo file chosen |          |         |        |                 |         |    |
|             |                  |          |            |             | 🕹 Upload Fir   | mware    |         |        |                 |         |    |
|             | Access Point Fin | mware Up | ograde     |             |                |          |         |        | Filter          | V       |    |
|             | NAME             | MAC      |            | IP          | MODEL          | ACTIVE   | BACKUP  | STATUS | ACTIONS         |         |    |
|             | E500-9F33F0 堂    | 00-04-56 | 5-9F-33-F0 | 10.10.0.7   | cnPilot E500   | 3.11-b11 | 3.11-b9 |        | INSTALL O REBOO | г       |    |

3. Select the required firmware file and click **Open**. For example, firmware file: E400\_E50X-3.4.2-b27.img.

| Cancel      | File Upload                                  | <u>Click on Open</u> – |         | Open     |
|-------------|--|------------------------|---------|----------|
| 🛇 Recent    |  |                        |         |          |
| 🛈 Home      | Name   | *                      | Size    | Modified |
| Documents   | Cnmaestro-export_cnmaestr_20170612T070701.ta | ar.gz                  | 95.2 kB | 12 Jun   |
|             | 🖉 config.json                                |                        | 30.9 kB | Mon      |
| 🕹 Downloads | Config.txt                                   |                        | 1.8 kB  | 7 Jul    |
| d Music     | E400_E50X-3.4.2-b27.img                      | irmware file           | 17.6 MB | 8 Jul    |

Figure 123 To open required Firmware

4. Click **Upload Firmware** button and wait for upload.

Figure 124 Upload firmware on Master AP

|  | Browse | E400_E50X-3.4.2-b27.img |
|--|--------|-------------------------|
| Glick here to upload firmware on master AP - |        | Upload Firmware         |
|  |        |                         |

5. By clicking on **Upgrade All Devices** button, the firmware can be upgraded on all APs simultaneously or can be upgraded on each AP separately by clicking on **Install** button provided for every AP on the list.



|                     |                    | _             | Firmware              | version 3.4.2    | -b27 loaded  | i                                  |                       |
|---------------------|--------------------|---------------|-----------------------|------------------|--------------|------------------------------------|-----------------------|
| Upgrade all /       | APs simultaneously | $\rightarrow$ | ♦ Upgrade All Devices | 🔿 Reboot All Dev | vices 📄 Dele | te Firmware                        |                       |
| Access Point Firmwa | are Upgrade        |               |                       |                  |              | Upgrade firm                       | nare on individual AP |
| NAME                | MAC                | IP            | MODEL                 | ACTIVE           | BACKUP       | STATUS                             | ACTIONS               |
| E500-BEA714         | 00-04-56-BE-A7-14  | 10.10.10.153  | cnPilot E500          | 3.4.2-b27        | 3.4.2-b27    | Upgraded successfully to 3.4.2-b27 | S INSTALL O REBOOT    |
| E500-914ED0         | 00-04-56-91-4E-D0  | 10.10.10.157  | cnPilot E500          | 3.4.2-b27        | 3.4.2-b27    | Upgraded successfully Reboot ind   |                       |

Once step 5 is done, the following statuses during the Firmware upgrade can be seen in Figure 126.



#### Figure 126 Firmware upgraded sequence

6. Different statuses of the firmware upgrade can be seen in Figure 127.

|                    |                   |              | Figure 12    | 27 Firmw  | are upgi  | raded status   |                           |
|--------------------|-------------------|--------------|--------------|-----------|-----------|--|---------------------------|
| Access Point Firmv | vare Upgrade      |              |              |           |           |  | Fiter                     |
| NAME               | MAC               | 19           | MODEL        | ACTIVE    | BACKUP    | STATUS   | ACTIONS                   |
| E500-BEA714        | 00-04-56-BE-A7-14 | 10.10.10.153 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | File downloaded. Starting upgrade                      | SINSTALL OREBOOT          |
| 500-914ED0         | 00-04-56-91-4E-D0 | 10.10.10.157 | cnPilot E500 | 3.4.2-627 | 3.4.2-b27 | File downloaded. Starting upgrade                      | INSTALL O REBOOT          |
| 500-BEA758         | 00-04-56-BE-A7-58 | 10.10.10.120 | cnPilot E500 | 3.4.2·b27 | 3.4.2-b27 | Firmware download<br>File downloaded. Starting upgrade | ed on master AP           |
| 400-B16CD0 🍲       | 00-04-56-81-6C-D0 | 10.10.10.40  | cnPilot E400 | 3.4.2-b27 | 3.4.2-b27 | Starting upgrade                                       | S INSTALL O REBOO         |
| 500-917722         | 00-04-56-91-77-22 | 10.10.165    | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | File downloaded. Starting upgrade                      | f upgrade on AP           |
| 400-AF0782         | 00-04-56-85-5D-8A | 10.10.10.197 | cnPilot E400 | 3.4.2·b27 | 3.4.2-b27 | Queued. Starting in 10 seconds                         | S INSTALL C REBOO         |
| 410-93F1AD         | 00-04-56-93-F1-AD | 10.10.138    | cnPilot E410 | 3.4.2-b27 | 3.4.2-b20 | firmware verification failed                           | S INSTALL O REBOO         |
| 500-BEA54A         | 00-04-56-BE-A5-4A | 10.10.161    | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | File downloaded. Starting upgrade                      | INSTALL O REBOO           |
| 500-BEA650         | 00-04-56-BE-A6-50 | 10.10.10.109 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | Queued. Starting in 20 seconds                         | S INSTALL Ø REBOO         |
| 400-AF0782         | 00-04-56-AF-07-82 | 10.10.198    | cnPilot E400 | 3.4.2-b27 | 3.4.2-b27 |  | aster ap INSTALL O REBOO  |
| 500-914F3C         | 00-04-56-91-4F-3C | 10.10.10.152 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | File downloaded. Starting upgrade                      | S INSTALL O REBOO         |
| 500-BEA588         | 00-04-56-BE-A5-88 | 10.10.10.92  | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | File downloaded. Starting upgrade                      | () INSTALL () REBOO       |
| 400-85805A         | 00-04-56-85-80-5A | 10.10.10.166 | cnPilot E400 | 3.4.2-b27 | 3.4.2-b27 | Queued. Starting in 15 seconds                         | SINSTALL CREBOO           |
| Access Point Firmv | vare Upgrade      |              |              |           |           |  | Filter                    |
| IAME               | MAC               | IP           | MODEL        | ACTIVE    | BACKUP    | STATUS   | ACTIONS                   |
| 500-BEA714         | 00-04-56-BE-A7-14 | 10.10.10.153 | cnPilot E500 | 3.4.2·b27 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27                     | SINSTALL OREBOO           |
| 500-914ED0         | 00-04-56-91-4E-D0 | 10.10.10.157 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27                     | S INSTALL O REBOO         |
| 500-BEA758         | 00-04-56-8E-A7-58 | 10.10.10.120 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27                     | SINSTALL OREBOO           |
| 400-B16CD0 🔹       | 00-04-56-B1-6C-D0 | 10.10.10.40  | cnPilot E400 | 3.4.2-627 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27                     | S INSTALL O REBOI         |
| 500-917722         | 00-04-56-91-77-22 | 10.10.165    | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | Upgraded succi Súccessfully Upgr                       | aded Firmware             |
| 400-AF0782         | 00-04-56-85-5D-8A | 10.10.10.197 | cnPilot E400 | 3.4.2-b27 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27                     | S INSTALL O REBO          |
| 410-93F1AD         | 00-04-56-93-F1-AD | 10.10.10.138 | cnPilot E410 | 3.4.2-b27 | 3.4.2-b20 | firmware verification failed                           | S INSTALL O REBOI         |
| 500-BEA54A         | 00-04-56-8E-A5-4A | 10.10.10.161 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27 Fail                | ed firmware upgrade REBOI |
| 500-BEA650         | 00-04-56-8E-A6-50 | 10.10.10.109 | cnPilot E500 | 3.4.2-b27 | 3.4.2-b27 | Upgraded successfully to 3.4.2-b27                     | S INSTALL O REBOO         |

Note

In case of any error/failure in upgrade status such as **Firmware verification failed** is shown in status column:

- 1. APs can be rebooted individually by using **Reboot** option.
- 2. All the APs can be rebooted simultaneously using **Reboot All Devices** option.
- 3. The loaded firmware can be deleted from the master AP using **Delete Firmware** option.

|                     |                          |                    | FILITIVA              | re version 3.4 | +.2-D27 10aue   | ed Version of load                 | ied Firmware         |
|---------------------|--------------------------|--------------------|-----------------------|----------------|-----------------|------------------------------------|----------------------|
| All APs             | upgraded simultaned      | ously              | စ် Upgrade All Device | s 👌 Reboot All | Devices 🚺 🖻 Del | lete Firmware Loaded firmw         | /are can be deleted. |
|                     |                          |                    |                       | 1              |                 |                                    |                      |
| Access Point Firn   | nware Upgrade            |                    | All APs c             | an be reboot   | ed simultan     | reously                            | Filter 5             |
|                     |                          |                    | MODEL                 | ACTIVE         | BACKUP          | STATUS                             | ACTIONS              |
| AME                 | MAC                      | IP                 | MODEL                 | ACTIVE         | brickor         |                                    |                      |
| NAME<br>E500-BEA714 | MAC<br>00-04-56-BE-A7-14 | IP<br>10.10.10.153 | cnPilot E500          | 3.4.2-b27      | 3.4.2-b27       | Upgraded successfully to 3.4.2-b27 | INSTALL O REBOOT     |

### System

This section provides the following options:

- **Reboot All**: This option is used to reboot all the APs including the master AP simultaneously.
- Disable Autopilot: This button is used to disable Autopilot and the entire network of master AP.

#### Figure 128 System

| Rebootall APs - | 🔶 🕐 Reboot All       | 🕫 Disable Autopilot    | Disable Autopilot network |
|-----------------|----------------------|------------------------|---------------------------|
|                 | Import Configuration | 🕹 Export Configuration |                           |

- **Import Configuration**: This button is used to load any essential configuration and configure Autopilot. Configuration files are stored in .json format.
- **Export configuration**: This button is used to export any new or essential configuration from Autopilot setup and store in .json format for future use.

#### Figure 129 System > Import/Export Configuration

|                 | 🗢 Reboot All                                   | 🕫 Disable Autopilot             |          |          |
|-----------------|--|---------------------------------|----------|----------|
| or importing co |  | Export Configuration For export | tingconf | iguratio |
| Cancel          | File Upload                                    |                                 | ٩        | Open     |
| Recent          |  | ick on Open to load 🛩           |          |          |
| Home            | Name   |                                 | Size     | Modifie  |
| Documents       | cnmaestro-export_cnmaestr_20170612T070701.tar. | gz                              | 95.2 kB  | 12 Jun   |
|                 | Select Config                                  | uration file                    | 30.9 kB  | Mon      |
| 🕹 Downloads     | - Contigen                                     |                                 | 1.8 kB   | 7 Jul    |
| J Music         | E400_E50X-3.4.2-b27.img                        |                                 | 17.6 MB  | 8 Jul    |
| dd Music        |  | 2월 11일 2월 2일 2월 2일 - 영화 이번      |          |          |

### Access Point Management

This section provides the following options:

- LED: This button triggers the LED light on the AP (Hardware) for easy identification.
- **Reboot**: This button is used to individually reboot APs in Autopilot network.
- **Default**: This button is used to set the APs to their default configuration.
- **Delete**: This button is used to delete member APs from the Autopilot network.

#### Figure 130 Access Point management

| Access Point Management |                   |                                    |                    |                    |  |
|-------------------------|-------------------|------------------------------------|--------------------|--------------------|--|
| NAME                    | MAC               | IP                                 | ACTIONS            | Autopilot's networ |  |
| E400-B16CD0 💇           | 00-04-56-B1-6C-D0 | 10.10.10.40                        | 🗲 LED 🕺 🔿 REBOOT   |                    |  |
| E400-B5AD58             | 00-04-56-B5-AD-58 | Triggers led light —               | 🔶 🗲 LED 🚺 🖄 REBOOT | DEFAULT            |  |
| E410-93F1AD             | 00-04-56-93-F1-AD | 10.10.10.138 Reboots A             |                    | 5 DEFAULT          |  |
| E500-BEA714             | 00-04-56-B5-AE-FC | Brings AP to default configuration | on - 🗡 📫 🔂         | S DEFAULT          |  |

### Tools

This section supports downloading technical support file for troubleshooting and viewing User Interfaces of APs.

| Troubleshoot                           |  |                           |                               |
|--|--|---------------------------|-------------------------------|
| This button generates techsupport file | Cownload Techsupport                                   |                           |                               |
| Access Point Management                | •  |                           | Filter                        |
| NAME                                   | Opening techsupport.tar.gz                             | ×P                        | ACTIONS                       |
| E400-B16CD0 🖢                          | You have chosen to open:                               | 10.10.10.40               | VIEW DEVICE UI                |
| E400-B5AD58                            | techsupport.tar.gz<br>which is: Gzip archive (63.9 KB) | 10.10.10.169              | of VIEW DEVICE UI             |
| E410-93F1AD                            | from: https://10.10.10.40                              | 10.10.138                 | d <sup>●</sup> VIEW DEVICE UI |
| E500-BEA714                            | What should Firefox do with this file?                 | 10.10.10.167              | VIEW DEVICE UI                |
| E500-917722                            | Open with Archive Manager (default)      Save File     | • 10.10.10.165            | VIEW DEVICE UI                |
| E400-BSB05A                            | Do this automatically for files like this from now on. | 10.10.10.166              | o <sup>0</sup> VIEW DEVICE UI |
| E400-AF0782                            | , .  | 10.10.10.198              |                               |
| mesh-client2-E410-93F19F               | Cancel OK  | c Dffline                 | d <sup>₽</sup> VIEW DEVICE UI |
| E500-BEA65E                            | 00-04-56-96-61-6C UI of p                              | particular AP can be view |                               |
| mesh-base1-E410-93F185                 | 00-04-56-93-F1-85                                      | Offline                   |                               |
| E500-BEA758                            | 00-04-56-BE-A7-58                                      | 10.10.10.120              |                               |

#### Figure 131 Tools > Troubleshoot

### Dashboard

The Dashboard of Autopilot UI provides excellent monitoring capability of the complete setup.

Various graphs and statistics of events, performance, and system information of clients and application is evidently made available to the user. It comprises of following components through which the data is available for monitoring.


#### Figure 132 Dashboard

### Overview

The Dashboard tab comprises of data and various graphs as follows:

- Site information
- Discovered devices
- Events
- Clients
- Throughput
- **Top Ap**
- Top clients

- Clients by Band/Radio type
- Channel distribution
- Clients by WLAN
- Clients by device type

#### Site information

This section provides the information of number of configured APs, online APs, and number of clients provided.



#### Figure 133 Dashboard > Overview > Site information

#### Discovered devices

This table lists all the discovered devices with their names, IP addresses, and actions performed over them. Every device discovered and displayed here should be **APPROVED** for it to be connected to APs network and ready for configuration.

#### Figure 134 Dashboard > Overview > Discovered devices

| DISCOVERED DEVICES     |              | Approve All |
|------------------------|--------------|-------------|
| NAME                   | IP           | ACTIONS     |
| E410-93F17C            | 10.10.10.119 | ✓ APPROVE   |
| mesh-base1-E410-93F185 | 10.10.137    | ✓ APPROVE   |

#### Events

This section continuously streams all the events occurring on the network of AP both graphically and digitally. Graphical spikes can be helpful in representing the network to know how the network is behaving. Any configuration error is also displayed as an event with the reasons mentioned due to which the application of respective configuration failed. For example, check the highlighted event in the below figure.



#### Figure 135 Dashboard > Overview > Events

#### Clients

This section graphically streams information about the number of clients connected to specific frequency (2.4 Hz or 5 Hz) and total number of clients at a given time on the present day.



Figure 136 Dashboard > Overview > Clients

### Throughput

This section graphically represents the TX, RX of each client and total Throughput of all clients against each channel. User can hover over the graph and get more granular details.



#### Figure 137 Dashboard > Overview > Throughput

#### Top Aps

This section graphically displays the top five APs connected to Autopilot's network along with numbers of clients and traffic in respective frequencies (2.4hz or 5hz).



### Top clients

This section graphically represents the top five clients connected to APs with highest traffic flow.

#### Figure 139 Dashboard > Overview > Top clients



#### Clients by Band/Radio type

This section provides pie chart representation of the radio types of clients. This shows pie chart based on the percentage of 2.4 GHz and 5 GHz clients connected to Autopilot network. Another pie chart is plotted based on types of clients such as 802.11a, 802.11b/g/n, 802.11ac.



#### Channel distribution

This section plots and displays the channel distribution between master and member APs as shown below. This helps to know which channels are being used and how many APs are using the channels.

Figure 141 Dashboard > Overview > Channel distribution



#### Clients by WLANs

This section provides a pie chart representation of all the Clients and WLANs. This helps to instantly know the load on the WLANs.



Figure 142 Dashboard > Overview > Clients by WLANs

#### Clients by device type

This section provides a pie chart representation of device type (Respective Platforms) of the Clients. This classifies the clients based on type such as Android, Windows clients, Linux, Ipad, Iphone clients, and so on.





### Access Points

This tab contains details such as Performance, System details, Client details, and so on of all the APs connected to Autopilot. Under Access Point tab, there are four tabs which are as follows:

#### Overview

This tab provides information such as Name, MAC address, IP Address, Model, number of Clients, Power, Channels, and State of radio of all the APs'.

#### Performance

This tab displays MAC, IP, Link speed, Total TX (Transmit from APS), and Total RX (Received to APS). For example, if AP transmits data at the speed of 10mbps, then its TX is equal to 10mbps.

| Cambium Networks*          | 🖵 DASHBOARD 🧮 INSIGH | 🕈 🏟 CONFIGURE 🛛 🧐 MANAGE   |            |          | ₿ LOGOUT                      |
|----------------------------|----------------------|----------------------------|------------|----------|-------------------------------|
| OVERVIEW                   | ACCESS POINTS        | SS CLIENTS 🔊 WIRELESS LANS |            |          |                               |
| Overview Performan         | Confi                | g                          |            |          | Search V                      |
| NAME                       | IP ADDRESS           | MAC                        | LINK SPEED | TOTAL TX | TOTAL RX                      |
| E500-9F33F0 堂              | 10.10.0.7            | 00-04-56-9F-33-F0          | 1000M      | 1.2 Kbps | 0 bps                         |
| E400-B16F48                | 192.168.15.10        | 00-04-56-B1-6F-48          | 1000M      | 0 bps    | 0 bps                         |
| E400-B558D2                | 10.10.0.5            | 00-04-56-B5-58-D2          | 1000M      | 0 bps    | 0 bps                         |
| Displaying 1-3 of 3 items. | Items per page: 25 💌 |                            |            |          | <ul><li>&lt; 1 &gt;</li></ul> |

#### Figure 144 Dashboard > Access Points > Performance

#### System

This tab displays name, IP address, model, firmware, backup, CPU usage, memory, uptime, and synced configurations of all APs. This helps to know the performance of the APs. Config synched option lets a user to know whether the configuration of an AP is synched with the configuration done on Master. If there is any config sync issue, a red **x** is displayed as shown in Figure 145.

#### Figure 145 Dashboard > Access Points > System

| OVERVIEW         | (••) ACCESS POINTS  | ♥ WIRELESS CLIENTS | WIRELESS LA | NS      |      |        |          |               |   |
|------------------|---------------------|--------------------|-------------|---------|------|--------|----------|---------------|---|
| Overview Perform | mance System RF Sta | ts Config          |             |         |      |        |          | Search        | 7 |
| NAME             | IP ADDRESS          | MODEL              | FIRMWARE    | BACKUP  | CPU  | MEMORY | UPTIME   | CONFIG SYNCED |   |
| E500-9F33F0 堂    | 10.10.0.7           | cnPilot E500       | 3.11-b11    | 3.11-b9 | 10 % | 48 %   | 16 hours | ~             |   |
| E400-B16F48      | 192.168.15.10       | cnPilot E400       | 3.11-b11    | 3.11-b9 | 10 % | 45 %   | 16 hours | 4             |   |
| E400-B558D2      | 10.10.0.5           | cnPilot E400       | 3.11-b11    | 3.11-b9 | 10 % | 45 %   | 16 hours | ~             |   |
| E410-93F1AD      | 10.10.138           | cnPilot E400       | 3.11-b11    | 3.11-b9 | 0%   | 0%     | 16 hours | ×             |   |
| E400-AF0782      | 10.10.10.25         | cnPilot E400       | 3.11-b11    | 3.11-b9 | 0%   | 0%     | 16 hours | ×             |   |

#### RF stats

This tab displays the number of 2.4G Clients, 5G Clients, TX to 2.4G clients, TX to 5G clients, RX from 2.4G clients, RX from 5G clients. Tx statistic signifies the downlink data speed to the client and Rx signifies uplink data speed from the client.

| Cambium Networks*          |                          | 🛠 INSIGHT 🏾 🏟 CONFIGURE | S MANAGE      |            |         |         |          | 🕞 LOGOUT |
|----------------------------|--------------------------|-------------------------|---------------|------------|---------|---------|----------|----------|
| OVERVIEW                   | ACCESS POINTS            | 🗢 WIRELESS CLIENTS 🔊    | WIRELESS LANS |            |         |         |          |          |
| Overview Performan         | ce System <b>RF Stat</b> | s Config                |               |            |         |         | Search   | Y        |
| NAME                       | IP ADDRESS               | MAC                     | 2.4G CLIENTS  | 5G CLIENTS | 2.4G TX | 2.4G RX | 5G TX    | 5G RX    |
| E500-9F33F0 堂              | 10.10.0.7                | 00-04-56-9F-33-F0       | 0             | 1          | 0 bps   | 0 bps   | 1.3 Kbps | 0 bps    |
| E400-B16F48                | 192.168.15.10            | 00-04-56-B1-6F-48       | 0             | 0          | 0 bps   | 0 bps   | 0 bps    | 0 bps    |
| E400-B558D2                | 10.10.0.5                | 00-04-56-B5-58-D2       | 0             | 0          | 0 bps   | 0 bps   | 0 bps    | 0 bps    |
| Displaying 1-3 of 3 items. | tems per page: 25 💌      | ]                       |               |            |         |         |          | د1       |

#### Figure 146 Dashboard > Access Points > RF Status

### Wireless clients

This tab represents details of wireless clients such as vendor type, WLANs, VLANs, RF Stats, and so on.

#### Overview

The details in this tab include Name, MAC, IP, Vendor type of clients, Usernames (WPA2 enterprise and guest access), Device type (Platform) of Clients, list of WLANs to which clients are connected, and VLAN information of respective WLANs.

| OVERVIEW       | (•)) ACCESS POINTS |              | S WIRELESS LANS |             |          |             |           |      |
|----------------|--------------------|--------------|-----------------|-------------|----------|-------------|-----------|------|
| verview RF Sta | ats                |              |                 |             |          |             | Search    |      |
| ME MA          | ιC                 | IP           | AP              | VENDOR      | USERNAME | DEVICE TYPE | WLAN      | VLAN |
| 02-            | 00-46-00-00-01     | 10.10.155    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-02     | 10.10.10.122 | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-03     | 10.10.153    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-04     | 10.10.158    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-05     | 10.10.10.120 | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-06     | 10.10.10.100 | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-07     | 10.10.154    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-08     | 10.10.159    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-09     | 10.10.156    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |
| 02-            | 00-46-00-00-0A     | 10.10.155    | E400-B16CD0     | [Local MAC] |          | Linux       | beta-test | 1    |

#### Figure 147 Dashboard > Wireless clients

#### **RF** Stats

This tab includes details such as frequency type, radio type, signal, Signal to Noise (SNR), physical rate, TX and RX of clients along with names, MAC, and IP addresses of clients.



Note Less the number in signal better is the signal. For example, -20 is better signal than -70. Similarly, more the SNR better is the signal quality.

#### Figure 148 Dashboard > Wireless clients > RF status

| Cambium Netv       | vorks" DASHBOARD            | 🍕 insight 🛛 🔅   | CONFIGURE | MANAGE        |       |         |       |          |            | <b>₽</b> 1 | .OGOUT |
|--------------------|-----------------------------|-----------------|-----------|---------------|-------|---------|-------|----------|------------|------------|--------|
| OVERVIEW           | (•) ACCESS POINTS           | 奈 WIRELESS CLIE | NTS 🔊 V   | VIRELESS LANS |       |         |       |          |            |            |        |
| Overview RF        | Stats                       |                 |           |               |       |         |       |          |            | Search     | ٢      |
| IAME               | MAC                         | IP              |           | TYPE          | RADIO | SIGNAL  | SNR   | PHY RATE | ТХ         | RX         |        |
|                    | 02-00-46-00-00-01           | 10.10.10.155    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 885.1 Kbps | 6.9 Kb     | ps     |
|                    | 02-00-46-00-00-02           | 10.10.10.122    |           | 5GHz          | ac    | -38 dBm | 57 dB | 780 M    | 900.2 Kbps | 7 Kbps     | 5      |
|                    | 02-00-46-00-00-03           | 10.10.10.153    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 872.6 Kbps | 6.6 Kb     | ps     |
|                    | 02-00-46-00-00-04           | 10.10.10.158    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 863 Kbps   | 6.7 Kb     | ps     |
|                    | 02-00-46-00-00-05           | 10.10.10.120    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 895.2 Kbps | 7 Kbps     | 5      |
|                    | 02-00-46-00-00-06           | 10.10.10.100    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 876.3 Kbps | 6.7 Kb     | ps     |
|                    | 02-00-46-00-00-07           | 10.10.10.154    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 865.1 Kbps | 6.8 Kb     | ps     |
|                    | 02-00-46-00-00-08           | 10.10.10.159    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 885.4 Kbps | 6.8 Kb     | ps     |
|                    | 02-00-46-00-00-09           | 10.10.10.156    |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 864.4 Kbps | 6.6 Kb     | ps     |
|                    | 02-00-46-00-00-0A           | 10.10.10.55     |           | 5GHz          | ac    | -39 dBm | 56 dB | 780 M    | 884.2 Kbps | 6.8 Kb     | ps     |
| splaying 1-10 of 1 | 8 items. Items per page: 10 | Ŧ               |           |               |       |         |       |          |            | ۲ د        | 2      |

### Wireless LANs

This tab provides details of all the configured WLANs as follows:

- **GROUP**: Name of the group under which the WLAN is created. WLAN group is used to club single or multiple WLANs and then push the WLAN configurations to selected APs.
- **SSID**: SSID of the WLAN.
- **SECURITY**: Security of the WLAN which can be WPA2-PSK, WPA2-Enterprise, or Open.
- **Tx**: The actual data speed of downlink data. AP to clients.
- **Rx**: The actual data speed of uplink data. Clients to AP.

#### Figure 149 Dashboard > Wireless LANs

| Cambium Networks"          | DASHBOARD          | 🤻 Insight 🛛 🖨 Config | SURE 🛇 MANAGE   |         |        | Digout  | т |
|----------------------------|--------------------|----------------------|-----------------|---------|--------|---------|---|
| OVERVIEW                   | (*)) ACCESS POINTS | 🗢 WIRELESS CLIENTS   | S WIRELESS LANS | _       |        |         |   |
| Overview                   |                    |                      |                 |         |        | Search  | V |
| GROUP                      | SSID               | SECURIT              | Y               | CLIENTS | ТХ     | RX      |   |
| Default                    | Auto_pilot_8       | open                 |                 | 0       | 0 bps  | 0 bps   |   |
| diva1                      | diva_wlan1         | open                 |                 | 0       | 0 bps  | 0 bps   |   |
| Default                    | Auto_pilot_4       | open                 |                 | 1       | 74 bps | 140 bps |   |
| Default                    | Auto_pilot_1       | wpa2-ent             | terprise        | 0       | 0 bps  | 0 bps   |   |
| Displaying 1-4 of 4 items. | Items per page: 25 | •                    |                 |         |        | c 1     | > |

### Insight

Insight option of Autopilot UI provides accurate insights on an AP anomalies which are distributed on the sub tabs as follows:

- Pulse
- Timeview
- Events

On the top left corner of the page the master and the member APs can be selected from the drop-down list. Site default gives overall details.

#### S MANAGE Cambium Networks DASHBOARD 💐 INSIGHT CONFIGURE 🕞 LOGOUT Ar PULSE TIMEVIEW EVENTS Site : Default A ACCESS POINT ANOMALIES Select Site / AP High CPU Usage High Memory Usage AP: E500-9F33F0 1 0 Tracks Access Points which use very high CPU. Threshold is currently configured at 90%. Tracks Access Points which use very high memory. Threshold is currently configured at 90%. AP : E400-B16F48 AP : E400-B558D2 No WLANs Mapped No Clients Ó 6 0 2 Tracks Access Points which do not have any wireless Tracks Access Points which do not have any clients lans configured. associated. No Gigabit Ethernet Less uptime ${\mathscr S}$ Ð Tracks Access Points which did not auto-neg Gigabit 0 0 Tracks Access Points which came up within the last network speed. 30 minutes. Client overload Mistmatched Firmware Ś Ô 0 0 Tracks Access Points which have more than 100 Tracks Access Points which do not have the latest clients.

#### Figure 150 Insight > Pulse

### Pulse

This tab provides the detailed information of the following:

- **High CPU usage**: On clicking, this option leads to **TIMEVIEW** page of Insight tab and tracks the CPU usage of all APs graphically.
- No WLANs mapped: This option leads to APs page of Dashboard tab and tracks number of APs without wireless LANs configured.

- **No Gigabit ethernet**: This option leads to APs page of Dashboard tab and tracks APs which do not auto negotiate Gigabit network speed.
- **Client overload**: This option leads to AP page of Dashboard and gives the number of clients connected to every AP and also points the AP connected by highest number of clients.
- **High memory usage**: Tracks the memory usage of all APs and the highest memory usage and leads to **TIMEVIEW** page of the Insight tab, when clicked upon.
- No clients: Tracks the APs which do not have any clients connected to them along with their details like IP Address, Mac Address, and Model etc. On clicking leads to APs page on Dashboard.
- Less uptime: Lists all the APs which were activated within the last 30 minutes along with their details and leads to Overview page on Dashboard.
- **Mismatched firmware:** Provides information related to mismatch of software with respect to Master device.



In current version not all of these options are supported.

### Timeview

This tab provides the graphical interpretation of CPU usage, Memory Usage, Clients, Overall Throughput, and Throughput by frequencies and Events. Also, the maximum (Graphical Peaks) and minimum values of all the mentioned components can be tracked accurately.



### Events

This tab provides the list of all the latest events of master and member APs. Events can be filtered for specific APs based on their event name, content, Mac or IP address. All the old events can be cleared to start afresh.

| Cambium Networks | 🖵 DASH  | BOARD    | 🤻 INSIGHT         | CONFIGURE             | S MANAGE  |  |                      |                                |  |
|------------------|---------|----------|-------------------|-----------------------|---|--|----------------------|--------------------------------|--|
| ሎ PULSE 🛛 🔊 TI   | IMEVIEW | 🔊 EVE    | INTS              |                       |   |  |                      |                                |  |
|                  |         | Filter t | ext : Can include | event name, conte     | nt, IP or MAC                                       |  | Filter Events        | Clear Events                   |  |
|                  |         |          |                   |                       | — Events  | $\land$  |                      |                                |  |
|                  |         | 0        | WIFI-AUTORF-CHA   | NNEL-SWITCH: Chani    | nel switched from [1] to                            | [6] on [2.4GHz] radio, [High Intf on channel]                                    |                      | Sep 1, 22:06:37<br>E400-B558D2 |  |
|                  |         | 0        | WIFI-AUTORF-CHA   | NNEL-SWITCH: Chan     | nel switched from [6] to                            | [11] on [2.4GHz] radio, [High Intf on channel]                                   |                      | Sep 1, 22:06:06<br>E500-9F33F0 |  |
|                  |         | 0        | WIFI-AUTORF-CHA   | NNEL-SWITCH: Chanı    | nel switched from [11] t                            | o [6] on [2.4GHz] radio, [High Intf on channel]                                  |                      | Sep 1, 22:05:46<br>E400-B16F48 |  |
|                  |         | 0        | WIFI-AUTORF-CHA   | NNEL-SWITCH: Chani    | nel switched from [100]                             | to [116] on [5GHz] radio, [High Intf on channel]                                 | 0                    | Sep 1, 20:25:46<br>E400-B558D2 |  |
|                  |         |          |                   |                       | 8-7B-8A-9A-9E-77] disco<br>0] mintx [0] avgrx [0] m | nnected from WLAN [Auto_pilot_4] after [59] se<br>axrx [0] minrx [0]             | ecs roamed [yes]     | Sep 1, 18:52:46<br>E400-B16F48 |  |
|                  |         | 0        | WIFI-CLIENT-CON   | IECTED: Client [78-78 | 3-8A-9A-9E-77] connecte                             | ed to wireless lan [Auto_pilot_4]  |                      | Sep 1, 18:52:46<br>E500-9F33F0 |  |
|                  |         |          |                   |                       |   | nnected from WLAN [Auto_pilot_4] after [13759<br>] avgrx [0] maxrx [0] minrx [0] | 9] secs roamed [yes] | Sep 1, 18:51:47<br>E500-9F33F0 |  |
|                  |         | 0        | WIFI-CLIENT-CON   | IECTED: Client [78-7B | 3-8A-9A-9E-77] connecte                             | ed to wireless lan [Auto_pilot_4]  |                      | Sep 1, 18:51:47<br>E400-B16F48 |  |
|                  |         | 0        | DHCPSRVR-IP-ASS   | GNED: Client [78-7B-  | -8A-9A-9E-77], assigned                             | [dynamic] IP [192.168.15.12] from DHCP pool [                                    | 2]                   | Sep 1, 18:43:41<br>E500-9F33F0 |  |

#### Figure 152 Insight > Unfiltered Events



| Cambium Networks 🛛 📮 DASH       | SOARD KINSIGHT & CONFIGURE & MANAGE   | 🕑 LOGOUT         |
|---------------------------------|---|------------------|
| J <sub>№</sub> PULSE 🤭 TIMEVIEW | € EVENTS  | Site : Default 🔻 |
|                                 | disconnect Filter Events Clear Events   |                  |
|                                 | - Events  |                  |
|                                 | WIRI-CLIENT-DISCONNECTED: Client [78-78-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [59] secs roamed [yes]     txbytes [0] rxbytes [0] avgtx [0] maxtx [0] mintx [0] avgtx [0] maxrx [0] mintx [0]     sep 1, 18:5246     E400-816F48  |                  |
|                                 | WIFI-CLIENT-DISCONNECTED: Client (78-78-8A-9A-9E-77) disconnected from WLAN (Auto_pilot_4) after (13759) secs roamed (yes)         Sep 1, 18-51:47           bxbytes [114047] rxbytes [219436] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxtx [0] mintx [0]         Sep 1, 18-51:47  |                  |
|                                 | WIRI-CLIENT-DISCONNECTED: Client (78-78-8A-9A-9E-77) disconnected from WLAN [Auto_pilot_4] after [1943] secs roamed [yes] Sep 1, 15:02.28     Evbytes [15150] rxbytes [26173] avgbx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] mintx [0] avgrx [0] mintx [0]   |                  |
|                                 | WIFI-CLENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [1163] secs roamed [yes]         Sep 1, 14-30.04           bt/btytes [14198] rxbytes [41673] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] mintx [0]         Sep 1, 14-30.04  |                  |
|                                 | WIFI-CLENT-DISCONNECTED: Client [78-78-8A-94-9E-77] disconnected from WLAN [Auto_pilot_4] after [1654] secs roamed [yes]         Sep 1, 14:10:41           txbytes [14298] rxbytes [26150] avgtx [0] maxtx [0] mintx [0] avgtx [0] maxtx [0] mintx [0] avgtx [0] maxtx [0]         Sep 1, 14:10:41  |                  |
|                                 | WIFI-CLENT-DISCONNECTED: Client [78-78-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [112] secs roamed [yes]     Sep 1, 13:43:10     E500-9F33F0     E500-9F33F0   |                  |
|                                 | WIFI-CLENT-DISCONNECTED: Client (78-78-8A-9A-9E-77) disconnected from WLAN (Auto_pilot_4) after [21387] secs roamed [no]         Sep 1, 13:41:09           bt/btytes [191684] rxbytes [388282] avgtx [0] maxtx [0] mintx (0] avgrx [0] maxtx [0] mintx (0]         E400-816F48  |                  |
|                                 | WIFI-CLIENT-DISCONNECTED: Client [78-78-84-94-9E-77] disconnected from WLAN [Auto_pilot_4] after [99] secs roamed [yes]         Sep 1, 07-44-42           tobytes [42] rxbytes [46] avgtx [0] maxx [0] mintx [0] avgrx [0] maxx [0] mintx [0]         Sep 1, 07-44-42   |                  |
|                                 | WIFI-CLIENT-DISCONNECTED: Client (78-78-8A-9A-9E-77) disconnected from WLAN [Auto_pliot_4] after [1] secs roamed [no] txbytes [0] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxtx [0] mintx |                  |

## Chapter 16: Guest Access Portal- INTERNAL

### Introduction

Guest Access Portal services offers a simple way to provide secure access to internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browsers session to a captive portal login page where the user must enter valid credentials to be granted access to the network.

Modes of Captive Portal Services supported by cnPilot devices:

- Internal Access: Captive Portal server is hosted on access point and is local to access point.
- External Access: cnPilot is integrated with multiple third-party Captive Portal services vendor. Based on the vendor, device needs to be configured. More details on this Guest Access Portal method is described in Chapter 17.
- **cnMaestro:** Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login and Paid login is supported. More details on this Guest Access Portal method is described in **Chapter 18**.

Here in this chapter we will brief about Internal Captive Portal services supported by cnPilot Access Points. Figure 143 displays the basic topology of testing Internal Captive Portal Service.



Figure 154 Topology

## Configurable Parameters

Figure 144 displays multiple configurable parameters supported for Internal Guest Access hosted on AP. Access Policy – Clickthrough

| Basic Radius Server Gue        | est Access                              | Usage Limits                             | Scheduled Access  | Access                          | Passpoint                    |               | Delete |
|--------------------------------|---|--|---|---------------------------------|------------------------------|---------------|--------|
| Enable                         | •                                       |  |   |                                 |                              |               |        |
| Portal Mode                    | Interior                                | nal Access Point                         | External Hotspot   cnN  | laestro                         |                              |               |        |
| Access Policy                  | <ul> <li>Radii</li> <li>LDAF</li> </ul> | us Splash-page wi<br>P Redirect users to | age where users accept ter<br>th username & password,<br>a login page for authentic<br>Redirect users to a login pa | authenticated<br>ation by a LD, | with a RADIUS s<br>AP server | server        | ount   |
| Redirect Mode                  | ~                                       | OUse HTTP URLs<br>PS Use HTTPS UP        |   |                                 |                              |               |        |
| Redirect Hostname              |   |  |   |                                 |                              |               |        |
|                                | Redirect                                | Hostname for the s                       | plash page (up to 255 chai  | rs)                             |                              |               |        |
| Title                          | Welco                                   | me to Cambium                            | Networks  |                                 |                              |               |        |
|                                | Title text                              | in splash page (up                       | to 255 chars)   |                                 |                              |               |        |
| Contents                       | Free Wi-Fi Hotspot Services             |  |   |                                 |                              |               |        |
|                                | Main co                                 | ntents of the splash                     | page (up to 255 chars)  |                                 |                              |               |        |
| Terms                          | You h                                   | ereby expressly                          | acknowledge and agr   | ee that the                     | re are signific              | cant security | , pr   |
|                                | Terms &                                 | conditions displayed                     | d in the splash page (up to   | 255 chars)                      |                              |               |        |
| Logo                           | https://                                | //www.realwire.c                         | om/writeitfiles/Carr  |                                 |                              |               |        |
|                                | Logo t                                  | o be displayed on th                     | e splash page   |                                 |                              |               |        |
| Background Image               | https://                                | //backgrounddow                          | nload.com/wp-con  |                                 |                              |               |        |
|                                | Backg                                   | round image to be di                     | isplayed on the splash pag  | e                               |                              |               |        |
| Success Action                 | Interior                                | nal Logout Page 🔍                        | Redirect user to Externa  | I URL 🔍 Re                      | direct user to O             | riginal URL   |        |
| Success message                | You a                                   | re free to Use W                         | i-Fi services   |                                 |                              |               |        |
| Redirect                       |   | only Enable redi                         | rection for HTTP packets o  | only                            |                              |               |        |
| Redirect User Page             | 1.1.1.                                  | 1  |   |                                 |                              |               |        |
|                                | Config                                  | ure IP address for re                    | edirecting user to guest por  | tal splash pag                  | 1e                           |               |        |
| Proxy Redirection Port         |   | Port number                              | r(1 to 65535)   |                                 |                              |               |        |
| Session Timeout                | 28800                                   | Session time                             | e in seconds (60 to 259200  | )0)                             |                              |               |        |
| Inactivity Timeout             | 1800                                    | Inactivity tin                           | ne in seconds (60 to 25920  | 00)                             |                              |               |        |
| MAC Authentication<br>Fallback | 🔲 Use                                   | guest-access only a                      | s fallback for clients failing  | MAC-authen                      | tication                     |               |        |
| Extend Interface               |   | Configure th                             | ne interface which is extend  | led for guest a                 | access                       |               |        |
|                                | Save                                    | Cancel                                   |   |                                 |                              |               |        |

Figure 155 Configure: WLAN > Guest Access > Internal Access Point parameter

### Access policy

#### Click through

When this policy is selected, user will get a login page to accept "Terms and Conditions" to get access to network. No additional authentication is required.

RADIUS

When this policy is selected, user will be prompted for credentials, which is authenticated by Radius server. Radius server details can be configured on device at **Configure > WLAN > RADIUS**.

LDAP

When this policy is selected, user will be prompted for credentials, which is authenticated by LDAP/AD server. LDAP server details can be configured on device at **Configure > WLAN > Guest Access > LDAP**.

#### Local Guest Account

When this policy is selected, username and password is configured on device and it can be used as credentials for all wireless users connected to this WLAN profile to gain internet access.

### Splash page

#### Title

You can configure the contents of splash page using this field. Contents should not exceed more than 255 characters.

#### Contents

You can configure the contents of splash page using this field. Contents should not exceed more than 255 characters.

#### Terms and conditions

Terms and conditions to be displayed on the splash page can be configured using this field. Terms and conditions should not exceed more than 255 characters.

#### Logo

Displays the logo image updated in URL http(s)://<ipaddress>/<logo.png>. Either PNG or JPEG format of logo are supported.

#### Background image

Displays the background image updated in URL http(s)://<ipaddress>/background>/<image.png>. Either PNG or JPEG format of logo are supported.

### **Redirect Parameters**

#### Redirect hostname

User can configure a friendly hostname, which is added in DNS server and is resolvable to cnPilot IP address. This parameter once configured will be replaced with IP address in the redirection URL provided to wireless stations.

#### Success action

Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL:

#### • Internal logout Page

After successful login, Wireless client is redirected to logout page hosted on AP.

• Redirect users to external URL

Here users will be redirected to URL which we configured on device as below:

• Redirect users to Original URL

Here users will be redirected to URL that is accessed by user before successful captive portal authentication.

#### Figure 156 Success action

Success Action 
Internal Logout Page 

Redirect user to External URL 

Redirect user to Original URL

#### Redirect

By default, captive portal redirection is trigger when user access either HTTP or HTTPs WWW. If enabled, redirection to Captive Portal Splash Page is triggered when a HTTP WWW is accessed by end user.

#### Figure 157 Redirect

Redirect ITP-only Enable redirection for HTTP packets only

#### Redirect Mode

There are two redirect modes available:

HTTP Mode

When enabled, AP sends a HTTP POSTURL to the client.

HTTP(s) Mode

When enabled, AP sends HTTPS POST URL to the client

#### Proxy redirection port

Proxy redirection port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.

#### Redirect user page

IP address configured in this field is used as logout URL for Guest Access sessions. IP address configured should be not reachable to internet.

#### Figure 158 Redirect user page

| Redifect User Page | Configure IP address for redirecting user to guest portal splash page |
|--------------------|---|
| Redirect User Page | 1.1.1.1   |

Logout re-direction URLs are as follows:

http(s)://<Redirect user Page>/logout

### Success Message

This we can configure so that we can display success message on the splash page after successful authentication.

#### Figure 159 Success Message

| Success message |  |
|-----------------|--|
|                 |  |

### Timeout

#### Session

This is the duration of time which wireless client will be allowed internet after guest access authentication.

Figure 160 Configure: WLAN > Guest Access > Session timeout

| Session Timeout | 28800 | Session time in seconds (60 to 2592000) |
|-----------------|-------|---|
|                 |       |   |

#### Inactivity

This is the duration of time after which wireless client will be requested for re-login.

Figure 161 Configure: WLAN > Guest Access > Inactivity timeout

| Inactivity Timeout | 1800 | Inactivity time in seconds (60 to 2592000) |
|--------------------|------|--|
|                    |      |  |

### MAC Authentication fallback

It is a fall back mechanism in which wireless clients will be redirected to Guest access login Page after Radius based Mac authentication failure. This means When AP detects RADIUS authentication has failed for a wireless client, AP will send a HTTTP Post with respect to redirection URL to the client for guest access authentication. Figure 162 Configure: WLAN > Guest Access > MAC Authentication fallback

MAC Authentication Fallback Use guest-access only as fallback for clients failing MAC-authentication

### Extended interface

Provision to support Guest Access on Ethernet interface.

#### Figure 163 Configure: WLAN > Guest Access > Extended interface

| Extend Interface | Configure the interface which is extended for guest access |
|------------------|--|
|------------------|--|

### Whitelist

Provision to configure either Ips or URLs to bypass traffic, therefor user can access those Ips or URLs without Guest Access authentication.

### Captive portal bypass user agent

Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.

| Add Wh | itelist | Captive P | ortal bypass | User Agent  |          |     |
|--------|---------|-----------|--------------|-------------|----------|-----|
| Index  | ¢       |           | 1            | v           |          |     |
| User   | Agent S | tring     |              |             |          |     |
| Statu  | is Code |           | 200          | Ŧ           |          |     |
| нтм    | L Respo | nse       |              |             |          | 11  |
| Ind.X  | Match   |           | Save         | .Y Html Rej | alv ~    | Act |
|        | NI      | o User    | Aden         | t rule a    | vailable |     |
|        | N       | 0001      | Agen         |             | Valiabio |     |
|        | INC     |           | Ngen         |             | vana bio |     |
|        | INC     |           | Jigen        |             |          |     |
|        | INC     |           | 7.9011       |             |          |     |

Figure 164 Configure: WLAN > Guest Access > Captive portal bypass user agent

### Configuration examples

This section briefs about configuring different methods of Internal Guest Access captive portal services hosted on AP.

### Access Policy - Clickthrough

### Configuration

| Basic | Radius Server  | Guest Access                             | Usage Limits  | Scheduled Access   | Access                         | Passpoint                 | De        |  |  |
|-------|--|--|---|--|--------------------------------|---------------------------|-----------|--|--|
|       | Enable   |  |   |  |                                |                           |           |  |  |
|       | Portal Mode  | Interna                                  | Access Point  | xternal Hotspot <sup>◯</sup> cnMa  | estro                          |                           |           |  |  |
|       | Access Policy  | <ul> <li>Radius</li> <li>LDAP</li> </ul> | Splash-page with<br>Redirect users to a             | e where users accept term<br>username & password, au<br>login page for authenticati<br>direct users to a login page            | thenticated w<br>ion by a LDAF | ith a RADIUS se<br>server | erver     |  |  |
|       | Redirect Mode <ul> <li>HTTP</li> <li>Use HTTP URLs for redirection</li> <li>HTTPS</li> <li>Use HTTPS URLs for redirection</li> </ul> |  |   |  |                                |                           |           |  |  |
|       | Redirect Hostname  | •  |   |  |                                |                           |           |  |  |
|       |  | Redirect H                               | ostname for the spla                                | ish page (up to 255 chars)   |                                |                           |           |  |  |
|       | Title  |  | e to Cambium N                                      |  |                                |                           |           |  |  |
|       |  |  | splash page (up to                                  |  |                                |                           |           |  |  |
|       | Contents   | 1100 111                                 | -Fi Hotspot Serv                                    | ices<br>ge (up to 255 chars)   |                                |                           |           |  |  |
|       | Terms  |  |   |  |                                |                           |           |  |  |
|       | lerns  |  |   | y expressly acknowledge and agree that there are significant securit<br>litions displayed in the splash page (up to 255 chars) |                                |                           |           |  |  |
|       | Logo   |  | https://www.cambiumnetworks.com/wri                 |  |                                |                           |           |  |  |
|       | 5  | · ·                                      | Logo to be displayed on the splash page             |  |                                |                           |           |  |  |
|       | Background Image   | https://v                                | https://www.cambiumnetworks.com/3d/                 |  |                                |                           |           |  |  |
|       |  | Backgrou                                 | Background image to be displayed on the splash page |  |                                |                           |           |  |  |
|       | Success Action   | <ul> <li>Internal</li> </ul>             | l Logout Page 🔍 R                                   | edirect user to External   | URL 🔍 Redir                    | ect user to Ori           | ginal URL |  |  |
|       | Success message  | You are                                  | free to Use Wi-Fi                                   | services   |                                |                           |           |  |  |
|       | Redirec  | t 🗹 HTTP-o                               | nly Enable redirect                                 | ion for HTTP packets only  |                                |                           |           |  |  |
|       | Redirect User Page   | e 1.1.1.1                                |   |  |                                |                           |           |  |  |
|       |  | Configure                                | IP address for redire                               | ecting user to guest portal sp   | plash page                     |                           |           |  |  |
|       | Proxy Redirection Por  | t  | Port number(1 t                                     | o 65535)   |                                |                           |           |  |  |
|       | Session Timeou   | t 28800                                  | Session time in                                     | seconds (60 to 2592000)  |                                |                           |           |  |  |
|       | Inactivity Timeou  | t 1800                                   | Inactivity time in                                  | e seconds (60 to 2592000)  |                                |                           |           |  |  |
|       | MAC Authentication<br>Fallbac  |  | est-access only as fa                               | llback for clients failing MA(   | C-authenticatio                | n                         |           |  |  |
|       | Extend Interface   | e  | Configure the in                                    | terface which is extended f  | or guest acces                 | s                         |           |  |  |
|       |  | Save                                     | Cancel  |  |                                |                           |           |  |  |

### Authentication - Redirected Splash Page



### Successful Login - Redirected Splash Page

| Cambium<br>Networks  |  |
|--|--|
| Welcome to Cambium<br>Networks<br>Welcome to Cambium<br>Powered Hotspot          |  |
| You are free to Use Wi-Fi services<br>Logout<br>Session time remaining: 07:59:54 |  |
|  |  |
|  |  |

### Access Policy - Radius

### Configuration

| Basic | Radius Server           | Guest Access                             | Usage Limits                            | Scheduled Access   | Access                         | Passpoint                              |          | Delete |
|-------|-------------------------|--|---|--|--------------------------------|--|----------|--------|
|       | Ena                     | able 💌                                   |   |  |                                |  |          |        |
|       | Portal M                | ode 💿 Interna                            | Access Point                            | xternal Hotspot 🔍 cnMa   | estro                          |  |          |        |
|       | Access Po               | <ul> <li>Radius</li> <li>LDAP</li> </ul> | Splash-page with<br>Redirect users to a | e where users accept term<br>username & password, au<br>login page for authenticat<br>direct users to a login page | thenticated w<br>ion by a LDAF | ith a RADIUS se<br><sup>2</sup> server | erver    | r      |
|       | Redirect M              |  | Use HTTP URLs fo<br>Use HTTPS URL       |  |                                |  |          |        |
|       | Redirect Hostna         | ame                                      |   |  |                                |  |          |        |
|       |                         | Redirect H                               | ostname for the spla                    | ash page (up to 255 chars)   |                                |  |          |        |
|       | 1                       | Title Welcom                             | e to Cambium N                          | etworks  |                                |  |          |        |
|       |                         | Title text in                            | splash page (up to                      | 255 chars)   |                                |  |          |        |
|       | Conte                   |  | -Fi Hotspot Serv                        |  |                                |  |          |        |
|       |                         |  | ents of the splash pa                   | ge (up to 255 chars)   |                                |  |          |        |
|       | Те                      |  |   | cknowledge and agree   |                                | e are significa                        | int seci | urit   |
|       |                         |  |   | n the splash page (up to 2   | 55 chars)                      |  |          |        |
|       |                         |  | vww.cambiumne                           |  |                                |  |          |        |
|       | Background Im           |  | www.cambiumne                           |  |                                |  |          |        |
|       | Buonground in           | -  |   | blayed on the splash page  |                                |  |          |        |
|       | Success Ac              | tion 💿 Interna                           | Logout Page 🔍 R                         | edirect user to External   | URL 🔍 Redii                    | rect user to Orig                      | ginal UR | ۲L     |
|       | Success mess            | age You are                              | free to Use Wi-                         | Fi services  |                                |  |          |        |
|       | Redi                    | rect 🗹 HTTP-                             | only Enable redire                      | ction for HTTP packets on  | ly                             |  |          |        |
|       | Redirect User P         | age 1.1.1.1                              |   |  |                                |  |          |        |
|       |                         | -  | e IP address for redi                   | irecting user to guest porta   | l splash page                  |  |          |        |
|       | Proxy Redirection       | Port                                     | Port number(1                           | to 65535)  |                                |  |          |        |
|       | Session Time            | eout 28800                               | Session time                            | in seconds (60 to 2592000)   | )                              |  |          |        |
|       | Inactivity Time         | eout 1800                                | Inactivity time                         | in seconds (60 to 2592000  | ))                             |  |          |        |
|       | MAC Authentica<br>Fallb |  | lest-access only as                     | fallback for clients failing $\mathbb N$   | IAC-authentic                  | ation                                  |          |        |
|       | Extend Inter            | face                                     | Configure the                           | interface which is extende   | d for guest ac                 | cess                                   |          |        |
|       |                         | Save                                     | Cancel                                  |  |                                |  |          |        |

| Basic Radius Server Gue    | est Access Usage                  | e Limits Schedule                | d Access Access   | Passpoint Delete          |
|----------------------------|-----------------------------------|----------------------------------|---|---------------------------|
| Authentication Server 1    | Host                              | Secret                           | Port  | Realm                     |
| Authentication Server 1    | sit.cambiumnet                    |                                  | 1812  | Realin                    |
|                            |                                   | 0                                |   | <b>D</b>                  |
| 2                          | da.cambiumnet                     | Secret                           | Port<br>1812  | Realm                     |
|                            |                                   |                                  |   |                           |
| 3                          | Host<br>dev.cambiumne             | Secret                           | Port 1812   | Realm                     |
|                            |                                   |                                  |   |                           |
| Timeout                    | 3                                 | Timeout in seconds of            | each request attempt (1-3                               | 30)                       |
| Attempts                   | 1                                 | Number of attempts be            | efore giving up (1-3)                                   |                           |
| Accounting Server 1        | Host                              | Secret                           | Port  |                           |
|                            | sit.cambiumnet                    | •••••                            | 1813  |                           |
| 2                          | Host                              | Secret                           | Port  |                           |
|                            | qa.cambiumnet                     | •••••                            | 1813  |                           |
| 3                          | Host                              | Secret                           | Port  |                           |
|                            | dev.cambiumne                     | •••••                            | 1813  |                           |
| Timeout                    | 3                                 | Timeout in seconds of            | each request attempt (1-                                | 30)                       |
| Attempts                   | 1                                 | Number of attempts be            | efore giving up (1-3)                                   |                           |
| Accounting Mode            | None •                            | Configure accounting             | g mode  |                           |
| Accounting Packet          |                                   | ing-On messages                  |   |                           |
| Accounting Packet          | _                                 | ing-On messages                  |   |                           |
| Sync Accounting<br>Records | Configure accou                   | inting records to be sync        | ed across neighboring AP                                | 's                        |
| Server Pool Mode           |                                   |                                  | qually among configured s<br>rlier servers are unreacha |                           |
| NAS Identifier             |                                   | NAS-Identifier attribute<br>name | e for use in Request packe                              | ets. Defaults to system   |
| Interim Update Interval    | 1800                              | Interval for RADIUS In           | terim-Accounting updates                                | (10-65535 Seconds)        |
| Dynamic Authorization      | Enable RADIUS                     | dynamic authorization (C         | COA, DM messages)                                       |                           |
| Dynamic VLAN               | Enable RADIUS                     | assigned VLANs                   |   |                           |
| Proxy through<br>cnMaestro | Proxy RADIUS p server from the AP | eackets through cnMaest          | ro (on-premises) instead c                              | of directly to the RADIUS |
|                            | [                                 | Save Cancel                      |   |                           |



### Authentication - Redirected Splash Page

Successful Login - Redirected Splash Page



### Access Policy - LDAP

### Configuration

| Basic | Radius Server     | Gue              | st Access  | Usage Limits  | Scheduled Access  | Access  | Passpoint                     | Delete                  |  |
|-------|-------------------|------------------|--|---|---|---|-------------------------------|-------------------------|--|
|       | E<br>Portal       | inable           | ☑  | Access Point O  | external Hotspot   cnMa   | aestro  |                               |                         |  |
|       | Access I          |                  | Clickthro  | ough Splash-page<br>Splash-page with<br>Redirect users to a | e where users accept term<br>username & password, au<br>login page for authentical<br>direct users to a login pag | ns & conditions<br>uthenticated w<br>tion by a LDAF   | ith a RADIUS serv<br>p server | <i>ier</i>              |  |
|       | LDAP Server       |                  |  |   |   |   |                               |                         |  |
|       | Base DN:          | DC=corp,0        | C=solutionlab,   | )C=com  |   | e.g DC= <nai< td=""><td>ME&gt;,DC=<name></name></td><td></td></nai<>                                | ME>,DC= <name></name>         |                         |  |
|       | Admin DN:         | CN=sadmi         | in,DC=corp,DC=s  | solutionlab,DC=com  |   | e.g CN= <na< td=""><td>ME&gt;OU=<name>,DC=&lt;1</name></td><td>IAME&gt;,DC=<name></name></td></na<> | ME>OU= <name>,DC=&lt;1</name> | IAME>,DC= <name></name> |  |
|       | Admin Password:   |                  |  |   |   | Specify LDA   | P Admin Password              |                         |  |
|       | Redirect          | Mode             |  | Use HTTP URLs fo<br>Use HTTPS URL                           |   |   |                               |                         |  |
|       | Redirect Host     | tname            |  |   |   |   |                               |                         |  |
|       |                   |                  | Redirect Ho  | Redirect Hostname for the splash page (up to 255 chars)     |   |   |                               |                         |  |
|       |                   | Title            | Welcome to Cambium Networks  |   |   |   |                               |                         |  |
|       |                   |                  | Title text in splash page (up to 255 chars)  |   |   |   |                               |                         |  |
|       | Cor               | ntents           | Free Wi-Fi Hotspot Services  |   |   |   |                               |                         |  |
|       |                   |                  | Main contents of the splash page (up to 255 chars)   |   |   |   |                               |                         |  |
|       |                   | Terms            | You hereby expressly acknowledge and agree that there are significant securit  |   |   |   |                               |                         |  |
|       |                   |                  | Terms & conditions displayed in the splash page (up to 255 chars)  |   |   |   |                               |                         |  |
|       |                   | Logo             | https://www.cambiumnetworks.com/wri  |   |   |   |                               |                         |  |
|       |                   |                  | Logo to be displayed on the splash page<br>https://www.cambiumnetworks.com/3d-   |   |   |   |                               |                         |  |
|       | Background I      | Image            |  |   |   |   |                               |                         |  |
|       |                   |                  |  |   | played on the splash page   |   |                               |                         |  |
|       | Success A         | Action           | Internal   | Logout Page   R   | Redirect user to External   | URL 🔍 Redi  | rect user to Orig             | inal URL                |  |
|       | Success me        | ssage            | You are  | free to Use Wi-   | Fi services   |   |                               |                         |  |
|       | Re                | direct           | ✓ HTTP-o   | nly Enable redire   | ction for HTTP packets or   | nly   |                               |                         |  |
|       | Redirect User     | Page             | 1.1.1.1  |   |   |   |                               |                         |  |
|       |                   |                  | Configure  | IP address for red  | irecting user to guest port   | al splash page  | )                             |                         |  |
|       | Proxy Redirection | n Port           |  | Port number(1   | 1 to 65535)   |   |                               |                         |  |
|       | Session Tir       | neout            | 28800  | Session time  | in seconds (60 to 259200  | ))  |                               |                         |  |
|       | Inactivity Tir    | neout            | 1800       Inactivity time in seconds (60 to 2592000)         Use guest-access only as fallback for clients failing MAC-authentication |   |   |   |                               |                         |  |
|       | MAC Authentio     | cation<br>Ilback |  |   |   |   |                               |                         |  |
|       | Extend Inte       | erface           |  | Configure the   | interface which is extende  | ed for guest ad   | ccess                         |                         |  |
|       |                   |                  | Save   | Cancel  |   |   |                               |                         |  |

| Cambium Networks | cnPilot E400 - E400-AFA308 |                        | 🙂 Reboot 🕞 Logo  |
|------------------|----------------------------|------------------------|--|
| LIII Dashboard   | Services                   |                        |  |
| 🔁 Monitor 🗸      | Network Bonjour            |                        |  |
| 🜣 Configure 🗸    | C LDAP                     |                        |  |
| System           |                            | ww.cambiumnetworks.cor | Configure LDAP server IP address<br>Configure LDAP server port address               |
| ∲ Radio          | Server Port 3              | 89                     | Configure EDAL Server port address   |
| 🗢 WLAN           | NAT Logging                |                        |  |
| 击 Network        | Enable                     |                        |  |
| 🚔 Services       | Server IP                  |                        | Configure NAT Logging server IP address  |
| ⋣ Operations     | Server Port                |                        | Configure NAT Logging server port address<br>Configure NAT Logging interval (5-3600) |
| 🗲 Troubleshoot - |                            |                        | seconds  |

### Authentication - Redirected Splash Page

| Welcome to Cambium<br>Networks       Free Wi-Fi Hotspot Services       Username   |
|---|
| Password Terms and Agreement Login  |
| You hereby expressly<br>acknowledge and agree that<br>there are significant security,<br>privacy and confidentiality risks<br>inherent in accessing or<br>transmitting information through<br>the internet. |
|   |



### Successful Login - Redirected Splash Page

### Access Policy - Local Guest Account

### Configuration

| Basic | Radius Server Gue  | est Access   | Usage Limits   | Scheduled Access   | Access                                 | Passpoint                        | Delete    |  |  |  |
|-------|--|--|--|--|--|----------------------------------|-----------|--|--|--|
|       | Enable       Internal Access Point       External Hotspot       cnMaestro         Access Policy       Clickthrough       Splash-page where users accept terms & conditions to get on the network         Radius       Splash-page with username & password, authenticated with a RADIUS server |  |  |  |  |                                  |           |  |  |  |
|       |  |  | Redirect users to a  | username & password<br>login page for authent<br>direct users to a login p | cation by a LDAF                       | <sup>o</sup> server              |           |  |  |  |
|       | User Name<br>User Password   |  |  |  | ternal radius gue<br>ternal radius gue | st user name<br>st user password |           |  |  |  |
|       | Redirect Mode  | -  | Use HTTP URLs fo<br>Use HTTPS URLs   |  |  |                                  | _         |  |  |  |
|       | Redirect Hostname  | Redirect H   | ostname for the spla   | ash page (up to 255 ch   | ars)                                   |                                  |           |  |  |  |
|       | Title  |  | Welcome to Cambium Networks<br>Title text in splash page (up to 255 chars) |  |  |                                  |           |  |  |  |
|       | Contents   | Free Wi-Fi Hotspot Services Main contents of the splash page (up to 255 chars) |  |  |  |                                  |           |  |  |  |
|       | Terms  |  |  | cknowledge and ag<br>n the splash page (up t                               |  | e are significan                 | t securit |  |  |  |
|       | Logo   | · ·  | ww.cambiumnet<br>e displayed on the s                                      |  |  |                                  |           |  |  |  |
|       | Background Image   |  | ww.cambiumnet  | tworks.com/3d  | ge                                     |                                  |           |  |  |  |
|       | Success Action   | Internal   | Logout Page 🔍 R  | edirect user to Exterr   | al URL 🔍 Redii                         | rect user to Origin              | nal URL   |  |  |  |
|       | Success message  | You are  | free to Use Wi-F   | Fi services  |  |                                  |           |  |  |  |
|       | Redirect<br>Redirect User Page   | 1.1.1.1  |  | ction for HTTP packets<br>recting user to guest po                         |  |                                  |           |  |  |  |
| P     | roxy Redirection Port  |  | Port number(1  | to 65535)  |  |                                  |           |  |  |  |
|       | Session Timeout  | 28800  | Session time i   | n seconds (60 to 25920   | 000)                                   |                                  |           |  |  |  |
|       | Inactivity Timeout   | 1800   | Inactivity time  | in seconds (60 to 2592   | 000)                                   |                                  |           |  |  |  |
|       | MAC Authentication<br>Fallback   | 🗖 Use gu   | est-access only as t   | fallback for clients failin  | g MAC-authentic                        | ation                            |           |  |  |  |
|       | Extend Interface   |  | Configure the  | interface which is exter   | ded for guest ac                       | cess                             |           |  |  |  |
|       |  | Save   | Cancel   |  |  |                                  |           |  |  |  |



### Authentication - Redirected Splash Page

Successful Login - Redirected Splash Page



# Chapter 17: Guest Access Portal- EXTERNAL

### Introduction

Guest access WLAN is designed specifically for BYOD (Bring your own device) setup, where large organizations have both staff and guests running on same WLAN or similar WLANs. Cambium Networks provides different options to the customers to achieve this based on where the captive portal page is hosted and who will be validating and performing authentication process.

External Hotspot is a smart Guest Access provision supported by cnPilot devices. This method of Guest Access provides a flexibility of integrating an external 3<sup>rd</sup> party Web/Cloud hosted captive portal, fully customized. More details on third party vendors who are integrated and certified with Cambium are listed in the URL https://www.cambiumnetworks.com/wifi\_partners/.

### **Configurable Parameters**

Figure 165 displays multiple configurable parameters supported for External Guest Access hosted on AP.

| asic | Radius Server                            | Guest Access                                  | Usage Limits   | Scheduled Access  | Access                          | Passpoint               |      |
|------|--|---|--|---|---------------------------------|-------------------------|------|
|      |  |   |  |   |                                 |                         | Dele |
|      | Enabl<br>Portal Mod                      | -   | Access Point 🖲 Ext   | ernal Hotspot 🔍 cnMaes  | stro                            |                         |      |
|      | Access Polic                             | <ul> <li>Radius</li> <li>LDAP</li> </ul>      | Splash-page with us<br>Redirect users to a lo<br>lest Account Redi | where users accept terms<br>sername & password, auth<br>gin page for authentication<br>rect users to a login page f | enticated with<br>h by a LDAP s | a RADIUS serv<br>server | ver  |
|      | Redirect Mod                             |   | Use HTTP URLs for<br>Use HTTPS URLs f                              |   |                                 |                         |      |
|      | Redirect Hostnam                         |   | stname for the splasi  | h page (up to 255 chars)  |                                 |                         |      |
| W    | /ISPr Clients Externa<br>Server Logi     |   |  |   |                                 |                         |      |
|      | External Page<br>UR                      |   | /external.com/log  | gin.html  |                                 |                         |      |
|      | External Portal Pos<br>Through cnMaestre |   |  |   |                                 |                         |      |
|      | External Portal Typ                      | e Standard                                    |  | <ul> <li>External Portal</li> </ul>   | Type Standar                    | rd/XWF                  |      |
|      | Success Action                           | n <ul> <li>Internal I</li> <li>URL</li> </ul> | Logout Page 🔍 Red  | direct user to External UI  | RL   Redire                     | ct user to Origir       | nal  |
|      | Success messag                           | e You are f                                   | ree to Use Wi-Fi   | services  |                                 |                         |      |
| Re   | edirection URL Quer<br>Strin             | g 🛛 RSSI //                                   | nclude rssi value of c   | in the redirection url quer<br>lient in the redirection url q<br>cation in the redirection url                      | uery strings                    |                         |      |
|      | Redirec                                  | t 🛛 HTTP-or                                   | nly Enable redirecti   | on for HTTP packets only  |                                 |                         |      |
|      | Redirect User Pag                        |   | IP address for redire  | cting user to guest portal s  | plash page                      |                         |      |
| Pi   | roxy Redirection Po                      | rt  | Port number(1 to   | 65535)  |                                 |                         |      |
|      | Session Timeou                           | ıt 28800                                      | Session time in  | seconds (60 to 2592000)   |                                 |                         |      |
|      | Inactivity Timeou                        | <b>It</b> 1800                                | Inactivity time in   | seconds (60 to 2592000)   |                                 |                         |      |
|      | MAC Authenticatio<br>Fallbac             | 5   | est-access only as fal   | lback for clients failing MA  | C-authenticati                  | ion                     |      |
|      | Extend Interfac                          | e   | Configure the in   | terface which is extended i   | for guest acce                  | 255                     |      |
|      |  | Save  | Cancel   |   |                                 |                         |      |
|      |  |   |  |   |                                 |                         |      |

#### Figure 165 Configure: WLAN > Guest Access > External Access Point parameter

### Access policy

#### Click through

When this policy is selected, user will get a login page to accept "Terms and Conditions" to get access to network. No additional authentication is required.

RADIUS

When this policy is selected, user will be prompted for credentials, which is authenticated by Radius server. Radius server details can be configured on device at **Configure > WLAN > RADIUS**.

LDAP

When this policy is selected, user will be prompted for credentials, which is authenticated by LDAP/AD server. LDAP server details can be configured on device at **Configure > WLAN > Guest** Access > LDAP.

Local Guest Account

When this policy is selected, username and password is configured on device and it can be used as credentials for all wireless users connected to this WLAN profile to gain internet access.

### WISPr

WISPr Clients External Server Login

Provision to enable re-direction of guest access portal URL obtained through WISPr.

### External Portal Post Through cnMaestro

This is required when HTTPS is only supported by external guest access portal. This option when enabled minimizes certification. Certificate is required to install only in cnMaestro On-Premises.

### External Portal Type

Two modes of portal types are supported by cnPilot products.

#### Standard

This mode is selected, for all third-party vendors whose Guest Access services is certified and integrated with cnPilot products.

#### XWF

This mode is selected for Facebook Express Wi-Fi deployment.

### Redirect Parameters

#### Redirect hostname

Note

User can configure a friendly hostname, which is added in DNS server and is resolvable to cnPilot IP address. This parameter once configured will be replaced with IP address in the redirection URL provided to wireless stations.



This can be used to mask the IP address of the AP with some string.

#### Success action

Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL:

#### • Internal logout Page

After successful login, Wireless client is redirected to logout page hosted on AP.

• Redirect users to external URL

Here users will be redirected to URL which we configured on device as below:

• Redirect users to Original URL

Here users will be redirected to URL that is accessed by user before successful captive portal authentication.

#### Figure 166 Success action

Success Action 
Internal Logout Page 

Redirect user to External URL 

Redirect user to Original URL

#### Redirect

By default, captive portal redirection is trigger when user access either HTTP or HTTPs WWW. If enabled, redirection to Captive Portal Splash Page is triggered when a HTTP WWW is accessed by end user.

#### Figure 167 Redirect

Redirect ITP-only Enable redirection for HTTP packets only

#### Redirect Mode

There are two redirect modes available:

HTTP Mode

When enabled, AP sends a HTTP POSTURL to the client.

HTTP(s) Mode

When enabled, AP sends HTTPS POST URL to the client

#### Proxy redirection port

Proxy redirection port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.

#### Redirect user page

IP address configured in this field is used as logout URL for Guest Access sessions. IP address configured should be not reachable to internet.

#### Figure 168 Redirect user page

| Redirect User Page | 1.1.1.1  |         |  |
|--------------------|--|---------|--|
|                    | Configure IP address for redirecting user to guest portal spla | sh page |  |

Logout re-direction URLs are as follows:

http(s)://<Redirect user Page>/logout

#### Redirection URL Query String

Following information is appended in the redirection URL, if "Prefix Query Strings in Redirect URL" is enabled.

- Client IP
- RSSI
- AP Location

### Success Message

This we can configure so that we can display success message on the splash page after successful authentication

#### Figure 169 Success Message

| Success message |  |
|-----------------|--|
|                 |  |

### Timeout

#### Session

This is the duration of time which wireless client will be allowed internet after guest access authentication.

#### Figure 170 Configure: WLAN > Guest Access > Session timeout

| Session Timeout | 28800 | Session time in seconds (60 to 2592000) |
|-----------------|-------|---|
|                 | 20000 | Session lime in Seconds (00 to 2092000) |

#### Inactivity

This is the duration of time after which wireless client will be requested for re-login.

Figure 171 Configure: WLAN > Guest Access > Inactivity timeout

| Inactivity Timeout | 1800 | Inactivity time in seconds (60 to 2592000) |
|--------------------|------|--|
|                    |      |  |

### MAC Authentication fallback

It is a fall back mechanism in which wireless clients will be redirected to Guest access login Page after Radius based Mac authentication failure. This means When AP detects RADIUS authentication has failed for a wireless client, AP will send a HTTTP Post w.r.t redirection URL to the client for guest access authentication

Figure 172 Configure: WLAN > Guest Access > MAC Authentication fallback

| MAC Authentication Fallback |  | Use guest-access only as fallback for clients failing MAC-authentication |
|-----------------------------|--|--|
|-----------------------------|--|--|

### Extended interface

Provision to support Guest Access on Ethernet interface.

Figure 173 Configure: WLAN > Guest Access > Extended interface

| Configure the interface which is extended for guest access |
|--|
|  |
|  |

### Whitelist

Provision to configure either Ips or URLs to bypass traffic, therefor user can access those Ips or URLs without Guest Access authentication.

### Captive portal bypass user agent

Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.

|        |              | 1         | T           |       |
|--------|--------------|-----------|-------------|-------|
|        | Agent String |           |             |       |
| Statu  | s Code       | 200       | Ŧ           |       |
| нтм    | Response     |           |             |       |
|        |              |           |             | h     |
|        |              | Save      |             |       |
| Ind.:: | Match        | ✓ Http C. | Html Reply  | ~ Act |
|        |              |           |             |       |
|        | No Use       | er Agen   | t rule avai | lable |
|        | 110 000      | on rigen  |             |       |
|        |              |           |             |       |
|        |              |           |             |       |
|        |              |           |             |       |
|        |              |           |             |       |

Figure 174 Configure: WLAN > Guest Access > Captive portal bypass user agent

## Configuration examples

This section briefs about configuring different methods of External Guest Access captive portal services hosted on AP.
# Access Policy - Clickthrough

# Configuration

|   | lest Access  | Usage Limits  | Scheduled Access   | Access  | Passpoint                                      | De         |
|---|--|---|--|---|--|------------|
| Enable  |  |   |  |   |  |            |
| Endble  | _  | _   |  |   |  |            |
| Portal Mode   | lntern   | al Access Point   | External Hotspot   | laestro   |  |            |
| Access Policy   | C Radiu  | IS Splash-page with<br>Redirect users to  | nge where users accept te<br>th username & password,<br>a login page for authentic<br>Redirect users to a login page   | authenticated<br>ation by a LD/   | with a RADIUS s<br>AP server                   | server     |
| Redirect Mode   | -  | Use HTTP URLs<br>S Use HTTPS UF   |  |   |  |            |
| Redirect Hostname   |  | Hostname for the sp   | plash page (up to 255 cha  | rs)   |  |            |
| WISPr Clients Externa<br>Server Logir   |  |   |  |   |  |            |
| External Page   |  | /region1.purplep  | oortal.net/access/   |   |  |            |
| URL   | URL of e   | xternal splash page   |  |   |  |            |
| External Portal Post<br>Through cnMaestro   |  |   |  |   |  |            |
|   |  |   |  |   |  |            |
| External Portal Type  | Standa   | ard   | <ul> <li>Exteri</li> </ul>   | nal Portal Type   | Standard/XWF                                   |            |
| External Portal Type<br>Success Actior  |  |   | Redirect user to Extern  |   |  | iginal URL |
|   | n O Interr   |   |  |   |  | iginal URL |
| Success Actior<br>Prefix Query Strings ir   | n ○ Intern   |   | Redirect user to Externa   |   |  | iginal URL |
| Success Actior<br>Prefix Query Strings ir<br>Redirect URL   | https://   | al Logout Page (*)<br>/www.google.com<br>IP Include IP of c<br>Include rssi value   | Redirect user to Externa   | al URL Red<br>uery strings<br>url query strings   | direct user to Or                              | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query  | <ul> <li>Interr</li> <li>https://</li> <li>Client</li> <li>RSSI</li> <li>AP Lo</li> </ul>  | al Logout Page<br>/www.google.com<br>IP Include IP of co<br>Include rssi value<br>pocation Include AF   | Redirect user to Externa<br>n<br>lient in the redirection url o<br>of client in the redirection  | al URL Red<br>uery strings<br>url query string<br>n url query string  | direct user to Or                              | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String  | <ul> <li>Interr</li> <li>Inter</li> <li>Inter</li> <li>Inter</li> <li>Inter</li> <li>Inter<td>al Logout Page<br/>/www.google.cor<br/>IP Include IP of co<br/>Include rssi value<br/>ocation Include AF<br/>-only Enable redir</td><td>Redirect user to Externa<br/>m<br/>lient in the redirection url of<br/>of client in the redirection<br/>clocation in the redirection</td><td>al URL Red<br/>uery strings<br/>url query string<br/>n url query string</td><td>direct user to Or</td><td>iginal URL</td></li></ul> | al Logout Page<br>/www.google.cor<br>IP Include IP of co<br>Include rssi value<br>ocation Include AF<br>-only Enable redir  | Redirect user to Externa<br>m<br>lient in the redirection url of<br>of client in the redirection<br>clocation in the redirection   | al URL Red<br>uery strings<br>url query string<br>n url query string  | direct user to Or                              | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String<br>Redirect  | h Interr<br>https://<br>Client<br>RSSI<br>AP Lc<br>HTTP  | al Logout Page<br>/www.google.cor<br>IP Include IP of c.<br>Include rssi value<br>pocation Include AF<br>-only Enable redir   | Redirect user to Externa<br>m<br>lient in the redirection url of<br>of client in the redirection<br>clocation in the redirection   | al URL Red<br>uery strings<br>url query string<br>n url query stri<br>nly   | direct user to Or<br>gs<br>ings                | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String<br>Redirect  | <ul> <li>Interr</li> <li>https://</li> <li>Client</li> <li>RSSI</li> <li>AP Lc</li> <li>HTTP</li> <li>1.1.1.1</li> <li>Configu</li> </ul>  | al Logout Page<br>/www.google.cor<br>IP Include IP of c.<br>Include rssi value<br>pocation Include AF<br>-only Enable redir   | Redirect user to Externation<br>m<br>lient in the redirection url of<br>of client in the redirection<br>P Location in the redirection<br>ection for HTTP packets of<br>directing user to guest por   | al URL Red<br>uery strings<br>url query string<br>n url query stri<br>nly   | direct user to Or<br>gs<br>ings                | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String<br>Redirect<br>Redirect User Page  | https://   | Aal Logout Page<br>//www.google.com<br>IP Include IP of cl<br>Include rssi value<br>ocation Include AF<br>-only Enable redir<br>re IP address for re<br>Port number                 | Redirect user to Externation<br>m<br>lient in the redirection url of<br>of client in the redirection<br>P Location in the redirection<br>ection for HTTP packets of<br>directing user to guest por   | al URL Red<br>uvery strings<br>url query string<br>n url query stri<br>nly<br>tal splash pag                              | direct user to Or<br>gs<br>ings                | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String<br>Redirect<br>Redirect User Page<br>Proxy Redirection Port  | https://   | Aal Logout Page<br>/www.google.cor<br>IP Include IP of co<br>Include rssi value<br>ocation Include AF<br>-only Enable redir<br>re IP address for re-<br>Port number<br>Session time | Redirect user to Externation<br>m<br>lient in the redirection url of<br>of client in the redirection<br>P Location in the redirection<br>ection for HTTP packets of<br>directing user to guest por<br>(1 to 65535)   | al URL Red<br>uery strings<br>url query string<br>n url query stri<br>nly<br>tal splash pag                               | direct user to Or<br>gs<br>ings                | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String<br>Redirect<br>Redirect User Page<br>Proxy Redirection Port<br>Session Timeout   | https://<br>https://<br>Client<br>RSSI<br>AP LC<br>HTTP<br>1.1.1.1<br>Configu<br>28800<br>1800<br>Use g  | Aal Logout Page (*)   | Redirect user to Externation<br>m<br>lient in the redirection url of<br>of client in the redirection<br>P Location in the redirection<br>ection for HTTP packets of<br>directing user to guest por<br>(1 to 65535)<br>e in seconds (60 to 259200                               | al URL Red<br>uery strings<br>url query string<br>n url query strin<br>nly<br>tal splash pag<br>00)                       | direct user to Or<br>gs<br>ings                | iginal URL |
| Success Action<br>Prefix Query Strings in<br>Redirect URL<br>Redirect URL<br>Redirection URL Query<br>String<br>Redirect<br>Redirect User Page<br>Proxy Redirection Port<br>Session Timeout<br>Inactivity Timeout<br>MAC Authentication | <ul> <li>Interr</li> <li>Inter</li> <li>Interr</li> <li>Interr</li> <li>Interr</li> <li>Inter&lt;</li></ul>  | Aal Logout Page (*)   | Redirect user to Externation<br>m<br>lient in the redirection url of<br>of client in the redirection<br>P Location in the redirection<br>ection for HTTP packets of<br>directing user to guest por<br>(1 to 65535)<br>e in seconds (60 to 259200<br>e in seconds (60 to 259200 | al URL Red<br>uery strings<br>url query string<br>n url query strin<br>nly<br>tal splash pag<br>00)<br>00)<br>MAC-authent | direct user to Or<br>gs<br>ngs<br>e<br>ication | iginal URL |

| Choose how to access                         | our WiFi network | Free Wi-Fi Hotpspot | Services |  |
|--|------------------|---------------------|----------|--|
| f)<br>ebook                                  | Form             |                     |          |  |
|  |                  |                     |          |  |
|  |                  |                     |          |  |
| y Wi-Fi Services<br>ered by Cambium Networks |                  |                     |          |  |
|  |                  |                     |          |  |
|  |                  |                     |          |  |

Successful Login - Redirected Splash Page

| facebook                        | Create New Account                                     |
|---------------------------------|--|
|                                 |  |
|                                 | Log in to Facebook                                     |
|                                 | Email address or phone number Password                 |
|                                 | Log in   |
|                                 | Forgotten account? - Sign up for Facebook<br>Not now   |
|                                 |  |
|                                 |  |
|                                 |  |
| English (UK) रुत्रूख اربو मराठी | ອັలుగు हिन्दी தமிழ் മലയാളം वाश्ना ગુજરાતી र्यत्तण्यी 🔶 |

# Chapter 18: Guest Access - cnMaestro

Cambium supports end-to-end Guest Access Portal services with combination of cnPilot and cnMaestro. cnMaestro supports various types of authentication mechanism for wireless clients to obtain Internet access. Following is an overview of types of Guest Access Portal services supported in cnMaestro:

- Free
  - Authentication Mechanisms
    - Social Login
      - ✤ Google
      - Twitter
      - Facebook
      - ✤ Office365
    - > SMS Authentication
      - SMS Country
      - SMS Gupchup
      - Twilio
      - Victory Link SMS
      - Fast SMS
- Paid
  - Paypal Payment Gateway
  - Ippay Gateway
  - o Quickpay Gateway
  - o Orange Gateway
  - o mPesa Gateway
- Voucher

This section describes how to configure Guest Access using cnMaestro.

# **Configurable Parameters**

For Guest Access to be operational, both cnPilot and cnMaestro has to be configured for Guest Access Portal services. Below are the configurable parameters:

#### cnPilot

Figure 175 displays multiple configurable parameters supported for cnMaestro Guest Access hosted on AP.

| Basic Radius Server            | Guest Access | Usage Limits                              | Scheduled Access             | Access                        | Passpoint | Delete |
|--------------------------------|--------------|---|------------------------------|-------------------------------|-----------|--------|
| Enable                         |              |   |                              |                               |           |        |
| Portal Mode                    | e 🔍 Internal | Access Point   Ex                         | ternal Hotspot 🖲 cnMae       | estro                         |           |        |
| Guest Portal<br>Name           |              | aestro-guest-por<br>rtal Name which is he |                              |                               |           |        |
| Redirect                       | t            | nly Enable redirect                       | tion for HTTP packets only   | ,                             |           |        |
| Redirect User Page             |              | IP address for redire                     | ecting user to guest portal  | enlash naria                  |           |        |
| Proxy Redirection Port         |              | Port number(1                             |                              | spiasii page                  |           |        |
| Inactivity Timeout             | t 1800       | Inactivity time in                        | n seconds (60 to 2592000)    | )                             |           |        |
| MAC Authentication<br>Fallback | -            | est-access only as fa                     | llback for clients failing M | AC-authentica                 | tion      |        |
| Extend Interface               | •            | Configure the in                          | nterface which is extended   | for guest acc                 | ess       |        |
|                                | Save         | Cancel                                    |                              |                               |           |        |
|                                | Add Whi      | telist Captive Po                         | ortal bypass User Agent      |                               |           |        |
|                                |              | dress or<br>in Name                       |                              |                               | Save      |        |
|                                | IP Add       | ress   Domain Name                        | 9                            | ~ Action                      |           |        |
|                                |              |   |                              |                               |           |        |
|                                |              | No wh                                     | ite list availal             | ble                           |           |        |
|                                |              |   |                              |                               |           |        |
|                                |              |   |                              |                               |           |        |
|                                |              |   |                              | <ul> <li>items per</li> </ul> | - page    |        |
|                                |              |   |                              |                               |           |        |

Figure 175 Configure: WLAN > Guest Access > cnMaestro parameter

## cnMaestro

Table 61 lists configurable parameters that are available under Services > Guest Access Portal tab:

| Parameters                    | Description Range Def   |   |          |  |  |  |  |  |
|-------------------------------|---|---|----------|--|--|--|--|--|
| Services > Guest Ad           | Services > Guest Access Portal > <gap profile=""> Basic</gap>   |   |          |  |  |  |  |  |
| Name                          | Provision to configure the name of the Guest Access<br>Portal services  | _ | _        |  |  |  |  |  |
| Description                   | Provision to add brief details as per customer requirement  | - | _        |  |  |  |  |  |
| Client Login Event<br>Logging | Enabling this will provision cnMaestro to record all the client events and their details. Client details available when this is enabled are as follows: | _ | Disabled |  |  |  |  |  |
|                               | Client MAC  |   |          |  |  |  |  |  |
|                               | • Portal  |   |          |  |  |  |  |  |
|                               | • WLAN  |   |          |  |  |  |  |  |
|                               | Access Point  |   |          |  |  |  |  |  |
|                               | Voucher Code  |   |          |  |  |  |  |  |
|                               | Login Time  |   |          |  |  |  |  |  |
|                               | Access Type   |   |          |  |  |  |  |  |
|                               | • Email   |   |          |  |  |  |  |  |
|                               | Mobile Number   |   |          |  |  |  |  |  |

| -#         | <u>Guest Access Portal</u> > Test_Cambium_Free   |
|------------|--|
| ŵ          | Basic         Access         Splash         Sessions   |
| <i>E</i> S | *Name: Test_Cambium_Free   |
|            | Description: This GAP Portal enables wireless clients to gain<br>internet access for a certain period configured<br>in session duration. |
| S.         | in session duration.   |
| ŝ          | Client Login Event Logging   |
| 段          | Save   |
| <b>∆</b> Я |  |

Figure 176 Configure: Services > Guest Access > Basic parameters

| Table 62 Configure: Services 3 | > Guest Access > / | Access > Free parameters |
|--------------------------------|--------------------|--------------------------|
|--------------------------------|--------------------|--------------------------|

| Parameters   | Description  | Range     | Default  |  |  |
|--|--|-----------|----------|--|--|
| Services > Guest A                                     | ccess Portal > <gap profile=""> Access &gt; Free</gap>   |           |          |  |  |
| Enable Free<br>Access                                  | _  | Disabled  |          |  |  |
| Enable Logout<br>Functionality for<br>the guest client | Provision to provide user Internet access for complete<br>session duration within renewal frequency. Internet<br>access timer is calculated based on real time user has<br>used. User can logout multiple times within renewal<br>frequency. | _         | Disabled |  |  |
| Bypass Captive<br>Portal Detection                     | Provision to disable Captive Network Assistant (I).  | _         | Disabled |  |  |
| Services > Guest A                                     | ccess Portal > <gap profile=""> Access &gt; Free &gt; Client Session</gap>   | on        |          |  |  |
| Session Duration                                       | The duration for which the client is provided internet access.   | 1-2628000 | _        |  |  |
| Renewable<br>Frequency                                 |  |           |          |  |  |
| Services > Guest A                                     | ccess Portal > <gap profile=""> Access &gt; Free &gt; Client Rate</gap>  | Limit     | 1        |  |  |

| Parameters                    | Description  | Range     | Default  |
|-------------------------------|--|-----------|----------|
| Downlink                      | Provision to limit downlink speed from Access Point<br>to wireless client when client is authenticated to gain<br>internet access.                                     | _         | -        |
| Uplink                        | Provision to limit uplink speed from wireless client to<br>Access Point when client is authenticated to gain<br>internet access.                                       | _         | _        |
| Services > Guest A            | ccess Portal > <gap profile=""> Access &gt; Free &gt; Client Quot</gap>  | a Limit   |          |
| Quota Type                    | <ul><li>Provision to limit the bandwidth of wireless client.</li><li>Two categories are supported based on Data quantity:</li><li>Directional</li></ul>                | _         | None     |
|                               | <ul> <li>Downlink</li> <li>Uplink</li> </ul>   |           |          |
|                               | • Total  |           |          |
| Services > Guest A            | ⊥<br>ccess Portal > <gap profile=""> Access &gt; Free &gt; Social Logir</gap>  | 1         | I        |
| Guest Portal<br>Hostname / IP | Provision to configure the hostname that is share with<br>supported social login website APIs. More details on<br>supported social logins are provided in Social Login | -         | Disabled |
|                               | For each type of Social login required, respective<br>configuration parameters needs to be configured.<br>These parameters vary based on Social Login.                 |           |          |
| Services > Guest A            | ccess Portal > <gap profile=""> Access &gt; Free &gt; SMS Auther</gap>   | ntication |          |
| Enable                        | Provision to enable SMS Authentication   | -         | Disabled |
| SMS Gateway<br>Provider       | Provision to configure SMS gateway. More details on supported SMS gateway are provided in SMS Authentication.  | _         | -        |
|                               | For each type of Gateway vendors, configuration parameters vary and needs to be configured as per requirement.   |           |          |
| Services > Guest A            | ccess Portal > <gap profile=""> Access &gt; Free &gt; Add Whiteli</gap>  | st        |          |
| IP Address /<br>Domain Name   | Provision to allow internet traffic, when user is not authenticated.   | -         | -        |

|            | Cambium Networks         |   |                 |                          | Ĵ.                   | $\bigcirc$   | S=0          | 3<br> | 04 |
|------------|--------------------------|---|-----------------|--------------------------|----------------------|--------------|--------------|-------|----|
| -14        | Guest Access Po          | <u>ortal</u> > test   |                 |                          |                      |              |              |       | C  |
|            | Basic Access Spla        |   |                 |                          |                      |              |              |       |    |
| ŵ          | Free Paid Vouchers       |   |                 |                          |                      |              |              |       |    |
| E.S.       | Enable Free Access       |   |                 |                          |                      |              |              |       |    |
|            | _                        | tionality for the guest client                                    |                 |                          |                      |              |              |       |    |
| S.         | Bypass Captive Port      | al Detection  |                 |                          |                      |              |              |       |    |
|            | 🗆 Client Session         |   |                 |                          |                      |              |              |       |    |
| ŝ          | Renewal                  | 10  | Min(s) 🗸        | Valid range is 1-262800  | 00 minutes           |              |              |       |    |
| 岛          | Frequency:               |   |                 |                          |                      |              |              |       |    |
| <b>∆</b> Я | Session Duration:        | 10  | Min(s) 🗸        | Valid range is 1-262800  | 00 minutes           |              |              |       |    |
| 2427       | 🖯 Client Rate Limit      |   |                 |                          |                      |              |              |       |    |
|            | Downlink:                | 10  | Kbps            |                          |                      |              |              |       |    |
|            | Uplink:                  | 10  | Kbps            |                          |                      |              |              |       |    |
|            |                          |   |                 |                          |                      |              |              |       |    |
|            | 🖯 Client Quota Limit     | Ľ   |                 |                          |                      |              |              |       |    |
|            | Quota Type:              | None 🕶  |                 |                          |                      |              |              |       |    |
|            | 🖯 Social Login           |   |                 |                          |                      |              |              |       |    |
|            | Guest Portal             | qa-us-e1-guest.cloud.cambiu                                       | 0               |                          |                      |              |              |       |    |
|            | Hostname / IP:           | Note: Captive portal bypass will b                                | o onablad if co | cial login with Eacobook | or Coogle is enabled | d This is ra | quirod as th | 20    |    |
|            |                          | Captive-portal Network Assistant (<br>provided by these services. |                 |                          |                      |              |              |       |    |
|            |                          | Google  |                 |                          |                      |              |              |       |    |
|            |                          | Twitter   |                 |                          |                      |              |              |       |    |
|            |                          | Facebook Office 365   |                 |                          |                      |              |              |       |    |
|            | _                        |   |                 |                          |                      |              |              |       |    |
|            |                          | n   |                 |                          |                      |              |              |       |    |
|            |                          | Enable  |                 |                          |                      |              |              |       |    |
|            | SMS Gateway<br>Provider: | Twilio 🔻  |                 |                          |                      |              |              |       |    |
|            | 🗆 Add Whitelist          |   |                 |                          |                      |              |              |       |    |
|            | IP Address               |   |                 | Add                      |                      |              |              |       |    |
|            | ID Addre                 | Name:   |                 | Delete                   |                      |              |              |       |    |
|            |                          |   |                 |                          |                      |              |              |       |    |
|            | NoIP                     | Address or Domain N   | lame Av         | ailable                  |                      |              |              |       |    |
|            |                          |   |                 |                          |                      |              |              |       |    |
|            |                          |   |                 |                          |                      |              |              |       |    |
|            | <                        |   |                 | $\rightarrow$            |                      |              |              |       |    |
|            |                          |   |                 |                          |                      |              |              |       |    |
|            | Save                     |   |                 |                          |                      |              |              |       |    |

Figure 177 Configure: Services > Guest Access > Access > Free parameters

| Parameter         | Description  | SMS Gateway Provider |                |                |        |                     |            |                    |
|-------------------|--|----------------------|----------------|----------------|--------|---------------------|------------|--------------------|
|                   |  | Fast<br>SMS          | SMS<br>Country | SMS<br>Gupshup | Twilio | Victory<br>Link SMS | SMS<br>API | Generic<br>SMS API |
| Enable            | It indicates to<br>enable the<br>SMS<br>Authentication<br>feature.   | ~                    | ~              | ~              | ~      | ~                   | ×          | X                  |
| Username          | Indicates the<br>username of<br>the vendor.  | ~                    | ~              | ~              | x      | ~                   | x          | X                  |
| Sender<br>ID/Name | It is the name<br>or number<br>which flashes<br>on the<br>recipients<br>mobile phone<br>when they<br>receive SMS.<br>This is<br>optional not<br>mandatory. | ~                    | ~              | ~              | X      | ~                   | ~          | X                  |
| API Key           | It's a token<br>which is<br>provided by<br>vendors.  | ~                    | x              | x              | x      | X                   | x          | X                  |
| Account<br>Type   | It shows type<br>of accounts<br>such as<br>International,<br>OTP,<br>Promotional<br>and<br>Transaction.  | ~                    | X              | X              | X      | X                   | x          | X                  |
| OTP<br>Template   | The template<br>with which<br>SMS has to be<br>sent.   | ~                    | ~              | ~              | ~      | ~                   | ~          | x                  |
| Password          | It indicates the password.   | X                    | ~              | ~              | x      | ~                   | X          | X                  |
| Country<br>Code   | It enables to<br>select country<br>code based on<br>deployments.   | X                    | ~              | ~              | x      | X                   | ~          | X                  |

#### Table 63 Configure: Services > Guest Access > Access > Free > SMS

| Parameter                              | Description                                  |             |                | SMS G          | iateway F | Provider            |            |                    |
|--|--|-------------|----------------|----------------|-----------|---------------------|------------|--------------------|
|  |  | Fast<br>SMS | SMS<br>Country | SMS<br>Gupshup | Twilio    | Victory<br>Link SMS | SMS<br>API | Generic<br>SMS API |
| Auth<br>Token                          | It acts as a password.                       | X           | X              | X              | ~         | X                   | ~          | X                  |
| Account<br>SID                         | It acts as a<br>username.                    | x           | x              | x              | ~         | x                   | x          | x                  |
| From                                   | It enables to<br>select the<br>country code. | x           | X              | X              | ~         | X                   | x          | x                  |
| Language                               | It indicates the<br>Language.                | X           | X              | x              | x         | ~                   | x          | x                  |
| Fast<br>Delivery                       |  | x           | x              | x              | x         | x                   | ~          |                    |
| Template<br>Name                       |  | x           | x              | x              | x         | x                   | ~          |                    |
| SMS<br>Gateway<br>Provider<br>Name     |  | x           | x              | x              | x         | x                   | X          | ~                  |
| HTTP<br>Request<br>Type                |  | x           | x              | x              | x         | x                   | x          | ~                  |
| HTTP<br>Request<br>Header<br>Key       |  | x           | x              | x              | x         | x                   | x          | ~                  |
| HTTP<br>Request<br>Header<br>Key Value |  | x           | x              | x              | x         | x                   | x          | ~                  |
| API URL                                |  | x           | x              | x              | x         | x                   | x          | ~                  |
| API URL<br>Information                 |  | x           | x              | x              | x         | x                   | x          | ~                  |
| Message<br>Parameter<br>Name           |  | x           | x              | x              | x         | x                   | x          | ~                  |
| Mobile<br>Number                       |  | x           | x              | x              | x         | x                   | x          | ~                  |

| Parameter         | Description |             | SMS Gateway Provider |                |        |                     |            |                    |
|-------------------|-------------|-------------|----------------------|----------------|--------|---------------------|------------|--------------------|
|                   |             | Fast<br>SMS | SMS<br>Country       | SMS<br>Gupshup | Twilio | Victory<br>Link SMS | SMS<br>API | Generic<br>SMS API |
| Parameter<br>Name |             |             |                      |                |        |                     |            |                    |

#### Table 64 Configure: Services > Guest Access > Access > Paid parameters

| Parameters                  | Description  | Range | Default  |  |  |  |
|-----------------------------|--|-------|----------|--|--|--|
| Services > Guest Ac         | Services > Guest Access Portal > <gap profile=""> Access &gt; Paid</gap>         |       |          |  |  |  |
| Enable Paid<br>Access       | Provision to enable payment gateway services                                     | -     | Disabled |  |  |  |
| Services > Guest Ac         | ccess Portal > Access > Paid > Paypal Payment Gateway                            |       |          |  |  |  |
| Enable                      | Provision to enable Paypal payment gateway services                              | -     | Disabled |  |  |  |
| Configuration<br>Parameters | For successful Paypal transactions, following parameters needs to be configured: | -     | -        |  |  |  |
|                             | Auto Return URL  |       |          |  |  |  |
|                             | PDT Identity token   |       |          |  |  |  |
|                             | • IPN  |       |          |  |  |  |
| Services > Guest Ac         | ccess Portal > Access > Paid > Ippay Gateway                                     |       |          |  |  |  |
| Enable                      | Provision to enable Ippay payment gateway services                               | -     | Disabled |  |  |  |
| Configuration<br>Parameters | For successful Ippay transactions, following parameters needs to be configured:  | -     | -        |  |  |  |
|                             | Callback URL   |       |          |  |  |  |
|                             | Gateway URL  |       |          |  |  |  |
|                             | Merchant ID  |       |          |  |  |  |
|                             | Customer ID  |       |          |  |  |  |
|                             | Terminal ID  |       |          |  |  |  |
|                             | Password   |       |          |  |  |  |
| Services > Guest Ac         | Services > Guest Access Portal > Access > Paid > QuickPay Gateway                |       |          |  |  |  |
| Enable                      | Provision to enable Quickpay gateway services                                    | _     | Disabled |  |  |  |

| Parameters                  | Description  | Range | Default  |
|-----------------------------|--|-------|----------|
| Configuration<br>Parameters | For successful Ippay transactions, following parameters needs to be configured:        | -     | -        |
|                             | Callback URL   |       |          |
|                             | Merchant ID  |       |          |
|                             | Merchant Key   |       |          |
|                             | Payment Window Agreement ID  |       |          |
|                             | Payment Window API Key   |       |          |
| Services > Guest A          | ccess Portal > Access > Paid > Orange Money  | I     |          |
| Enable                      | Provision to enable Orang Money gateway services                                       | _     | Disabled |
| Configuration<br>Parameters | For successful Orange Money transactions, following parameters needs to be configured: | -     | -        |
|                             | Callback URL   |       |          |
|                             | Merchant Key   |       |          |
|                             | Consumer Key   |       |          |
|                             | • Language   |       |          |
|                             | Currency   |       |          |
|                             | Reference  |       |          |
|                             | Return URL   |       |          |
|                             | Payment URL  |       |          |
| Services > Guest A          | ccess Portal > Access > Paid > mPesa Money   |       |          |
| Enable                      | Provision to enable Orang Money gateway services                                       | -     | Disabled |
| Configuration<br>Parameters | For successful Orange Money transactions, following parameters needs to be configured: | -     | -        |
|                             | Consumer Key   |       |          |
|                             | Consumer Secret  |       |          |
|                             | Short Code   |       |          |
|                             | Validation URL   |       |          |
|                             | Confirmation URL   |       |          |
| Services > Guest A          | ccess Portal > Access > Paid > Plan Details  |       |          |
| Plan Name                   | Configure Internet Plan with name  | -     | -        |

| Parameters             | Description  | Range | Default |
|------------------------|--|-------|---------|
| Plan Cost              | Cost of Internet plan. This field supports to configure<br>various currency types and user can select<br>appropriate currency as per location.   | -     | USD     |
| Session Duration       | <ul> <li>Period in which user is provisioned with Internet access. Following attributes are supported:</li> <li>Minutes</li> <li>Hours</li> <li>Days</li> </ul>  | _     | Minutes |
| Uplink Rate Limit      | Configurable wireless rate limit for the traffic flowing from user to Access Point.  | -     | -       |
| Downlink Rate<br>Limit | Configurable wireless rate limit for the traffic flowing from Access Point to User.  | _     | -       |
| Quota Type             | <ul> <li>Configurable parameter to limit the amount of<br/>Internet data transfer. User data can be limited using<br/>either of the following options:</li> <li>None<br/>There is no limit on Quota. User can use internet<br/>for whole duration configured.</li> <li>Directional <ul> <li>Uplink Quota</li> <li>Downlink Quota</li> </ul> </li> <li>Total<br/>Provision to limit Quota which includes total of<br/>downlink and uplink traffic.</li> </ul> | _     | None    |
| Device Limit           | Number of devices User can connect with current<br>plan. For unlimited client sessions, user has provision<br>to enable unlimited checkbox.  | _     | 1       |

| Guest Access Pr           | ortal > Test_Cambium_Free                                       |   |
|---------------------------|---|---|
| Basic Access Spl          | ash Sessions  |   |
| Free Paid Voucher         | 6   |   |
| C Enable Paid Access      |   |   |
| E Paypal Payment C        | ateway  |   |
|                           | 🕑 Enable  |   |
| Auto return URL:          | https://qa-us-e1-guest.cloud.cambiamnetworks.com/cn-ctir/guest/ | 0   |
| PDT Identity Token:       |   |   |
| IPN:                      | Enable  |   |
|                           | Use Sandbox   |   |
| Get                       | Update Button Code  |   |
| E IPpay Gateway           |   |   |
|                           | 🖉 Enable  |   |
| Callback URL:             | http://gs-us-et.guest.dood.cambiumnetworkc.com/cn-ctb/guest/    | 0   |
| Gateway URL               |   |   |
| Merchant ID               |   |   |
| 🖯 QuickPay Gatewa         |   |   |
|                           | 🖉 Enable  |   |
| Callback URL:             | https://qa-us-et-guest.cloud.cambiumnetworks.com/cn-ctlr/guest/ | 0   |
| Merchant ID               |   |   |
| Merchant Key              | (Construction)  |   |
| Payment Window            |   |   |
| Agreement ID              |   |   |
| Payment Window API<br>Key |   |   |
| Orange Money              | )   |   |
|                           | Enable  |   |
| Callback URL:             | https://go-us-e3-guest.cloud.cambiumnetworks.com/cn-ctk/guest/  | 0   |
| Customer ID               |   |   |
| Terminal ID               |   |   |
| Password                  | 100 A   |   |
| Merchant Key              |   |   |
| Consumer Key              |   |   |
| Language                  | tr.   |   |
| Currency                  | OUV   |   |
| Reference                 |   |   |
|                           |   |   |
| Return URL:               | https://qa-us-e3-guest.cloud.cambiamoetworks.com/assets/viewer/ |   |
| Payment URL:              | Use Sandbox   |   |
| 🖯 mPesa Gateway           |   |   |
|                           | 🖓 Enable  |   |
| Consumer Key              | Call Frances  |   |
| Consumer Secret           |   |   |
|                           | - Band  |   |
| Short Code                |   |   |
| Validation URL:           | https://qa-us-e1-guest.cloud.cambiumnetworks.com/ce-ctli/guest/ |   |
| Confirmation URL:         | https://qa-us-et-guest.doud.cambiumnetworks.com/ca-ctl/guest)   |   |
| Use Sandb                 | 08  |   |
| 🖯 Plan Details            |   |   |
|                           | Add New   | 1   |
|                           |   | and the second se |

Figure 178 Configure: Services > Guest Access > Access > Paid parameters

| Parameters               | Description  | Range | Default  |  |  |  |
|--------------------------|--|-------|----------|--|--|--|
| Services > Guest Ad      | Services > Guest Access Portal > <gap profile=""> Access &gt; Vouchers</gap>   |       |          |  |  |  |
| Enable Voucher<br>Access | Provision to support Voucher based Guest Access<br>Services  | -     | Disabled |  |  |  |
| Plans                    | Provision to add custom user plans. Following are the parameters that are user configurable:   | -     | -        |  |  |  |
|                          | 1. Plan Details  |       |          |  |  |  |
|                          | • Name: Configure user-friendly name to plan.  |       |          |  |  |  |
|                          | • Session Duration: Duration of time user can access Internet. Duration can be specified in terms of Minutes, Hours and Days.  |       |          |  |  |  |
|                          | • Voucher Expiry: Expiry details of voucher,<br>which can be configured for Minutes, Days and<br>Hours. Once voucher expires, user will not be<br>granted internet.  |       |          |  |  |  |
|                          | Rate Limit:  |       |          |  |  |  |
|                          | <ul> <li>Downlink Rate Limit: User can be<br/>restricted with downlink speed. If not<br/>configured, unlimited speed is provided to<br/>user.</li> </ul>   |       |          |  |  |  |
|                          | <ul> <li>Uplink Rate Limit: User can be restricted<br/>with uplink speed. If not configured,<br/>unlimited speed is provided to user.</li> </ul>   |       |          |  |  |  |
|                          | <ul> <li>Quota Type: Configurable parameter to limit<br/>the amount of Internet data transfer. User<br/>data can be limited using either of the<br/>following options:</li> </ul>                            |       |          |  |  |  |
|                          | <ul> <li>None: There is no limit on Quota. User can<br/>use internet for whole duration<br/>configured.</li> </ul>   |       |          |  |  |  |
|                          | o Directional  |       |          |  |  |  |
|                          | <ul> <li>Uplink Quota</li> </ul>   |       |          |  |  |  |
|                          | <ul> <li>Downlink Quota</li> </ul>   |       |          |  |  |  |
|                          | <ul> <li>Total: Provision to limit Quota which<br/>includes total of downlink and uplink<br/>traffic.</li> </ul>   |       |          |  |  |  |
|                          | • Voucher Device Limit: Number of devices<br>allowed to connect using same voucher code.<br>User has provision to configure unlimited. This<br>will allow user to use same voucher for<br>unlimited clients. |       |          |  |  |  |

#### Table 65 Configure: Services > Guest Access > Access > Vouchers parameters

| Parameters   | Description   | Range | Default |
|--------------|---|-------|---------|
|              | Bind Voucher to Device: Provision to bind single device to voucher.   |       |         |
|              | 2. Voucher Design   |       |         |
|              | Title Color   |       |         |
|              | Message Color   |       |         |
|              | Code Color  |       |         |
|              | Background Color  |       |         |
|              | Background Image  |       |         |
|              | • Title   |       |         |
|              | Message   |       |         |
|              | Access Code Message   |       |         |
| Card Preview | User can preview the format of Voucher access token<br>that has been configured in Plans section, which shall<br>be distributed to customers. | -     | -       |
| Export       | User can export Vouchers created for a plan and can<br>provide to customers on demand. Both PDF and CSV<br>formats are supported.             | -     | -       |
| Add Vouchers | User can add more Vouchers if required in the plan selected.  | -     | -       |
| Delete       | User can delete vouchers based on requirement:  | -     | -       |
|              | Delete Selected:  |       |         |
|              | This option provisions user to delete only selected vouchers.   |       |         |
|              | Delete Expired:   |       |         |
|              | This option provisions user to delete all expired vouchers.   |       |         |

|            | <u>Guest Access Portal</u> > GAP-Test-Portal   |
|------------|--|
| ŝ          | Basic Access Splash Sessions   |
| വ          | Free Paid <b>Vouchers</b>  |
| <i></i>    | Enable Voucher Access  |
|            | Plans Add New  |
| S.         | new 🖉 🗙  |
| Ĥ          | Card Preview   Export  Add Vouchers Delete Selected Delete Expired                         |
| રંડુર      | Voucher ID Status Creation Time Claimed Time   |
| 岛          |  |
|            | No Generated Vouchers  |
| <b></b> ∦Я |  |
|            |  |
|            |  |
|            | Save Note: Splash page needs to be saved to reflect any changes in Access portal settings. |

Figure 179 Configure: Services > Guest Access > Access > Vouchers parameters

#### Table 66 Configure: Services > Guest Access > Splash parameters

| Parameters         | Description  | Range | Default |
|--------------------|--|-------|---------|
| Services > Guest A | Access Portal > Splash > Logo  |       |         |
| Logo               | User has provision to select Logo and selected background color that will be appeared in Splash page.  | -     | -       |
| Services > Guest A | Access Portal > Splash > Background  |       |         |
| Background         | <ul> <li>Background Image<br/>Provision to select background image.</li> <li>Opacity<br/>Transparency of background image.</li> <li>Repeat Background<br/>When enabled, background image will be<br/>repeated</li> <li>Background Placement<br/>Flexibility to place image at selective locations<br/>in splash page.</li> </ul> | -     | -       |

| Parameters                  | Description   | Range | Default   |
|-----------------------------|---|-------|---|
| Services > Guest            | Access Portal > Splash > Text Design  |       |   |
| Text Design                 | Flexibility to change text design that is displayed in splash page.   | -     | -   |
| Services > Guest            | Access Portal > Splash > Content  |       |   |
| Page Title                  | Text to appear as the title of the page.  | -     | -   |
| Message                     | Text to appear as the welcome text. You can<br>choose the font style and size for the welcome<br>text.      | -     | -   |
| Login Title                 | Text to appear for login.   | -     | Access Internet   |
| Accept Terms<br>Message     | Text to appear as the accept terms message.   | -     | Please accept<br>Terms and<br>Conditions<br>before signing<br>in! |
| Terms &<br>Conditions Title | Text to appear as the title for the terms and the conditions.   | -     | -   |
| Terms &<br>Conditions       | Provision to add list of terms and conditions that<br>needs to be shared with end user before<br>accepting. | -     | -   |
| Login Success<br>Message    | Message to appear after successful login.   | -     | Congratulations,<br>your login is<br>successful                   |
| Login Failure<br>Message    | Message to appear after login failure.  | -     | Login Failure   |
| Server Error<br>Message     | Text to appear if there is an error while contacting server.  | -     | Error<br>Contacting<br>Server                                     |
| Please Wait<br>Message      | Message to appear when contacting server.   | -     | Please Wait   |
| Terms Agree<br>Button       | Prefix message that appends to Terms and Conditions Agree option in splash page.                            | -     | I Agree with the  |
| Terms Cancel<br>Button      | Message that appears to Terms and Conditions<br>Cancel option in splash page.                               | -     | Cancel  |
| Login Button                | Enter the text that should appear on the button to submit in splash page.                                   | -     | Login   |

| Parameters                    | Description  | Range | Default       |
|-------------------------------|--|-------|---------------|
| Select Plans<br>Label         | User defined text to guide user to select plans.   | -     | Select a Plan |
| Footer                        | Enter the text to appear as the footer of the page.<br>You can choose the font style and size for the<br>footer.   | -     | -             |
| On Success<br>Redirect to URL | Provision to configure URL that appears on successful Guest Access authentication.   | -     | -             |
| Services > Guest A            | Access Portal > Splash > Advanced  |       |               |
| Customer CSS<br>Design        | Provision to upload custom Splash page in CSS format.  | -     | -             |
| Download<br>Sample CSS        | User can download sample CSS files supported.  | -     | -             |
| Services > Guest A            | Access Portal > Splash > Custom Fields   |       |               |
| Name                          | Provision to configure user friendly name to customers.  | -     |               |
| Туре                          | <ul> <li>Five options are provided, so that they can appear<br/>in splash page.</li> <li>String</li> <li>Number</li> <li>Email</li> <li>Phone</li> <li>Date</li> </ul>                                     | -     | String        |
| Mandatory                     | If above selected types needs to be entered by customer, enable this field else it is optional to users.   | -     | Disabled      |
| Services > Guest A            | Access Portal > Splash > WiFi4EU   |       |               |
| Enable                        | Provision to enable WiFi4EU configuration.   | -     | Disabled      |
| Network UUID                  | The provided wifi4euNetworkIdentifier should be<br>of type string and should correspond to the<br>unique identifier (UUID) of the WiFi4EU network<br>installation as indicated in the installation report. | -     | -             |
| Captive Portal<br>URL         | URL of the captive portal page where in the<br>snippet will be integrated. The EC will verify the<br>compliance of this page with the WiFi4EU<br>requirements.   | -     | -             |

| Parameters                    | Description  | Range | Default |
|-------------------------------|--|-------|---------|
| Metrics Snippet<br>Script URL | A WiFi4EU supplier can test if the snippet is correctly installed and if its portal is compliant by enabling the snippet self-test modus.  | -     | -       |
| Language                      | Provision to set to the correct language code in<br>which the content of the portal page is served.<br>The language code should be one of the 24<br>predefined language codes (1). | -     | -       |
| Enable Self-test<br>Modus     | Provision to enable self-validation of the portal.   | -     | -       |
| Show Logo                     | Provision to display WiFi4EU logo.   | -     | -       |

#### Figure 180 Configure: Services > Guest Access > Splash parameters

| Guest Access Portal > WiFi4EU | 2   |
|-------------------------------|---|
| Voucher Code Error Message:   | Please enter voucher code or select any other access              |
| Mobile Number Label:          | Mobile Number   |
| Access Code Label:            | Access Code   |
| Enter Mobile Number Message:  | Please enter mobile number  |
| SMS Access Code Label:        | Send Code   |
| Select Plans Label:           | Select a Plan   |
| Footer                        | Powered by cnMaestro  |
|                               |   |
| On Success Redirect to URL: @ | e.g. https://www.google.com                                       |
| ⊞Advanced                     |   |
| ⊕ Custom Fields               |   |
|                               |   |
|                               | ✓ Enable  |
| Network UUID:0                | AyjhiCPrsh5fbGunBtfQQ   |
| Captive Portal URL:0          | https://eu-w1-guest.cloud.cambiumnetworks.com/ddadff939d2b773c1ar |
| Metrics Snippet Script URL-0  | https://collection.wifi4eu.ec.europa.eu/wifi4eu.min.js            |
| Language:                     | English -   |
|                               | ✓ Enable Self-test Modus  |
|                               | Show Logo   |
| 590                           |   |

| Parameters          | Description  | Range  | Default |
|---------------------|--|--------|---------|
| Services > Guest Ac | ccess Portal > <gap profile=""> Access &gt; Sessions &gt; Client S</gap> | ession |         |
| Client MAC          | Provides the MAC address of wireless client whose session is valid.      | -      | -       |
| Access Point        | Provides BSSID of radio to which wireless client is associated.          | -      | -       |

#### Table 67 Configure: Services > Guest Access > Sessions parameters

| Parameters         | Description  | Range        | Default |
|--------------------|--|--------------|---------|
| Access Type        | Provides type of Guest Access Portal services enabled<br>on wireless client. Following are the types:                      |              |         |
|                    | • Free   |              |         |
|                    | Type of Social Login   |              |         |
|                    | • SMS  |              |         |
|                    | Type of Payment Gateway  |              |         |
|                    | Vouchers   |              |         |
| WLAN               | Displays SSID of WLAN to which wireless client is associated.  | -            | -       |
| Remaining Time     | The time left for the client to access the internet. It depends upon the session duration configured in the Access Portal. | -            | -       |
| Voucher            | Displays Voucher code that has been used by wireless client for internet access.   | -            | -       |
| Disconnect         | Provision to disconnect wireless client on demand.   | -            | -       |
| Services > Guest A | Access Portal > <gap profile=""> Access &gt; Sessions &gt; Client L</gap>  | ogin Events. |         |
| Client MAC         | Provides the MAC address of wireless client whose session is valid.  |              |         |
| Portal             | Displays Guest Access Portal associated with wireless client.  |              |         |
| WLAN               | Displays SSID of WLAN to which wireless client is associated.  |              |         |
| Access Point       | Provides BSSID of radio to which wireless client is associated.  |              |         |
| Voucher Code       | Displays Voucher code that has been used by wireless client for internet access.   |              |         |
| Login Time         | Displays time stamp of wireless client after a successful.   |              |         |
| Access Type        | Provides type of Guest Access Portal services enabled on wireless client. Following are the types:                         |              |         |
|                    | • Free   |              |         |
|                    | Type of Social Login   |              |         |
|                    | • SMS  |              |         |
|                    | Type of Payment Gateway  |              |         |

| Parameters         | Description  | Range          | Default |
|--------------------|--|----------------|---------|
|                    | Vouchers   |                |         |
| Email              | Displays email address as provided by user during guest access portal authentication.                                    |                |         |
| Mobile Number      | Displays mobile number as provided by user during guest access portal authentication.                                    |                |         |
| Services > Guest A | ccess Portal > <gap profile=""> Access &gt; Sessions &gt; Client P</gap>   | aid Transactio | ns      |
| Client MAC         | Provides the MAC address of wireless client whose session is valid.  |                |         |
| Portal             | Displays Guest Access Portal associated with wireless client.  |                |         |
| Plan               | Displays plan name activated for user.   |                |         |
| Access Point       | Provides BSSID of radio to which wireless client is associated.  |                |         |
| Voucher Code       | Displays Voucher code that has been used by wireless client for internet access.   |                |         |
| Start Time         | Displays timestamp when wireless client is successfully authenticated using Guest Access portal services.                |                |         |
| End Time           | Displays valid session time based on configuration in<br>Plan. This value is always equal to (Start Time +<br>Duration). |                |         |
| Transaction ID     | Displays random value generated during payment process and can be used as reference for any debugging.                   |                |         |

| Basi | ic Access Splash                       | Sessions         |              |                          |                        |                        |                                  |                 |                    |       |
|------|--|------------------|--------------|--------------------------|------------------------|------------------------|----------------------------------|-----------------|--------------------|-------|
|      | nt Session                             |                  |              |                          |                        |                        |                                  |                 |                    |       |
|      | cher - Search                          |                  |              | Q                        | Managed Account        | t: Base Infrastructure | 2                                | D               | isconnect Selected | 2     |
|      | Client MAC                             | Access Type      | N            | VLAN                     | Access Poin            | t Remainir             | ng Time Vo                       | ucher           | Disconneo          | ct    |
|      | 7C-78-7E-6E-56-D4                      | Payment-Gat      |              | 700-Raja-GA              | 58:C1:7A:26:           |                        | -                                | RN3CZ           | Disconnec          |       |
|      | 101012023004                           | r dymene odd     | civity L     | noo naja on              | <u>50.01.17.20</u> .   | 201133                 |                                  | MINUCL          | Disconnee          |       |
|      |  |                  |              |                          |                        |                        | Showing 1 - 1 T                  | otal: 1 10 -    | < Previous         |       |
|      |  |                  |              |                          |                        |                        | Showing1 11                      |                 |                    |       |
|      | nt Login Events<br>ess Point - Search  |                  |              | Q                        | Managed Account        | t: Base Infrastructure |                                  |                 | Export 👻           |       |
|      |  |                  |              |                          | -                      |                        |                                  | - 11            |                    |       |
|      |  |                  | Access Type  | WLAN                     | Access Poi             |                        | 0                                | Email           | Mobile N           | vumbe |
|      | 78-7B-8A-9A-9E di                      |                  | Free         | diva_CP_cn               |                        |                        | Tue Oct 01 201                   |                 |                    |       |
|      | C4-0B-CB-DE-D di                       | -                | Free<br>Free | diva_CP_cn<br>diva_CP_cn |                        |                        | Tue Oct 01 201<br>Tue Oct 01 201 |                 |                    |       |
|      | C4-0B-CB-DE-D di                       | -                | Free         | diva_CP_cn               |                        |                        | Tue Oct 01 201                   |                 |                    |       |
|      | C4-0B-CB-DE-D di                       | -                | Free         | diva_CP_cn               |                        |                        | Tue Oct 01 201                   |                 |                    |       |
|      | C4-0B-CB-DE-D di                       | -                | Free         | diva_CP_cn               |                        |                        | Tue Oct 01 201                   |                 |                    |       |
|      | 78-7B-8A-9A-9E di                      | -                | Free         | diva_CP_cn               |                        |                        | Tue Oct 01 201                   |                 |                    |       |
|      | 78-7B-8A-9A-9E di                      | iva_GA           | Free         | diva_CP_cn               | ma <u>58:C1:7A:6</u> E | :D8                    | Tue Oct 01 201                   |                 |                    |       |
|      | C4-0B-CB-DE-D d                        | iva_GA           | Free         | diva_CP_cn               | ma <u>58:C1:7A:6</u>   | <u>:D8</u>             | Tue Oct 01 201                   |                 |                    |       |
|      | 78-7B-8A-9A-9E di                      | iva_GA           | Voucher      | diva_CP_cn               | ma <u>58:C1:7A:6</u> E | :D8 DNZQPBCZ           | Tue Oct 01 201                   |                 |                    |       |
|      |  |                  |              |                          |                        |                        |                                  |                 |                    |       |
|      |  |                  |              |                          |                        | Showing 1 - 10         | Total: 48 10 -                   | < Previous      | 2 3 4 5            | Next  |
|      |  |                  |              |                          |                        | 5110 Wing 1 - 10       | 10tal. 46                        | r Flevious      | 2 3 4 3            | Next  |
|      | nt Paid Transacti                      |                  |              |                          |                        |                        |                                  |                 |                    |       |
|      | aged Account: Base                     |                  |              |                          |                        |                        |                                  |                 |                    | -     |
|      | Client MAC                             | Portal           | Plan         | Acc                      | ess Point V            | /oucher Code St        | art Time                         | End Time        | Transactio         | on ID |
|      | 7C-78-7E-6E-56-D4                      | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 34-78-D7-C1-C0-24                      | HA-Standalone-   |              |                          |                        | -                      |                                  | Fri Nov 30 2018 |                    |       |
|      | 7C-78-7E-6E-56-D4                      | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 7C-78-7E-6E-56-D4<br>34-78-D7-C1-C0-24 | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 34-78-D7-C1-C0-24<br>7C-78-7E-6E-56-D4 | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 34-78-D7-C1-C0-24                      | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 7C-78-7E-6E-56-D4                      | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 34-78-D7-C1-C0-24                      | HA-Standalone-   |              |                          |                        |                        |                                  | Fri Nov 30 2018 |                    |       |
|      | 7C-78-7E-6E-56-D4                      | HA-Standalone-1  |              |                          |                        | -                      |                                  | Fri Dec 07 2018 |                    |       |
|      | 101012020001                           | in to contoine i |              | <u></u>                  | <u></u>                |                        | 00001202020                      |                 |                    |       |
|      |  |                  |              |                          |                        |                        |                                  |                 |                    |       |

#### Figure 181 Configure: Services > Guest Access > Sessions parameters

# Configuration examples

#### Prerequisites:

- Create Guest Access Portal
  - Login to cnMaestro > Navigate to Services > Guest Access Portal > Add Portal.
  - Enter Portal Name, Description, enable Client Login Event Logging and click on Save.

|     | cn <b>Maestro</b>  |  | MSP Vie |           | 261<br>!     |      |          | 115                   |        |
|-----|--|--|---------|-----------|--------------|------|----------|-----------------------|--------|
| -14 | Services > Guest Access Portal   | Add Guest Portal                       | ×       |           |              |      |          |                       | 2      |
| ŵ   | Guest Portal Hostname / IP   | Managed Account<br>Base Infrastructure | •       |           |              |      |          |                       |        |
| ES. | Save   | Name* Cambium_Guestaccess_Portal       |         |           |              |      |          |                       |        |
|     | A You must update your AP software to version 3<br>Managed Account: All Accounts - | Description                            |         |           |              |      |          | Add P                 | Portal |
| S.  | Guest Portal Name Description  |  |         | Vouc      | her Access   | Pai  | d Access |                       |        |
| Ű   | SIT AUTOMATION Google F SIT AUTOMATIO  |  |         | No        |              | No   |          | <b>A</b>              | ×      |
| Ð   | HA-Standalone-Test   |  |         | No        |              | Yes  |          | ø                     | ×      |
|     | <u>diva test</u>   | Client Login Event Logging             |         | No        |              | No   |          | ø                     | ×      |
| 岛   | diva_GA  | Save Cancel                            |         | Yes       |              | No   |          | <i>B</i> <sup>2</sup> | ~      |
| 18  |  |  |         | Showing 1 | - 4 Total: 4 | 10 🔻 |          | ous 🚺 I               |        |

# Free

### Configuration

1. Configure Guest Access portal enabled in pre-requisites for free internet access with pre-defined self-registration parameters.

| <u>Guest Access Portal</u> > diva_GA          |     |          |                                 |  |  |  |  |
|---|-----|----------|---------------------------------|--|--|--|--|
| Basic Access Splash Sessions                  |     |          |                                 |  |  |  |  |
| Free Paid Vouchers                            |     |          |                                 |  |  |  |  |
| ✓ Enable Free Access                          |     |          |                                 |  |  |  |  |
| Enable Logout functionality for the guest cli | ent |          |                                 |  |  |  |  |
| Bypass Captive Portal Detection               |     |          |                                 |  |  |  |  |
| Client Session                                |     |          |                                 |  |  |  |  |
| Renewal Frequency                             |     |          |                                 |  |  |  |  |
| 4   |     | Min(s) 🗸 | Valid range is 1-2628000 min(s) |  |  |  |  |
| Session Duration                              |     |          |                                 |  |  |  |  |
| 3   |     | Min(s) 🗸 | Valid range is 1-2628000 min(s) |  |  |  |  |
| 🗆 Client Rate Limit                           |     |          |                                 |  |  |  |  |
| Downlink                                      |     |          |                                 |  |  |  |  |
| 5000  | Kbj | ps       |                                 |  |  |  |  |
| Uplink  |     |          |                                 |  |  |  |  |
| 5000  | Kbj | ps       |                                 |  |  |  |  |
| 🗆 Client Quota Limit                          |     |          |                                 |  |  |  |  |
| Quota Type                                    |     |          |                                 |  |  |  |  |
| Directional -                                 |     |          |                                 |  |  |  |  |
| Downlink                                      |     |          |                                 |  |  |  |  |
| 20  |     | MB▼      |                                 |  |  |  |  |
| Uplink  |     |          |                                 |  |  |  |  |
| 20  |     | MB▼      |                                 |  |  |  |  |

| WLANS > TSK_V<br>Configuration APs | LAN1_5GHz_Open  |
|------------------------------------|---|
| WLAN                               | Basic Settings  |
| AAA Servers                        | Enable  |
| Guest Access >                     | Portal Mode<br>Internal Access Point External Hotspot CnMaestro |
| Access Control                     | Guest Portal Name   |
| Passpoint                          | diva_GA 🗸   |
| ePSK                               |   |
|                                    | ⊕ Whitelist   |
|                                    | 🕀 Captive Portal bypass User Agent                              |
|                                    |   |
|                                    | Save  |



Successful Login – Redirected Splash Page



## Free - Custom fields

#### Configuration

1. Configure Guest Access portal enabled in pre-requisites for free with self-registration parameters.



| WLANs > TSK_V<br>Configuration APs   | LAN1_5GHz_Open  |
|--|---|
| WLAN<br>AAA Servers<br>Guest Access ><br>Access Control<br>Passpoint<br>ePSK | Basic Settings<br>✓ Enable<br>Portal Mode<br>○ Internal Access Point ○ External Hotspot ④ cnMaestro<br>Guest Portal Name<br>diva_GA<br>➡ Advanced Settings<br>➡ Whitelist<br>➡ Captive Portal bypass User Agent |
|  | Save  |



Successful Login – Redirected Splash Page



# Free - Social Login

### Configuration

1. Configure Guest Access portal enabled in pre-requisites for free internet access with social login.

| <u>Guest Access Portal</u> > SIT_A  | UTOMATION_Google_FB_365  |
|---|--|
| 🖃 Social Login  |  |
| Guest Portal Hostname / IP  |  |
| ship-dimmerithese michigan  | Configure this URL in the Social login application settings.   |
|   | f social login with Facebook or Google is enabled. This is required as the Captive-portal Network Assistant (Guest<br>compatible with the social login API provided by these services. |
| 🖌 Google  |  |
| Id  |  |
| 27010000 L 01 00010 peringustori  | in con   |
| 🗹 Twitter   |  |
| Consumer API Key  |  |
|   |  |
| Consumer API Secret Key   |  |
|   | 14T7   |
| Callback URL  |  |
| ) standing the second |  |
| ✓ Facebook  |  |
| Id  |  |
| (1005)  |  |
| Secret  |  |
| ••••••  | Show   |
| Reply URL   | https://sitindia-noc62.camn  |
| ✓ Office 365  |  |
| Reply URL   |  |
| in the line in the second second  | Configure this URL as Reply URL under Office365 application settings   |
| Id  |  |
| 200000000000000000000000000000000000000   |  |

|                   | VLAN1_5GHz_Open  |
|-------------------|--|
| Configuration APs |  |
| WLAN              | Basic Settings   |
| AAA Servers       | Enable  Portal Mode  |
| Guest Access >    | Internal Access Point External Hotspot Internal Access Point |
| Access Control    | Guest Portal Name diva_GA                                    |
| Passpoint         | ⊕ Advanced Settings  |
| ePSK              | ⊕ Whitelist  |
|                   | ⊕ Captive Portal bypass User Agent                           |
|                   |  |
|                   | Save   |
|                   |  |

| Welcome To Cambium Networks             |           | Free Wi-Fi Services               |
|---|-----------|-----------------------------------|
| Please login to avail internet services |           | •Free for First 30 Min.           |
|   |           | Agree <u>Terms and Conditions</u> |
|   | LA        | Sign in with one of the following |
|   |           | G Sign in with Google             |
|   |           | y Sign in with Twitter            |
| International Providence                | -         | G Sign in with Facebook           |
| and the second second                   |           | Sign in with Microsoft            |
|   |           |                                   |
| Powered by C                            | ambium Ne | tworks                            |

Successful Login - Redirected Splash Page



# Free - SMS Authentication

#### Configuration

1. Configure Guest Access portal enabled in pre-requisites for free internet access with SMA authentication.

| <u>Guest Access Portal</u> > SIT_AU1   | OMATION_Google_FB_365  |
|--|--|
| 🕀 Client Rate Limit  |  |
| 🕀 Client Quota Limit   |  |
| 🕀 Social Login   |  |
| SMS Authentication   |  |
| 🗹 Enable   |  |
| SMS Gateway Provider   |  |
| SMS Gupshup  | •  |
| Username   |  |
| 200166285  |  |
| Password   |  |
| Sho  | w  |
| Sender ID  |  |
| Test SMS Gupchup Message   |  |
| Country Code   |  |
| US (+1) 💌  |  |
| OTP Template   |  |
| Your OTP is %code%   |  |
| The OTP template should include %code% as d<br>Provider. %code% will be replaced by the OTP code | isplayed in the sample text. Template may need to be approved, it's advised to contact respective SMS Gateway<br>e in the SMS. |

| WLANS > TSK_V<br>Configuration APs | LAN1_5GHz_Open   |
|------------------------------------|--|
| WLAN                               | Basic Settings   |
| AAA Servers                        | Enable   |
| Guest Access >                     | Portal Mode <ul> <li>Internal Access Point</li> <li>External Hotspot</li> <li>cnMaestro</li> </ul> |
| Access Control                     | Guest Portal Name  |
| Passpoint                          | diva_GA  |
| ePSK                               | ⊕ Whitelist  |
|                                    | ⊕ Captive Portal bypass User Agent   |
|                                    | Save   |



## Successful Login – Redirected Splash Page



# Paid - Payment Gateway

### Configuration

1. Configure Guest Access portal enabled in pre-requisites for free internet access with paid payment gateway.

| <u>Guest Access Portal</u> > diva_GA  |   |
|---|---|
| Basic Access Splash Sessions  |   |
| Free Paid Vouchers  |   |
| ✓ Enable Paid Access  |   |
| 🖃 Paypal Payment Gateway  |   |
| ✓ Enable  |   |
| Auto return URL   |   |
| https://sitindia-noc62.camnwk.com/cn-ctlr/guest/cnmaestro/diva_GA/gaPaymentStatus | 0 |
| PDT Identity Token  |   |
| Control and Method in the The State Conceptor in the Deco                         |   |
| EnableIPN   |   |
| Use Sandbox   |   |
| Update Button Code  |   |

| <u>WLANs</u> > TSK_VLAN1_5GHz_Open |   |  |  |  |
|------------------------------------|---|--|--|--|
| Configuration APs                  |   |  |  |  |
| WLAN                               | Basic Settings  |  |  |  |
| AAA Servers                        | Enable  |  |  |  |
| Guest Access >                     | Portal Mode<br>O Internal Access Point O External Hotspot O cnMaestro |  |  |  |
| Access Control                     | Guest Portal Name   |  |  |  |
|                                    | diva_GA 🗸   |  |  |  |
| Passpoint                          | ⊕ Advanced Settings   |  |  |  |
| ePSK                               | ⊕ Whitelist   |  |  |  |
|                                    | 🕀 Captive Portal bypass User Agent                                    |  |  |  |
|                                    |   |  |  |  |
|                                    | Save  |  |  |  |
|                                    |   |  |  |  |



### PayPal payment page



# Vouchers

### Configuration

1. Configure Guest Access portal enabled in pre-requisites for free internet access with Vouchers.

| Enable Vou | icher Access |                    |                                   |                                  |                                      |   |
|------------|--------------|--------------------|-----------------------------------|----------------------------------|--------------------------------------|---|
| ans        | Add New      | Card Preview - Exp | ort  Add Vouchers Delete Selected | Delete Expired                   |                                      |   |
| iva >      | <i>₫</i> ×   | Voucher ID         | Status                            | Creation Time                    | Claimed Time                         |   |
|            |              | GKDM48QH           | expired                           | Tue Oct 01 2019 14:58:56 GMT+053 | 0 Tue Oct 01 2019 14:59:53 GMT+0530  | × |
|            |              | 99K67NND           | expired                           | Mon Oct 07 2019 12:14:42 GMT+05: | 30 Mon Oct 07 2019 12:16:39 GMT+0530 | × |
|            |              | BFNC9JBG           | expired                           | Mon Oct 07 2019 12:14:42 GMT+05: | 30 -                                 | × |
|            |              | H4WXGR3N           | expired                           | Tue Oct 01 2019 14:58:56 GMT+053 | 0 -                                  | × |
|            |              | N3DX1LKZ           | expired                           | Tue Oct 01 2019 14:58:56 GMT+053 | 0 -                                  | × |
|            |              | SKGG6L3V           | expired                           | Mon Oct 07 2019 12:14:42 GMT+05  | 30 -                                 | × |
|            |              | SSHP1MTH           | expired                           | Mon Oct 07 2019 12:14:42 GMT+05  | 30 -                                 | × |
|            |              | T78ZK729           | expired                           | Tue Oct 01 2019 14:58:56 GMT+053 | 0 -                                  | × |
|            |              | VC6C91X1           | expired                           | Tue Oct 01 2019 14:58:56 GMT+053 | 0 -                                  | × |
|            |              | W1P6H7TS           | expired                           | Mon Oct 07 2019 12:14:42 GMT+05: | 30 -                                 | × |

| WLANS > TSK_VL | AN1_5GHz_Open  |
|----------------|--|
| WLAN           | Basic Settings   |
| AAA Servers    | ✓ Enable   |
| Guest Access > | Portal Mode O Internal Access Point External Hotspot O cnMaestro |
| Access Control | Guest Portal Name  |
| Passpoint      |  |
| ePSK           | ⊕ Whitelist  |
|                | ⊕ Captive Portal bypass User Agent                               |
|                | Save   |



Successful Login - Redirected Splash Page



## WiFi4EU

### Configuration

1. Configure Guest Access portal enabled in pre-requisites for WIFI4EU compatibility.

| ⊖ WiFi4EU                   |  |
|-----------------------------|--|
|                             | ✓ Enable   |
| Network UUID:               | AyjhiCPrsh5fbGunBtfQQ  |
| Captive Portal URL:         | https://eu-wl-guest.cloud.cambiumnetworks.com/ddadff939d2b773c1a |
| Metrics Snippet Script URL: | https://collection.wifi4eu.ec.europa.eu/wifi4eu.min.js           |
| Language:                   | English -  |
|                             | ✓ Enable Self-test Modus   |
|                             | Show Logo  |
|                             |  |

| WLANS > TSK_V<br>Configuration APs | LAN1_5GHz_Open   |
|------------------------------------|--|
| WLAN                               | Basic Settings   |
| AAA Servers                        | ✓ Enable   |
| Guest Access >                     | Portal Mode <ul> <li>Internal Access Point</li> <li>External Hotspot</li> <li>cnMaestro</li> </ul> |
| Access Control                     | Guest Portal Name  |
| Passpoint                          |  |
| ePSK                               | ⊕ Whitelist  |
|                                    | ⊕ Captive Portal bypass User Agent   |
|                                    |  |
|                                    | Save   |

| Co-funded by the<br>European Union<br>WIFi4EU                  |  |
|--|--|
| Welcome To Cambium Networks                                    |  |
| Please login to avail internet services                        |  |
| Access Internet<br>Please enter voucher code to get web access |  |
| Voucher      Free  Buy Internet                                |  |
| Voucher Code   |  |
| Login  |  |

#### Successful Login - Redirected Splash Page



# Chapter 19: Policy Based VLAN Assignment (PBA)

# Introduction

The PBA is intended to support zero-touch detection and configuration for connected Cambium devices (cnPilot AP's). New Cambium vendor specific LLDP TLVs are introduced starting with cnMatrix Release 2.1.0 to support "pushing" PBA policy data from Cambium devices (e.g., cnPilot) to cnMatrix. The new PBA TLVs are implemented as an extension to the LLDP standard, using its flexible extension mechanism. From a functional perspective, cnMatrix, acting as the upstream device, includes the PBA Authentication TLV in the regularly generated LLDPDUs for a port. The downstream device (e.g., cnPilot) receives the PBA Authentication TLV and, if policy action data (e.g., VLANs, native VLAN) is present to be pushed to cnMatrix, a PBA device settings TLV is constructed and added to the LLDPDU for the port.

Below table lists the fields that are required for configuring PBA:

#### Table 68 Configuring PBA parameters

| Parameters        | Description  | Range | Default |
|-------------------|--|-------|---------|
| lldp-pba          | New PBA TLVs will be shared with cnMatrix switch.  | -     | Enabled |
| lldp-pba-auth-key | The shared private key used during PBA TLV<br>authentication can be updated or reset from its<br>default value (by using the 'no' option). | -     | Enabled |

Note

**Ildp-pba-auth-key** is by default enabled; key value cannot be shared due to security concerns.

#### Configuration:

Syntax:

```
E410-0DA1AF(config)# 11

lldp : Enable periodic transmission of LLDP packets

lldp-pba : Enable PBA transmission in LLDP packets

lldp-pba-auth-key : Configure the SHA-KEY passphrase ascii (must contain 8

to 63 ascii or characters)
```

Example:

```
E410-0DA1AF(config)#
E410-0DA1AF(config)# show config | grep lld
lldp
lldp-pba
lldp-pba-auth-key $crypt$1$gwYqHt9rxt2FXeMsX11jsFUKBupXtZcd
E410-0DA1AF(config)#
```



PBA will not be functioning if more than 20 VLANs are configured on the AP.

To disable PBA:

Note

```
E410-0DA1AF(config)#
E410-0DA1AF(config)# no lldp-pba
```

# Chapter 20: Device Recovery Methods

# Factory reset via 'RESET' button

#### Table 69 Factory reset via RESET button

| cnPilot<br>Access Point | Procedure   | LED Indication  |
|-------------------------|---|---|
| E400                    | Press and hold <b>Reset</b> button for 15 seconds | Both LEDs will be <b>OFF</b> and turned onto <b>Amber</b> |
| e410                    | Press and hold <b>Reset</b> button for 25 seconds | LED will be <b>OFF</b> and turned onto <b>Amber</b>       |
| e410b                   | Press and hold <b>Reset</b> button for 25 seconds | LED will be <b>OFF</b> and turned onto <b>Amber</b>       |
| e600                    | Press and hold <b>Reset</b> button for 20 seconds | LED will be <b>OFF</b> and turned onto <b>Amber</b>       |
| e430                    | Press and hold <b>Reset</b> button for 25 seconds | LED will be <b>OFF</b> and turned onto <b>Amber</b>       |
| e700                    | Press and hold <b>Reset</b> button for 25 seconds | Both LEDs will be <b>OFF</b> and turned onto <b>Amber</b> |
| E500                    | Press and hold <b>Reset</b> button for 25 seconds | Both LEDs will be <b>OFF</b> and turned onto <b>Amber</b> |
| E501S                   | Press and hold <b>Reset</b> button for 25 seconds | Both LEDs will be <b>OFF</b> and turned onto <b>Amber</b> |
| e502S                   | Press and hold <b>Reset</b> button for 25 seconds | Both LEDs will be <b>OFF</b> and turned onto <b>Amber</b> |
| e425H                   | Press and hold <b>Reset</b> button for 20 seconds | LED will be <b>OFF</b> and turned onto <b>Amber</b>       |
| e505                    | Press and hold <b>Reset</b> button for 20 seconds | LED will be <b>OFF</b> and turned onto <b>Amber</b>       |
| e510                    | Press and hold <b>Reset</b> button for 20 seconds | Both LEDs will be <b>OFF</b> and turned onto <b>Amber</b> |

# Factory reset via power cycle

#### Table 70 Factory reset via power cycle

| cnPilot<br>Access Point | Procedure   |
|-------------------------|---|
| E400                    | Not Applicable  |
| e410                    | Not Applicable  |
| e410b                   | Not Applicable  |
| e600                    | Not Applicable  |
| e430                    | Not Applicable  |
| e700                    | Not Applicable  |
| E500                    | Follow power <b>ON</b> and <b>OFF</b> for 5 times with interval of 7 Sec (ON) and 5 Sec (OFF) |
| E501S                   | Follow power <b>ON</b> and <b>OFF</b> for 5 times with interval of 7 Sec (ON) and 5 Sec (OFF) |
| e502S                   | Follow power <b>ON</b> and <b>OFF</b> for 5 times with interval of 7 Sec (ON) and 5 Sec (OFF) |
| e425H                   | Not Applicable  |
| e505                    | Not Applicable  |
| e510                    | Not Applicable  |

To disable factory reset when above power sequence occurs, run the following CLI command:

E500-Factory\_Reset(config)# no service powercycle-factory-default E500-Factory\_Reset(config)# save

# Boot partition change via power cycle

#### Table 71 Boot partition change via power cycle

| cnPilot<br>Access Point | Procedure   |
|-------------------------|---|
| E400                    | Follow power <b>ON</b> and off for 9 times with interval of 7 Sec (ON) and 5 Sec (OFF)  |
| e410                    | Follow power <b>ON</b> and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF) |
| e410b                   | Follow power <b>ON</b> and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF) |
| e600                    | Follow power <b>ON</b> and off for 9 times with interval of 7 Sec (ON) and 5 Sec (OFF)  |
| e430                    | Follow power <b>ON</b> and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF) |

| e700  | Follow power <b>ON</b> and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF) |
|-------|---|
| E500  | Follow power <b>ON</b> and off for 9 times with interval of 7 Sec (ON) and 5 Sec (OFF)  |
| E501S | Follow power <b>ON</b> and off for 9 times with interval of 7 Sec (ON) and 5 Sec (OFF)  |
| e502S | Follow power <b>ON</b> and off for 9 times with interval of 7 Sec (ON) and 5 Sec (OFF)  |
| e425H | Follow power <b>ON</b> and off for 9 times with interval of 9 Sec (ON) and 5 Sec (OFF)  |
| e505  | Follow power <b>ON</b> and off for 9 times with interval of 9 Sec (ON) and 5 Sec (OFF)  |
| e510  | Follow power <b>ON</b> and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF) |

# Glossary

| _                 |   |
|-------------------|---|
| Term              | Definition  |
| АР                | Access Point Module. One module that distributes network or Internet services to subscriber modules.  |
| ΑΡΙ               | Application Program Interface   |
| ARP               | Address Resolution Protocol. A protocol defined in RFC 826 to allow<br>a network element to correlate a host IP address to the Ethernet<br>address of the host.   |
| внм               | Backhaul Timing Master (BHM)- a module that is used in a point to point link. This module controls the air protocol and configurations for the link.  |
| BHS               | Backhaul Timing Slave (BHS)- a module that is used in a point to point link. This module accepts configuration and timing from the master module.   |
| BT                | Bluetooth   |
| DFS               | See Dynamic Frequency Selection   |
| DHCP              | Dynamic Host Configuration Protocol defined in RFC 2131. Protocol<br>that enables a device to be assigned a new IP address and TCP/IP<br>parameters, including a default gateway, whenever the device<br>reboots. Thus, DHCP reduces configuration time, conserves IP<br>addresses, and allows modules to be moved to a different network<br>within the system. |
| Ethernet Protocol | Any of several IEEE standards that define the contents of frames that<br>are transferred from one network element to another through<br>Ethernet connections.   |
| FCC               | Federal Communications Commission of the U.S.A.   |
| GPS               | Global Positioning System. A network of satellites that provides<br>absolute time to networks on earth, which use the time signal to<br>synchronize transmission and reception cycles (to avoid interference)<br>and to provide reference for troubleshooting activities.   |
| UI                | User interface.   |
| нттр              | Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web.   |

| Term                              | Definition  |
|-----------------------------------|---|
| HTTPS                             | Hypertext Transfer Protocol Secure  |
| НТ                                | High Throughput   |
| IP Address                        | 32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.  |
| IPv4                              | Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.  |
| LUID                              | Logical Unit ID. The final octet of the 4-octet IP address of the module.   |
| MAC Address                       | Media Access Control address. The hardware address that the factory<br>assigns to the module for identification in the Data Link layer<br>interface of the Open Systems Interconnection system. This address<br>serves as an electronic serial number.              |
| Maximum Information Rate<br>(MIR) | The cap applied to the bandwidth of an SM or specified group of SMs.<br>In the Cambium implementation, this is controlled by the Sustained<br>Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data<br>Rate, and Downlink Burst Allocation parameters. |
| МІВ                               | Management Information Base. Space that allows a program (agent)<br>in the network to relay information to a network monitor about the<br>status of defined variables (objects).  |
| MIR                               | See Maximum Information Rate.   |
| PPPoE                             | Point to Point Protocol over Ethernet. Supported on SMs for<br>operators who use PPPoE in other parts of their network operators<br>who want to deploy PPPoE to realize per-subscriber authentication,<br>metrics, and usage control.                               |
| Proxy Server                      | Network computer that isolates another from the Internet. The proxy<br>server communicates for the other computer, and sends replies to<br>only the appropriate computer, which has an IP address that is not<br>unique or not registered.                          |
| SLA                               | Service Level Agreement   |
| VLAN                              | Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.   |

| Term | Definition   |
|------|--|
| VPN  | Virtual private network for communication over a public network.<br>One typical use is to connect remote employees, who are at home or<br>in a different city, to their corporate network over the Internet. Any of<br>several VPN implementation schemes is possible. SMs support L2TP<br>over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and<br>PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether<br>the Network Address Translation (NAT) feature enabled. |
| VHT  | Very High Throughput   |