Cambium Networks™

USER GUIDE

cnPilot Enterprise Wi-Fi Access Points

System Release 4.0

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

Restrictions

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

License Agreements

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

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Contents

List of Figures

List of Tables

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 1 Related documents

cnPilot Enterprise product details	https://www.cambiumnetworks.com/products/wifi/
cnPilot Enterprise AP User Guide (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-Series-Enterprise-APs/bd-p/cnPilot_E_Series/
Community	http://community.cambiumnetworks.com/
Support	https://www.cambiumnetworks.com/support/contact-support/
Warranty	https://www.cambiumnetworks.com/support/warranty/
Feedback	For feedback, e-mail to support@cambiumnetworks.com/

Features and Enhancements

System release 3.11 includes the following new features:

Table 2 Features

Features	Platform Support	Summary
Spectrum analyzer	All	RF tool.
WWAN	e600	LTE support on e600 to provide internet services.

System release 3.11 includes the following enhancements:

Table 3 Enhancements

Features	Platform Support	Summary
Static	All	Network wide client isolation is enabled. User must manually configure gateway MAC. This mode deprecates gateway keep-alive method.
Auth Type	All	User has provision to configure PPP authentication method.
Service Name	All	Provision to configure service name in PPPoE.

New platforms

System release 4.0 includes the following new Platforms:

Table 4 New platforms

Hardware	Description
e425H	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)

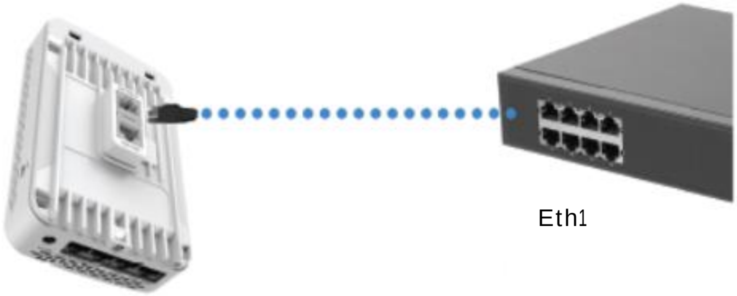
All devices can be powered by PoE switches supplying standard 802.3af or 802.3at power. The following restrictions apply if 802.3af power is used:

- On cnPilot E501S and e502S along with E500 and e430, 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

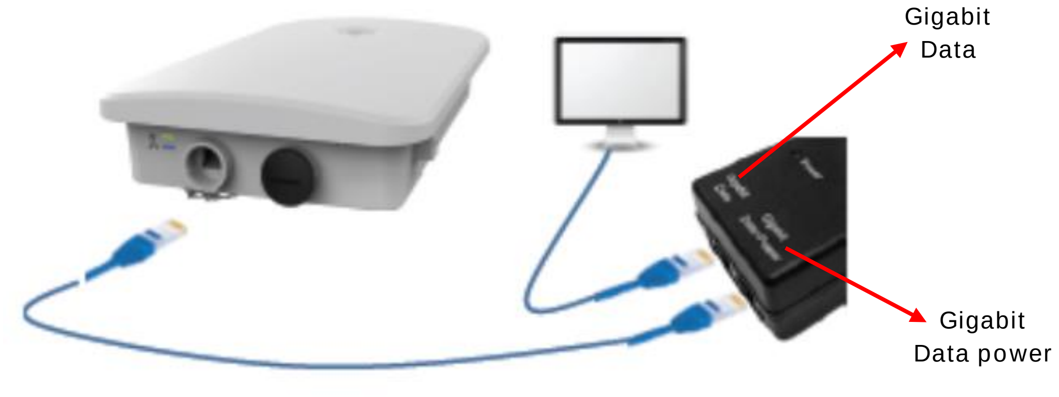


PoE adapter

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

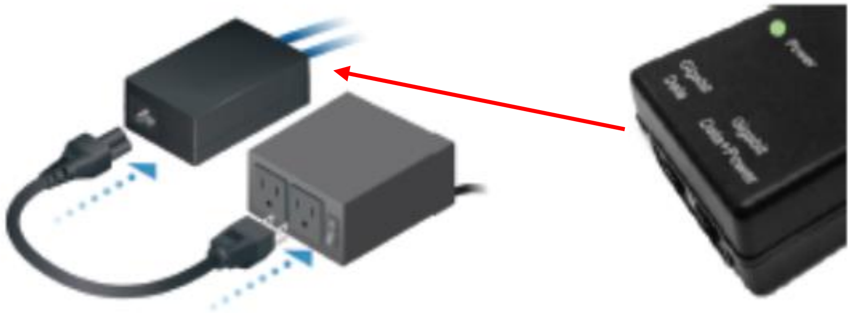


Notes

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

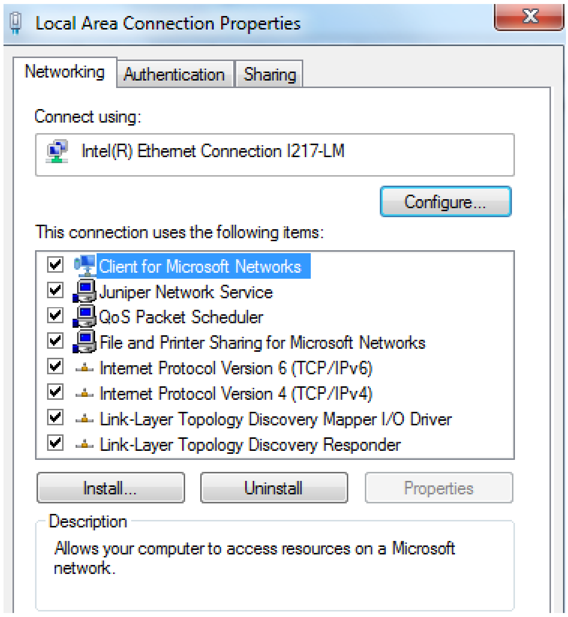
Once the device is powered up ensure the device is up and running before you try to access it based on LED status. Power LED on the cnPilot device should turn Green which indicates that the device is ready for access.

Device access using default/fallback IP

1. Select Properties for the Ethernet port. In Windows it is found in:

   a) Windows 7: Control Panel > Network and Internet > Network Connections > Local Area Connection

   b) Windows 10: Control Panel > Network and Internet > Network and Sharing Center > Local Area Connection



Connect using:

Intel(R) Ethernet Connection I217-LM

This connection uses the following items:

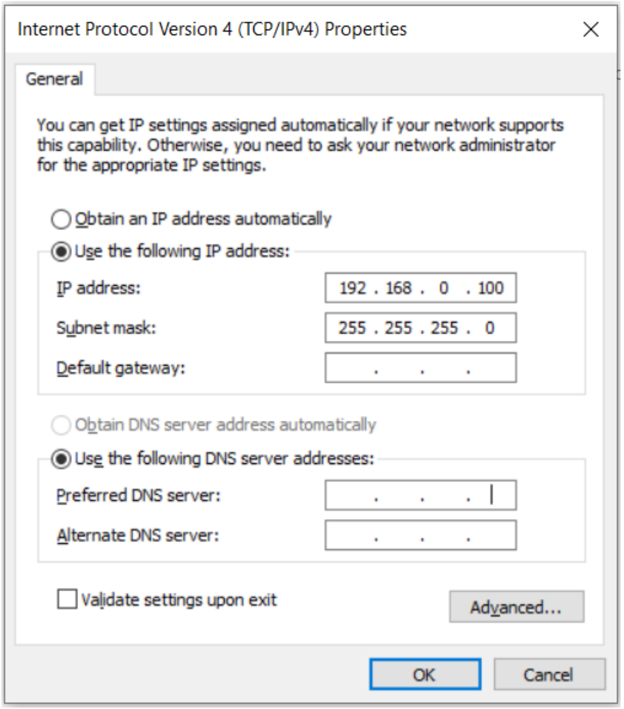
- ☑ Client for Microsoft Networks
- ☑ Juniper Network Service
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Allows your computer to access resources on a Microsoft 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 automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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

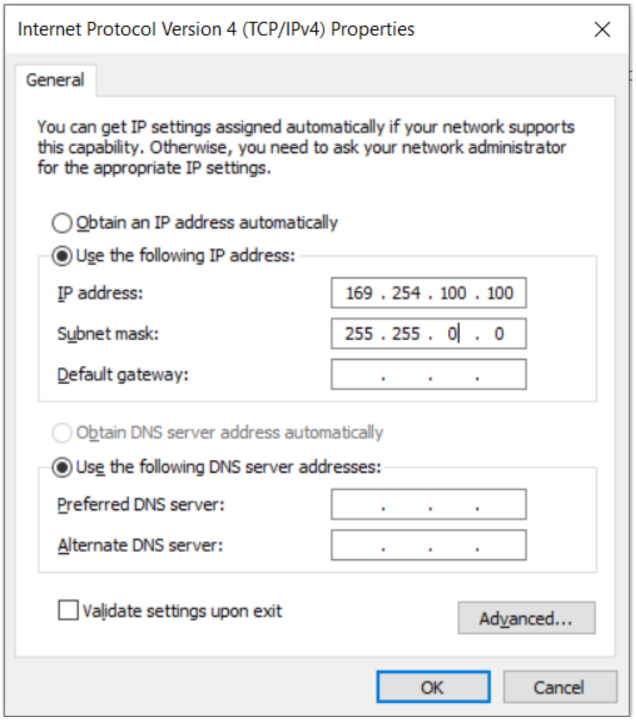
To access the device using zeroconf IP, follow the below steps:

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 automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	169 . 254 . 100 . 100
Subnet mask:	255 . 255 . 0 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

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/e430/e425H/e600 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 5 e410/e430/e425H/e600 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.
🟩	• Device is successfully up and accessible. • Wi-Fi services are up if configured.
🟦	• cnMaestro connection is successful.

The e700 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 6 e700 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.
🟩	🟧	• Device is successfully up and accessible. • Wi-Fi services are up if configured.
🟩	🟦	• Device is successfully up and accessible. • Wi-Fi services are up if configured. • cnMaestro connection is successful.

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 7 E400/E500/E501S/e502S 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.
🟩	🟧	• Device is successfully up and accessible. • Wi-Fi services are up if configured.
🟩	🟩	• Device is successfully up and accessible. • Wi-Fi services are up if configured. • cnMaestro connection is successful.

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:

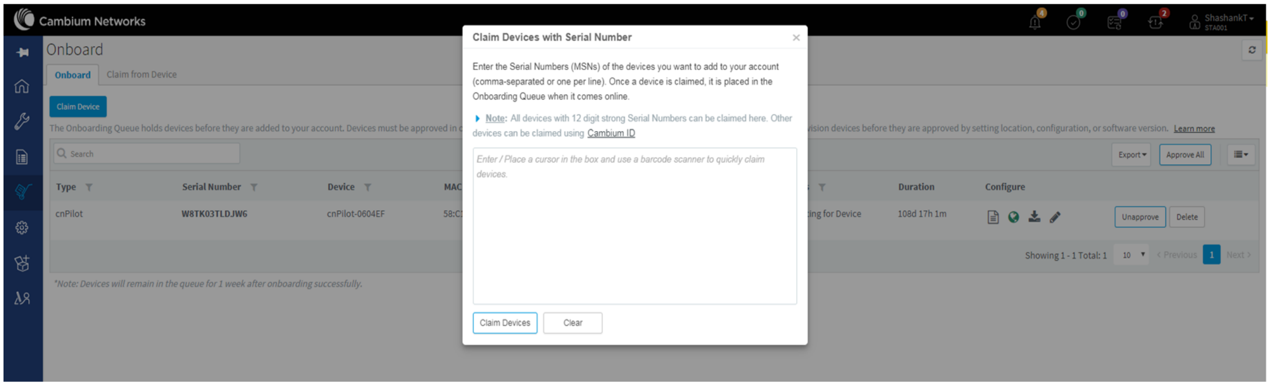
- Onboarding to cnMaestro cloud using MSN
- Onboarding to cnMaestro On-Premises
- Auto-Provisioning
- Other options

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.

Figure 4 Onboarding to cnMaestro cloud using MSN



The Onboarding Queue holds devices before they are added to your account. Devices must be approved in c… …ision devices before they are approved by setting location, configuration, or software version. Learn more

Type	Serial Number	Device	MAC		Duration	Configure
cnPilot	W8TK03TLDJW6	cnPilot-0604EF	58:C…	…ing for Device	108d 17h 1m	Unapprove Delete

Showing 1 - 1 Total: 1 10 ‹ Previous 1 Next ›

Note: Devices will remain in the queue for 1 week after onboarding successfully.

Enter the Serial Numbers (MSNs) of the devices you want to add to your account (comma-separated or one per line). Once a device is claimed, it is placed in the Onboarding Queue when it comes online.

Note: All devices with 12 digit strong Serial Numbers can be claimed here. Other devices can be claimed using Cambium ID

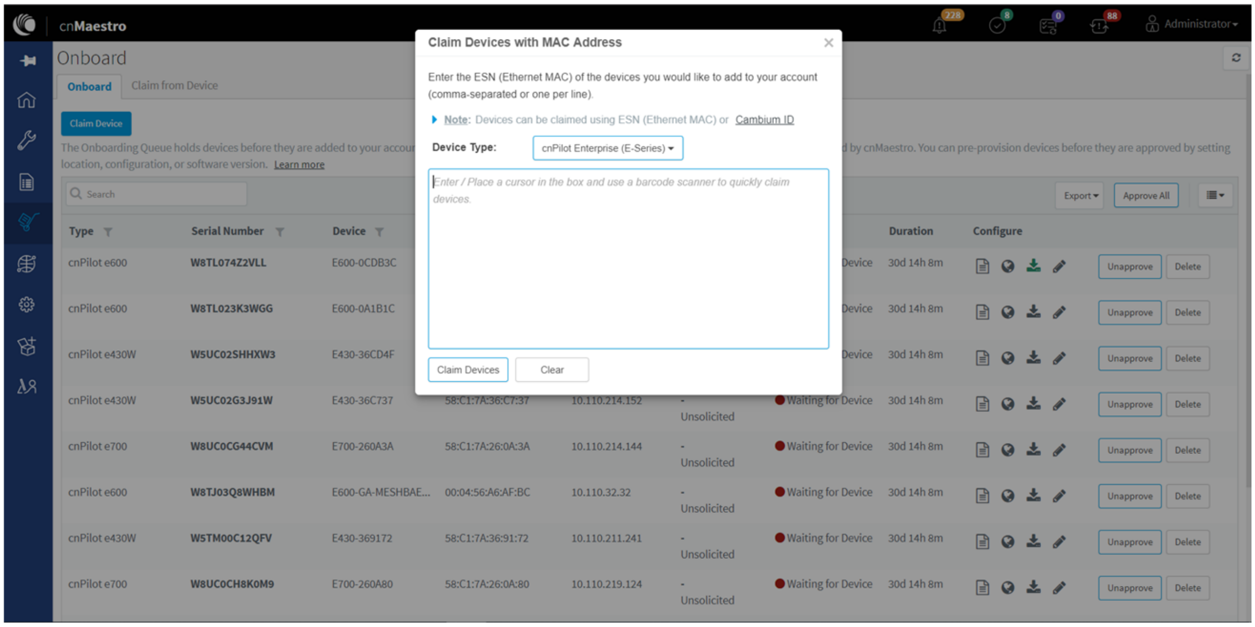
Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

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.

Figure 5 Onboarding to cnMaestro On-Premises



The Onboarding Queue holds devices before they are added to your accou… …d by cnMaestro. You can pre-provision devices before they are approved by setting location, configuration, or software version. Learn more

Enter the ESN (Ethernet MAC) of the devices you would like to add to your account (comma-separated or one per line).

Note: Devices can be claimed using ESN (Ethernet MAC) or Cambium ID

Device Type: cnPilot Enterprise (E-Series)

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Type	Serial Number	Device					Duration	Configure
cnPilot e600	W8TL074Z2VLL	E600-0CDB3C				…Device	30d 14h 8m	Unapprove Delete
cnPilot e600	W8TL023K3WGG	E600-0A1B1C				…Device	30d 14h 8m	Unapprove Delete
cnPilot e430W	W5UC02SHHXW3	E430-36CD4F				…Device	30d 14h 8m	Unapprove Delete
cnPilot e430W	W5UC02G3J91W	E430-36C737	58:C1:7A:36:C7:37	10.110.214.152	- Unsolicited	Waiting for Device	30d 14h 8m	Unapprove Delete
cnPilot e700	W8UC0CG44CVM	E700-260A3A	58:C1:7A:26:0A:3A	10.110.214.144	- Unsolicited	Waiting for Device	30d 14h 8m	Unapprove Delete
cnPilot e600	W8TJ03Q8WHBM	E600-GA-MESHBAE...	00:04:56:A6:AF:BC	10.110.32.32	- Unsolicited	Waiting for Device	30d 14h 8m	Unapprove Delete
cnPilot e430W	W5TM00C12QFV	E430-369172	58:C1:7A:36:91:72	10.110.211.241	- Unsolicited	Waiting for Device	30d 14h 8m	Unapprove Delete
cnPilot e700	W8UC0CH8K0M9	E700-260A80	58:C1:7A:26:0A:80	10.110.219.124	- Unsolicited	Waiting for Device	30d 14h 8m	Unapprove Delete

Auto-Provisioning

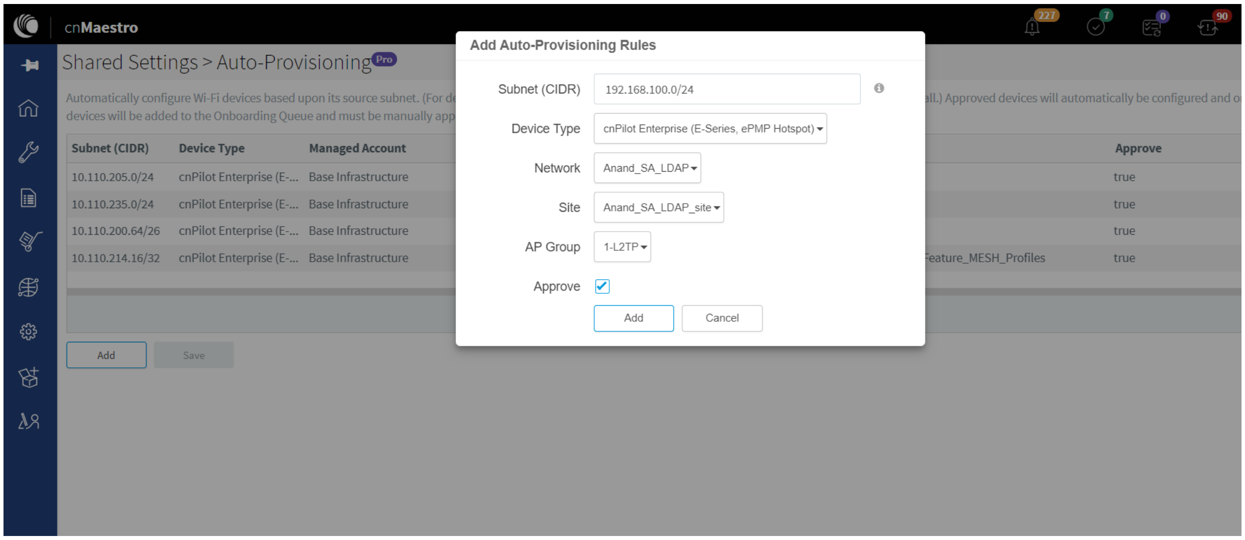
cnMaestro On-Premises supports Auto-Provisioning for cnPilot devices. This feature not only enables auto onboarding but also configures synchronization and positioning of device in the network architecture. It is triggered only at first instance of device onboarding. It can be configured on cnMaestro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

Figure 6 Auto-Provisioning



Automatically configure Wi-Fi devices based upon its source subnet. (For de ... ll.) Approved devices will automatically be configured and o
devices will be added to the Onboarding Queue and must be manually app

Subnet (CIDR)	Device Type	Managed Account		Approve
10.110.205.0/24	cnPilot Enterprise (E-...	Base Infrastructure		true
10.110.235.0/24	cnPilot Enterprise (E-...	Base Infrastructure		true
10.110.200.64/26	cnPilot Enterprise (E-...	Base Infrastructure		true
10.110.214.16/32	cnPilot Enterprise (E-...	Base Infrastructure	Feature_MESH_Profiles	true

Add Auto-Provisioning Rules

Subnet (CIDR): 192.168.100.0/24
Device Type: cnPilot Enterprise (E-Series, ePMP Hotspot)
Network: Anand_SA_LDAP
Site: Anand_SA_LDAP_site
AP Group: 1-L2TP
Approve: ☑
Add | Cancel

3. Enter the following details given in Table 8:

Table 8 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.

Parameter	Description
AP Group	Select the AP Group which needs to be applied on the device, once the device contacts the server while onboarding.
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.

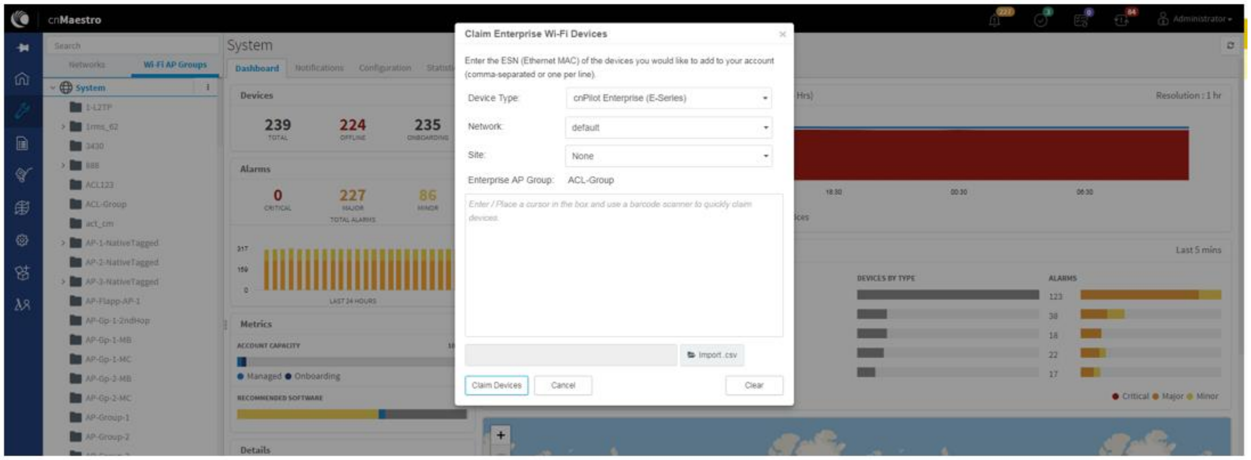
AP Group

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 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 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.

Figure 7 Claiming the device using MAC address (ESN)



Claim Enterprise Wi-Fi Devices

Enter the ESN (Ethernet MAC) of the devices you would like to add to your account (comma-separated or one per line).

Device Type: cnPilot Enterprise (E-Series)

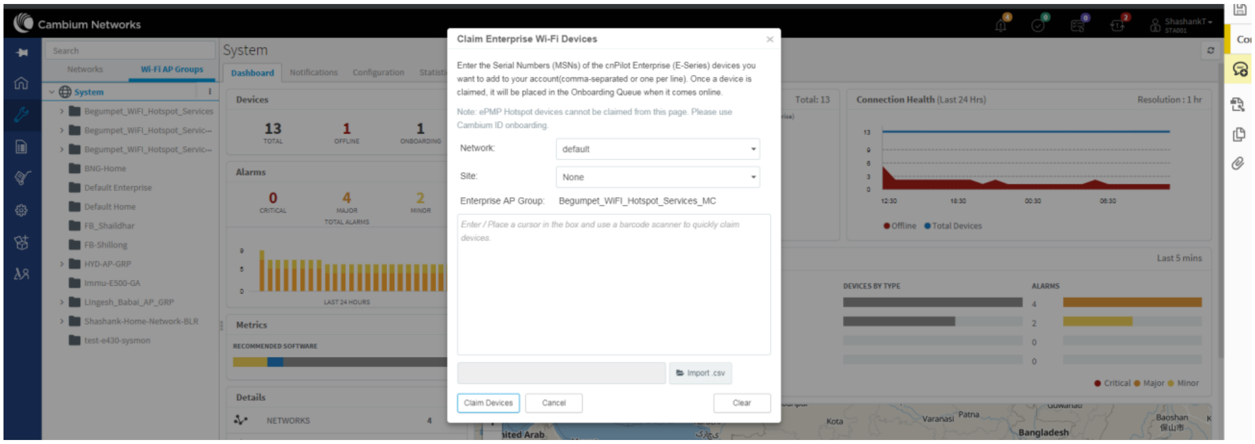
Network: default

Site: None

Enterprise AP Group: ACL-Group

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Figure 8 Claiming the device using Serial Number (MSN)



Claim Enterprise Wi-Fi Devices

Enter the Serial Numbers (MSNs) of the cnPilot Enterprise (E-Series) devices you want to add to your account(comma-separated or one per line). Once a device is claimed, it will be placed in the Onboarding Queue when it comes online.

Note: ePMP Hotspot devices cannot be claimed from this page. Please use Cambium ID onboarding.

Network: default

Site: None

Enterprise AP Group: Begumpet_WiFI_Hotspot_Services_MC

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

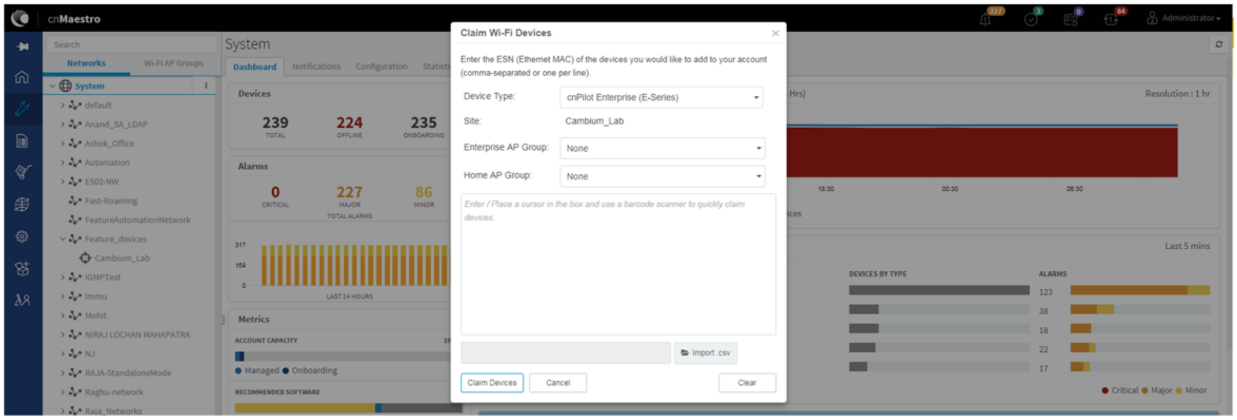
Site dashboard

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.
3. 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



Claim Wi-Fi Devices

Enter the ESN (Ethernet MAC) of the devices you would like to add to your account (comma-separated or one per line).

Device Type: cnPilot Enterprise (E-Series)

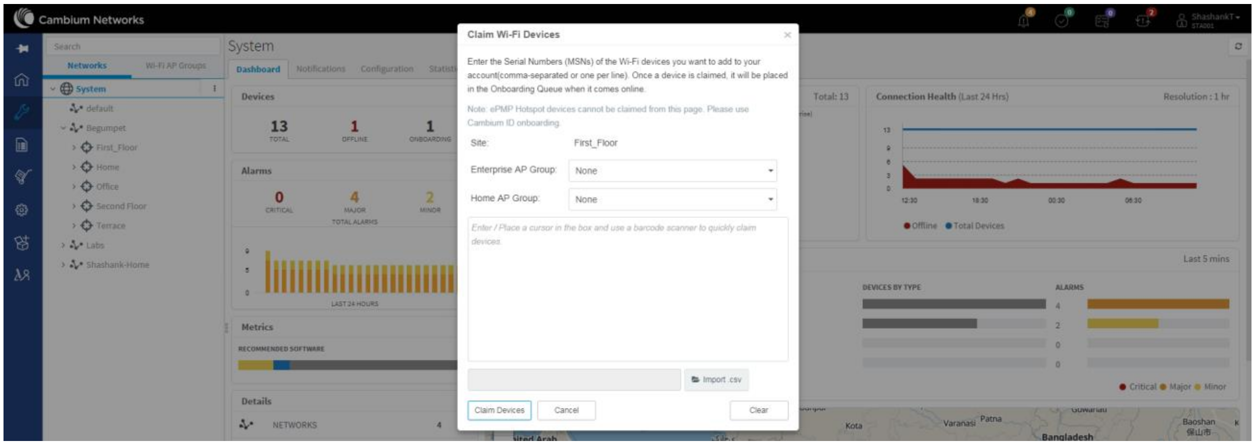
Site: Cambium_Lab

Enterprise AP Group: None

Home AP Group: None

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Figure 10 Claim the device using MSN



Claim Wi-Fi Devices

Enter the Serial Numbers (MSNs) of the Wi-Fi devices you want to add to your account(comma-separated or one per line). Once a device is claimed, it will be placed in the Onboarding Queue when it comes online.

Note: ePMP Hotspot devices cannot be claimed from this page. Please use Cambium ID onboarding.

Site: First_Floor

Enterprise AP Group: None

Home AP Group: None

Enter / Place a cursor in the box and use a barcode scanner to quickly claim devices.

Directing devices to the cnMaestro On-Premises server using DHCP

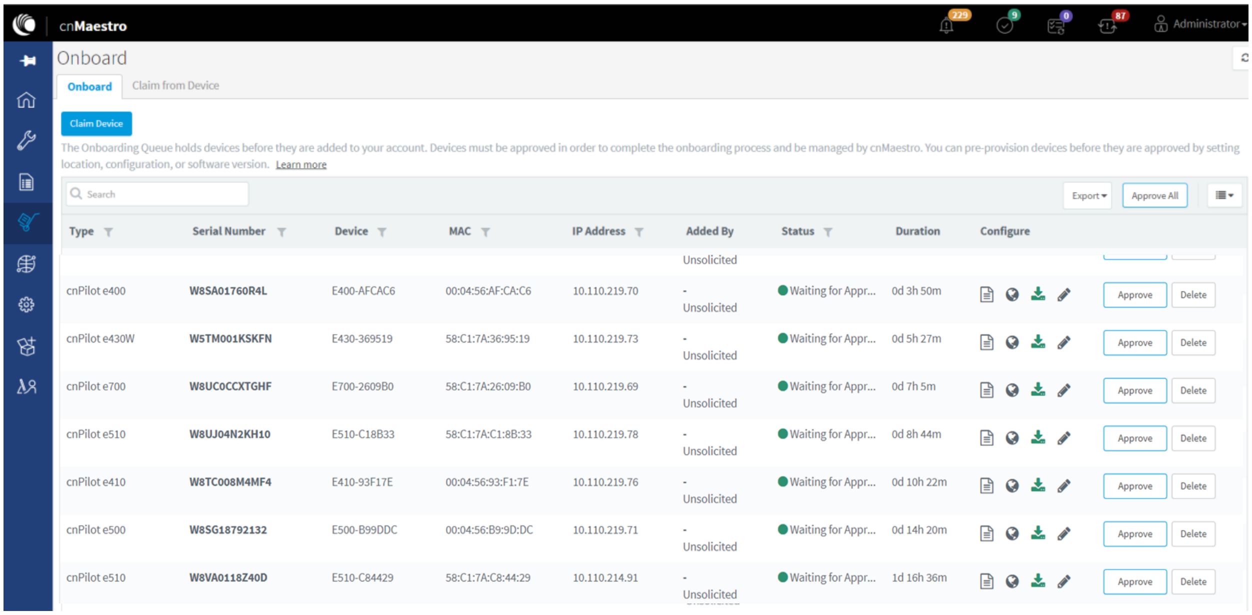
This section includes the following topics:

- DHCP Option 43
- DHCP Option 15

DHCP Option 43

This mode of onboarding is preferred to use when cnMaestro On-Premises is deployed at customer end. cnPilot reads Option 43 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 from DHCP transaction are available in Queue on cnMaestro, which needs to be further approved by end user.

Figure 11 DHCP option 43



Onboard

Onboard | Claim from Device

Claim Device

The Onboarding Queue holds devices before they are added to your account. Devices must be approved in order to complete the onboarding process and be managed by cnMaestro. You can pre-provision devices before they are approved by setting location, configuration, or software version. Learn more

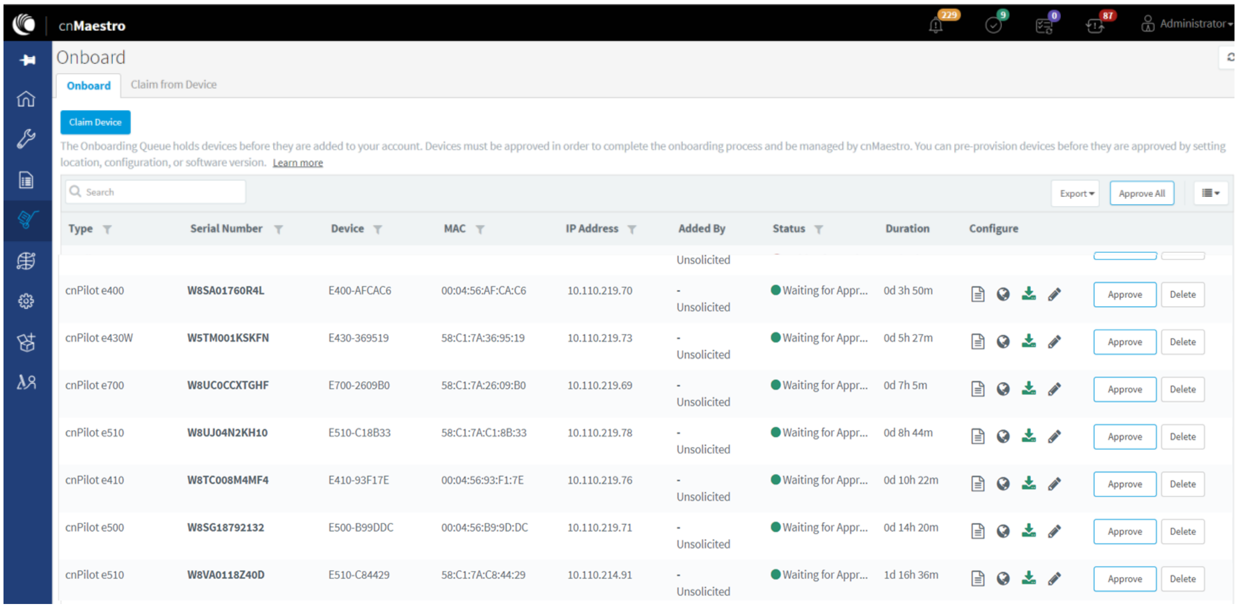
Search | Export | Approve All

Type	Serial Number	Device	MAC	IP Address	Added By	Status	Duration	Configure	
					Unsolicited				
cnPilot e400	W8SA01760R4L	E400-AFCAC6	00:04:56:AF:CA:C6	10.110.219.70	- Unsolicited	Waiting for Appr...	0d 3h 50m		Approve Delete
cnPilot e430W	W5TM001KSKFN	E430-369519	58:C1:7A:36:95:19	10.110.219.73	- Unsolicited	Waiting for Appr...	0d 5h 27m		Approve Delete
cnPilot e700	W8UC0CCXTGHF	E700-2609B0	58:C1:7A:26:09:B0	10.110.219.69	- Unsolicited	Waiting for Appr...	0d 7h 5m		Approve Delete
cnPilot e510	W8UJ04N2KH10	E510-C18B33	58:C1:7A:C1:8B:33	10.110.219.78	- Unsolicited	Waiting for Appr...	0d 8h 44m		Approve Delete
cnPilot e410	W8TC008M4MF4	E410-93F17E	00:04:56:93:F1:7E	10.110.219.76	- Unsolicited	Waiting for Appr...	0d 10h 22m		Approve Delete
cnPilot e500	W8SG18792132	E500-B99DDC	00:04:56:B9:9D:DC	10.110.219.71	- Unsolicited	Waiting for Appr...	0d 14h 20m		Approve Delete
cnPilot e510	W8VA0118Z40D	E510-C84429	58:C1:7A:C8:44:29	10.110.214.91	- Unsolicited	Waiting for Appr...	1d 16h 36m		Approve Delete

DHCP Option 15

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

Figure 12 DHCP option 15


cnMaestro
229
9
0
87
Administrator

Onboard

Onboard | Claim from Device

Claim Device

The Onboarding Queue holds devices before they are added to your account. Devices must be approved in order to complete the onboarding process and be managed by cnMaestro. You can pre-provision devices before they are approved by setting location, configuration, or software version. Learn more

Search | Export | Approve All

Type	Serial Number	Device	MAC	IP Address	Added By	Status	Duration	Configure	
					Unsolicited				
cnPilot e400	W8SA01760R4L	E400-AFCAC6	00:04:56:AF:CA:C6	10.110.219.70	- Unsolicited	Waiting for Appr...	0d 3h 50m		Approve Delete
cnPilot e430W	W5TM001KSKFN	E430-369519	58:C1:7A:36:95:19	10.110.219.73	- Unsolicited	Waiting for Appr...	0d 5h 27m		Approve Delete
cnPilot e700	W8UC0CCXTGHF	E700-2609B0	58:C1:7A:26:09:B0	10.110.219.69	- Unsolicited	Waiting for Appr...	0d 7h 5m		Approve Delete
cnPilot e510	W8UJ04N2KH10	E510-C18B33	58:C1:7A:C1:8B:33	10.110.219.78	- Unsolicited	Waiting for Appr...	0d 8h 44m		Approve Delete
cnPilot e410	W8TC008M4MF4	E410-93F17E	00:04:56:93:F1:7E	10.110.219.76	- Unsolicited	Waiting for Appr...	0d 10h 22m		Approve Delete
cnPilot e500	W8SG18792132	E500-B99DDC	00:04:56:B9:9D:DC	10.110.219.71	- Unsolicited	Waiting for Appr...	0d 14h 20m		Approve Delete
cnPilot e510	W8VA0118Z40D	E510-C84429	58:C1:7A:C8:44:29	10.110.214.91	- Unsolicited	Waiting for Appr...	1d 16h 36m		Approve Delete

DHCP server configuration

More details on various DHCP server configuration for Option 43 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:

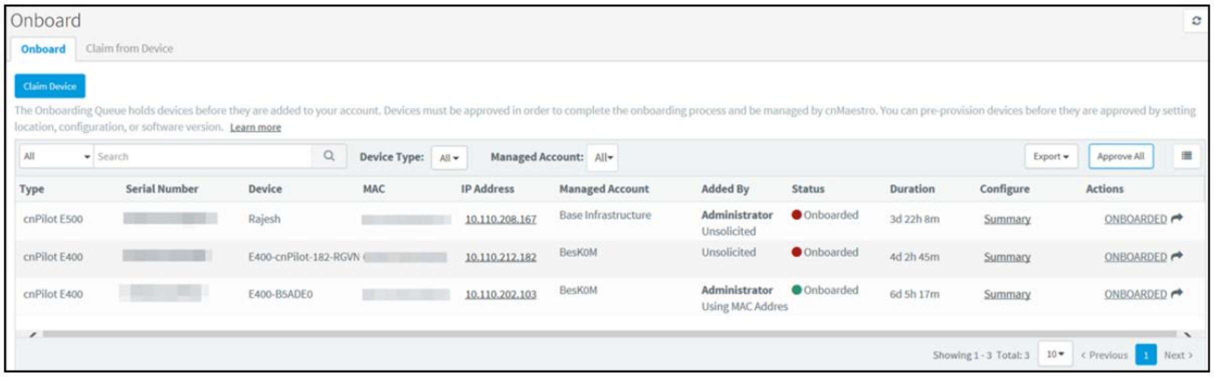
- Claim through static URL without Cambium ID and onboarding key
- Claim through static URL with Cambium ID and onboarding key

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.
2. 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.

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



Onboard

The Onboarding Queue holds devices before they are added to your account. Devices must be approved in order to complete the onboarding process and be managed by cnMaestro. You can pre-provision devices before they are approved by setting location, configuration, or software version. Learn more

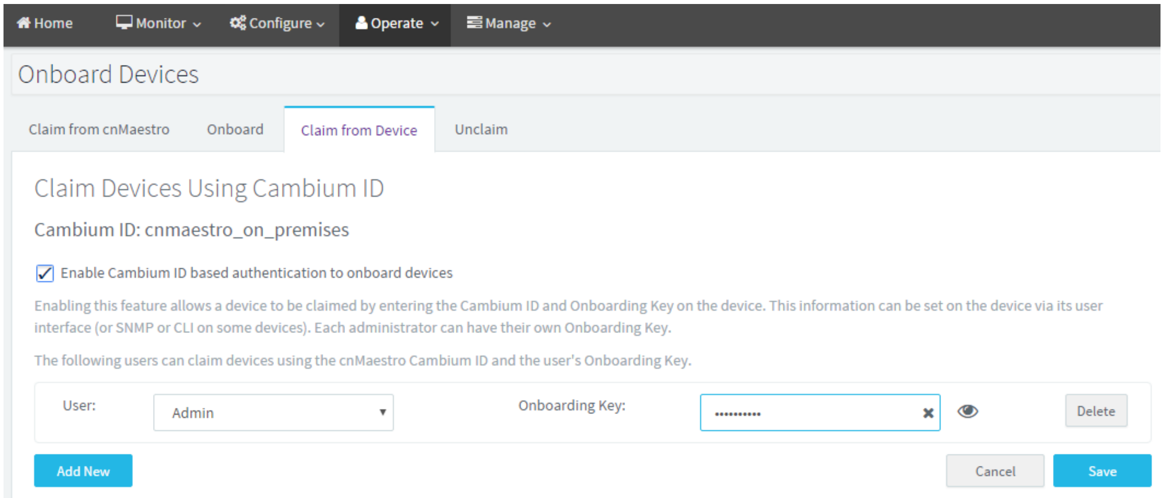
Type	Serial Number	Device	MAC	IP Address	Managed Account	Added By	Status	Duration	Configure	Actions
cnPilot E500	[redacted]	Rajesh	[redacted]	10.110.208.167	Base Infrastructure	Administrator Unsolicited	🟥 Onboarded	3d 22h 8m	Summary	ONBOARDED
cnPilot E400	[redacted]	E400-cnPilot-182-RGVN (	[redacted]	10.110.212.182	BesK0M	Unsolicited	🟥 Onboarded	4d 2h 45m	Summary	ONBOARDED
cnPilot E400	[redacted]	E400-B5ADE0	[redacted]	10.110.202.103	BesK0M	Administrator Using MAC Addres	🟩 Onboarded	6d 5h 17m	Summary	ONBOARDED

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.

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



Onboard Devices

Claim Devices Using Cambium ID

Cambium ID: cnmaestro_on_premises

☑ Enable Cambium ID based authentication to onboard devices

Enabling this feature allows a device to be claimed by entering the Cambium ID and Onboarding Key on the device. This information can be set on the device via its user interface (or SNMP or CLI on some devices). Each administrator can have their own Onboarding Key.

The following users can claim devices using the cnMaestro Cambium ID and the user's Onboarding Key.

User: Admin

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:

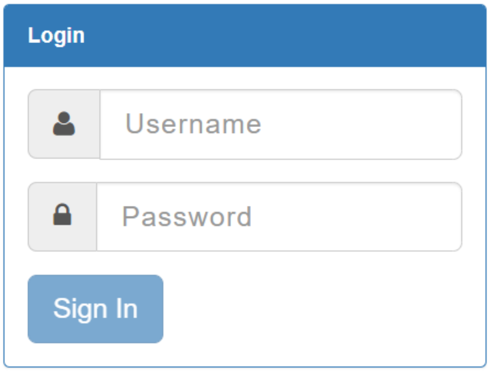
- Login screen
- Home page (Dashboard)

Login screen

To log to the UI, enter the following credentials:

- Username: admin
- Password: admin

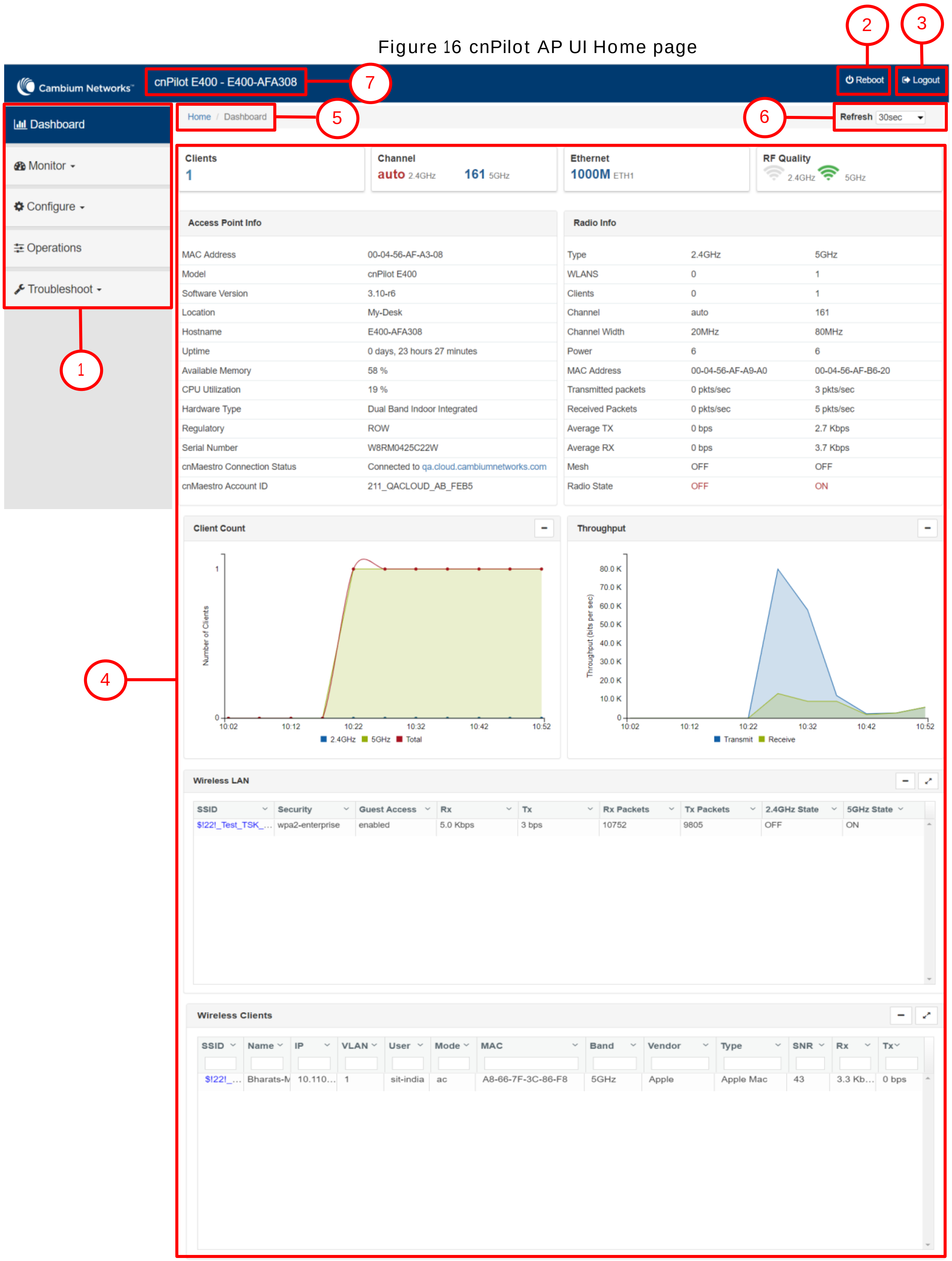
Figure 15 UI Login Page



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.

Figure 16 cnPilot AP UI Home page



Clients	Channel	Ethernet	RF Quality
1	auto 2.4GHz 161 5GHz	1000M ETH1	2.4GHz 5GHz

Access Point Info

MAC Address	00-04-56-AF-A3-08
Model	cnPilot E400
Software Version	3.10-r6
Location	My-Desk
Hostname	E400-AFA308
Uptime	0 days, 23 hours 27 minutes
Available Memory	58 %
CPU Utilization	19 %
Hardware Type	Dual Band Indoor Integrated
Regulatory	ROW
Serial Number	W8RM0425C22W
cnMaestro Connection Status	Connected to qa.cloud.cambiumnetworks.com
cnMaestro Account ID	211_QACLOUD_AB_FEB5

Radio Info

Type	2.4GHz	5GHz
WLANS	0	1
Clients	0	1
Channel	auto	161
Channel Width	20MHz	80MHz
Power	6	6
MAC Address	00-04-56-AF-A9-A0	00-04-56-AF-B6-20
Transmitted packets	0 pkts/sec	3 pkts/sec
Received Packets	0 pkts/sec	5 pkts/sec
Average TX	0 bps	2.7 Kbps
Average RX	0 bps	3.7 Kbps
Mesh	OFF	OFF
Radio State	OFF	ON

Wireless LAN

SSID	Security	Guest Access	Rx	Tx	Rx Packets	Tx Packets	2.4GHz State	5GHz State
$!22!_Test_TSK_…	wpa2-enterprise	enabled	5.0 Kbps	3 bps	10752	9805	OFF	ON

Wireless Clients

SSID	Name	IP	VLAN	User	Mode	MAC	Band	Vendor	Type	SNR	Rx	Tx
$!22!_…	Bharats-M	10.110…	1	sit-india	ac	A8-66-7F-3C-86-F8	5GHz	Apple	Apple Mac	43	3.3 Kb…	0 bps

Table 9 cnPilot AP web interface elements

Number	Element	Description
1	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 in Menu section. Usually, this area contains details of configuration or statistics or provision to configure cnPilot device.
5	UI path	Provides UI navigation path information to user.
6	UI refresh interval	Provision to reload updated statistics at regular intervals.
7	Model number	Provides information related to cnPilot model number and configured hostname.

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 10 Configuration: System parameters

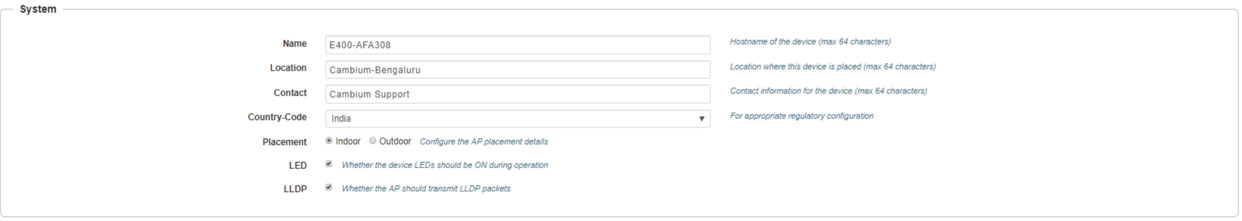
Parameter	Description	Range	Default
Name	Hostname of the device. Configurable maximum length of hostname is 64 characters.	–	cnPilot Model Number-Last 3 Bytes of ESN
Location	The location where the device is placed. The maximum length of location is 64 characters.	–	–
Contact	Contact information for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

Parameter	Description	Range	Default
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. Enable LED checkbox.
7. Enable LLDP checkbox.
8. Click Save.

Figure 17 Configuration: System page



System

Name: E400-AFA308 — *Hostname of the device (max 64 characters)*

Location: Cambium-Bengaluru — *Location where this device is placed (max 64 characters)*

Contact: Cambium Support — *Contact information for the device (max 64 characters)*

Country-Code: India ▾ — *For appropriate regulatory configuration*

Placement: ● Indoor ○ Outdoor — *Configure the AP placement details*

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:

Table 11 Configuration: System > Management parameters

Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	–	admin
Autopilot	Provision to configure mode of cnPilot device when Autopilot is enabled in network:	–	Default

Parameter	Description	Range	Default
	• Default Every cnPilot device by default operates as Auto-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 to add Public Key in this section. If configured, user has to login to AP using Private Keys. This is applicable for 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 Auth	User has provision to control login to AP using RADIUS authentication. If enabled, every credential that are provided by user undergo RADIUS authentication. If success, allowed to login to UI of AP. This is applicable for both CLI and GUI.	–	Disabled
RADIUS Server	Provision to configure RADIUS server for Management Authentication.	–	–
RADIUS Secret	Provision to configure RADIUS shared secret for Management authentication.	–	–
cnMaestro			
Cambium Remote Mgmt.	Enables support for Cambium Remote Management of this device.	–	Enabled

Parameter	Description	Range	Default
Validate Server Certificate	This allows HTTPs connection between cnMaestro and cnPilot device.	–	Enabled
cnMaestro URL	Static provision to onboard device.	–	–
Cambium ID	Cambium ID used for provisioning cnMaestro (Cambium Remote Management) of this device.	–	–
Onboarding Key	Password used for onboarding the device to cnMaestro.	–	–
SNMP			
Enabled	Provision to enable SNMPv2 or SNMPv3 support on device	–	–
SNMPv2c RO community	SNMP v2c read-only community string.	–	–
SNMPv2c RW community	SNMP v2c read-write community string.	–	–
Trap Receiver IP	Provision to configure SNMP trap receiver server IP.	–	–
SNMPv3 Username	Enter username for SNMPv3.	–	–
SNMPv3 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.

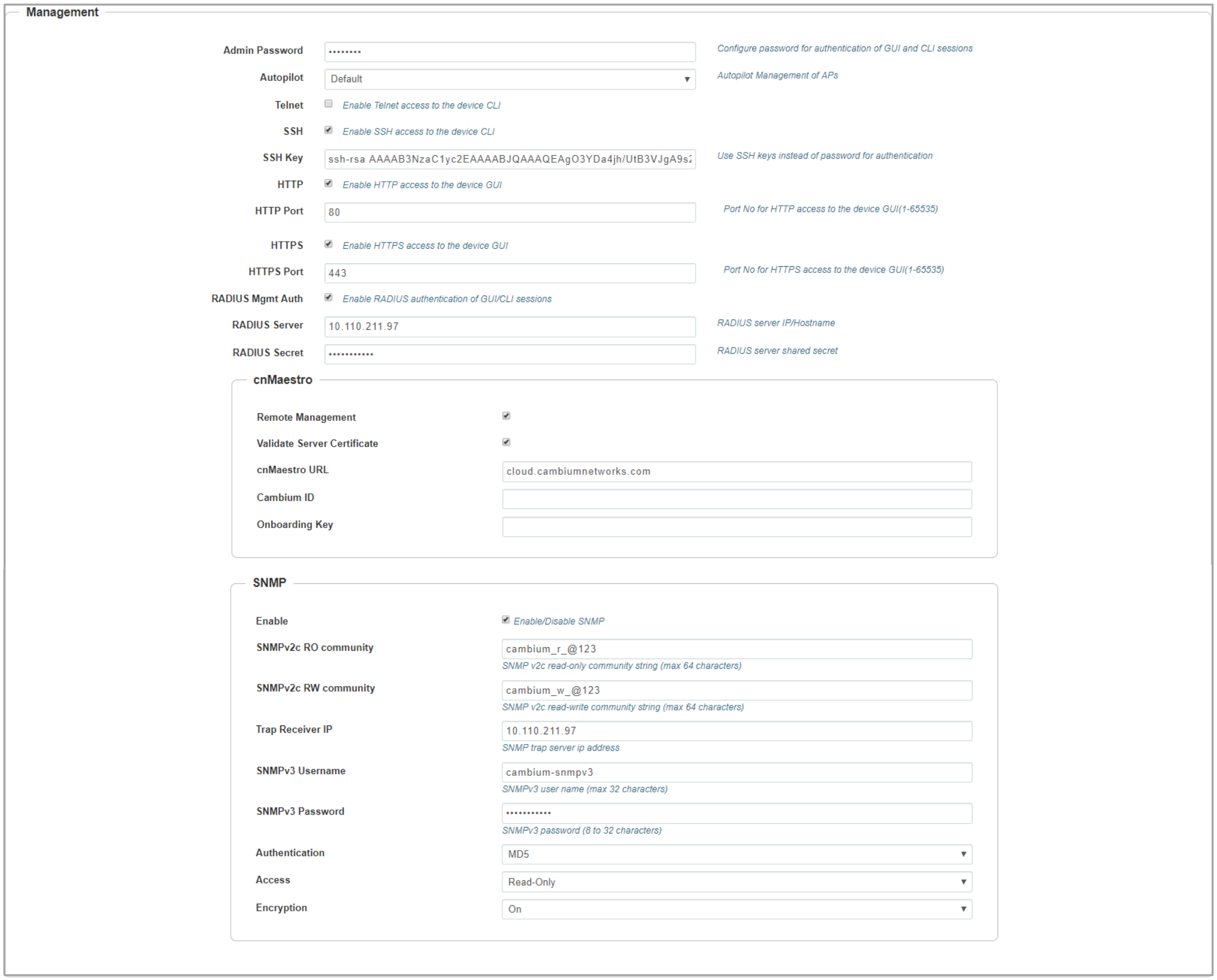
To configure cnMaestro:

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 IP (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.

Figure 18 Configuration: Management page



Management

Admin Password	••••••••	Configure password for authentication of GUI and CLI sessions
Autopilot	Default ▾	Autopilot Management of APs
Telnet	☐ Enable Telnet access to the device CLI	
SSH	☑ Enable SSH access to the device CLI	
SSH Key	ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAgO3YDa4jh/UtB3VJgA9s:	Use SSH keys instead of password for authentication
HTTP	☑ 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)
RADIUS Mgmt Auth	☑ Enable RADIUS authentication of GUI/CLI sessions	
RADIUS Server	10.110.211.97	RADIUS server IP/Hostname
RADIUS Secret	•••••••••••	RADIUS server shared secret

cnMaestro

Remote Management	☑
Validate Server Certificate	☑
cnMaestro URL	cloud.cambiumnetworks.com
Cambium ID	
Onboarding Key	

SNMP

Enable	☑ Enable/Disable SNMP
SNMPv2c RO community	cambium_r_@123 SNMP v2c read-only community string (max 64 characters)
SNMPv2c RW community	cambium_w_@123 SNMP v2c read-write community string (max 64 characters)
Trap Receiver IP	10.110.211.97 SNMP trap server ip address
SNMPv3 Username	cambium-snmpv3 SNMPv3 user name (max 32 characters)
SNMPv3 Password	••••••••••• SNMPv3 password (8 to 32 characters)
Authentication	MD5 ▾
Access	Read-Only ▾
Encryption	On ▾

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 IP 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:

Table 12 Configuration: System > Time Settings parameters

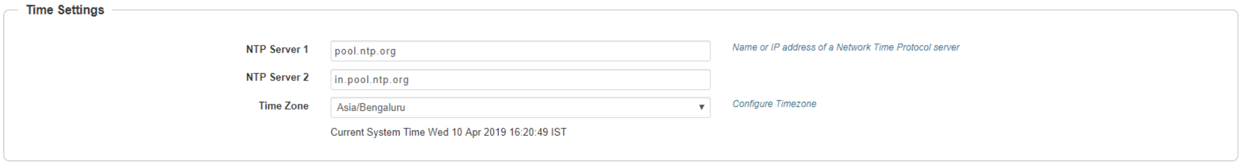
Parameter	Description	Range	Default
NTP Server 1	Name or IP address of a Network Time Protocol server 1.	–	–
NTP Server 2	Name or IP address of a Network Time Protocol server 2.	–	–

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. 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 IP address of the NTP server 1 in the NTP Server 1 textbox.
2. Enter the name or IP 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: pool.ntp.org — Name or IP address of a Network Time Protocol server

NTP Server 2: in.pool.ntp.org

Time Zone: Asia/Bengaluru — Configure Timezone

Current System Time Wed 10 Apr 2019 16:20:49 IST

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.

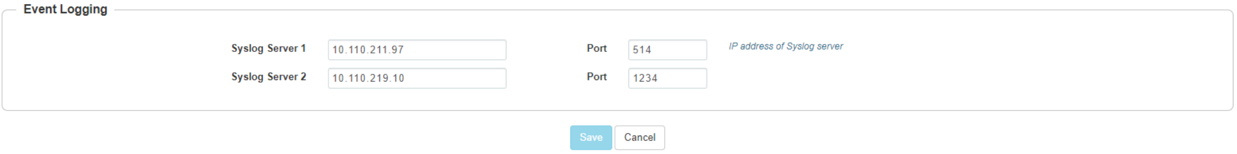
Table 13 Configuration: System > Event Logging parameters

Parameter	Description	Range	Default
Syslog Server 1	Hostname or IP address of the Syslog server and respective port number.	–	514
Syslog Server 2	Hostname or IP address of the Syslog server and respective port number.	–	514

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

1. Enter the FQDN or IP 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 IP 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. Click Save.

Figure 20 Configuration: Event Logging page



Event Logging

Syslog Server 1	10.110.211.97	Port	514	IP address of Syslog server
Syslog Server 2	10.110.219.10	Port	1234	

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.

Table 14 Configure: Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables operation of radio.	–	–
Channel	User can select the channel from the drop-down list. Channels in drop-down list is populated based on Country selected in Configuration > System UI.	• 2.4GHz: 1 - 14 • 5GHz: 36 - 173	Auto
Channel Width	User can select operating width of the channel. • For 2.4GHz: Only 20MHz channel width is supported. • For 5GHz: 20MHz, 40MHz and 80MHz channel width is supported.	–	• 20MHz for 2.4GHz • 80MHz for 5GHz
Transmit Power	User can configure transmit power of each radio based on coverage and SLA. Unit of transmit power is in dBm and its range is from 4 to 30. Maximum transmit power of cnPilot devices varies based on model number. More details of transmit power supported by each cnPilot device is available at	• 2.4GHz: 4 - 30 • 5GHz: 4 - 30	Auto

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

Parameter	Description	Range	Default
	• For 5GHz: ○ All ○ Specific ○ Prefer Non-DFS ○ Prefer DFS		
Mode	All cnPilot devices are either 802.11ac Wave 1 or 802.11ac Wave 2 supported. There are few legacy clients which might not work as expected, hence this parameter can be tuned to backward compatibility based on wireless clients.	• 2.4GHz: b, bg, n, gn • 5GHz: a, ac, an, n, n-ac.	• 11n mixed mode for 2.4GHz • 11ac for 5GHz
Short Guard 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 Selection Mode	AutoRF supports two modes of channel selection: • Interference based • Channel Utilization based	–	Interference
Channel Hold Time	Configure time period for the device to be on same channel selected by auto-rf algorithm, irrespective of quality of channel after selection.	5-1800	120 Min
Channel Utilization Threshold	Configure the utilization thresholds to trigger channel selection by auto-rf.	20-40	25%

Parameter	Description	Range	Default
Interference Avoidance			
Packet Error Rate Threshold	This is a trigger mechanism to move out of current channel when configured threshold is met.	0-100	30%
Enhanced Roaming			
Enable	Provision to enable enhanced roaming on device.	–	Disabled
Roam SNR threshold	cnPilot device triggers de-authentication of wireless station, when the wireless station is seen at configured 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 drop-down 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:

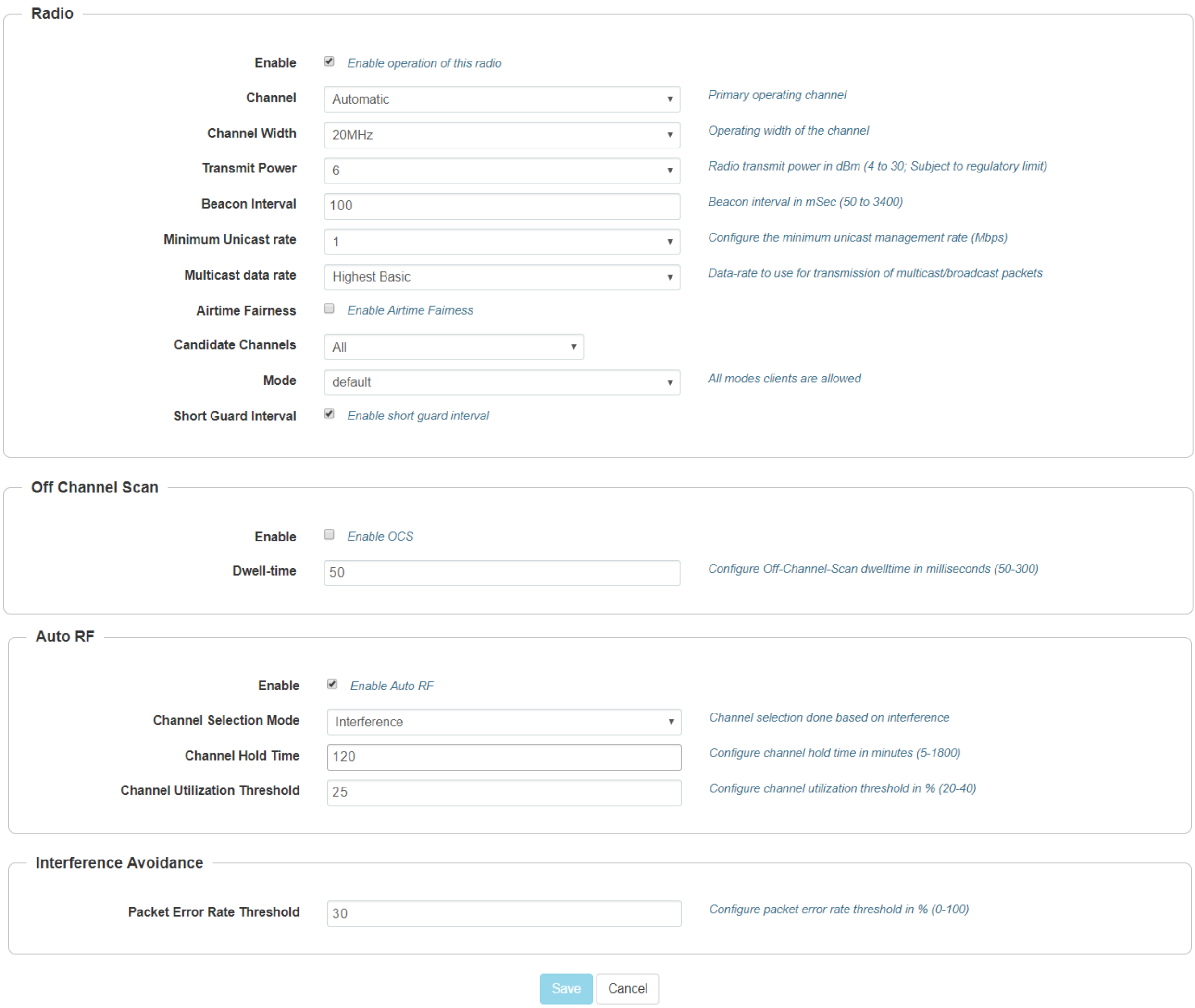
1. Select Enable checkbox to enable the operations of this radio.
2. Select Channel Selection Mode from the drop-down list.
3. Enter Channel Hold Time in minutes in the textbox.

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



Radio

Enable ☑ Enable operation of this radio

Channel: Automatic — Primary operating channel

Channel Width: 20MHz — Operating width of the channel

Transmit Power: 6 — Radio transmit power in dBm (4 to 30; Subject to regulatory limit)

Beacon Interval: 100 — Beacon interval in mSec (50 to 3400)

Minimum Unicast rate: 1 — Configure the minimum unicast management rate (Mbps)

Multicast data rate: Highest Basic — Data-rate to use for transmission of multicast/broadcast packets

Airtime Fairness ☐ Enable Airtime Fairness

Candidate Channels: All

Mode: default — All modes clients are allowed

Short Guard Interval ☑ Enable short guard interval

Off Channel Scan

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 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)

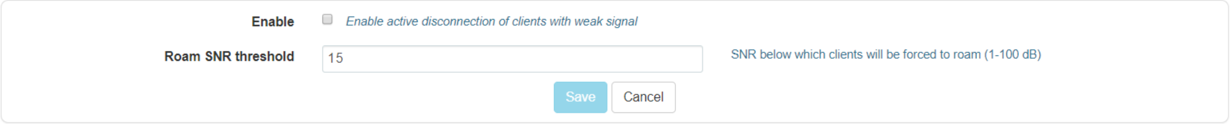
Interference Avoidance

Packet Error Rate Threshold: 30 — Configure packet error rate threshold in % (0-100)

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)

Chapter 8: Configuration - Wireless LAN

This chapter describes the following topics:

- Overview
- Configuring WLAN parameters

Overview

cnPilot devices support up-to 16 unique WLANs per radio. 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 15 Configure: WLAN > Basic parameters

Parameters	Description	Range	Default
WLAN > Basic			
Enable	Option to enable a WLAN profile. Once enabled, a Beacon is broadcasted with SSID and respective configured parameters in a WLAN profile.	–	–
Mesh	This parameter is required when a WDS connection is established with cnPilot devices. Four options are available under this parameter: 1. Base 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. 2. Client A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-based AP to connect.	–	OFF (Access Profile Mode)

Parameters	Description	Range	Default
	3. Recovery A WLAN profile configured as mesh-recovery will broadcast pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on mesh-base device. Mesh-client will auto scan for mesh-recovery SSID upon failure of mesh link. 4. Off Mesh support disable on WLAN profile.		
SSID	SSID is the unique network name that wireless stations scans and associates.	–	–
VLAN	VLAN is configured to segregate wireless station traffic from AP traffic in the network. Wireless stations obtain IP address from the subnet configured in VLAN field of WLAN profile.	1-4094	1
Security	This parameter determines key values that is encrypted based on selected algorithm. Following security methods are supported by cnPilot devices: 1. Open This method is preferred when Layer 2 authentication is built in the network. With this configured on cnPilot device, any wireless station will be able to connect. 2. Osen This method is extensively used when Passpoint 2.0 is enabled on cnPilot devices. If Passpoint 2.0 is disabled, this security plays no role in wireless station association. 3. WPA2-Pre-Shared Keys This mode is supported with AES encryption. 4. WPA2 Enterprise This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication method.	–	Open
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 and 5GHz

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

Parameters	Description	Range	Default
	1. Disable This option when selected disables client isolation feature. i.e. any wireless station can communicate to other wireless station. 2. Local 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. Static This option when configured enables client isolation feature across network. User has to configure gateway MAC to access device across subnets.		
cnMaestro Managed Roaming	By default, cnPilot devices support Layer 2 roaming. This option enables Layer 3 roaming. It is mandatory that cnPilot devices are connected to cnMaestro. Layer 3 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 Timeout	This field is specific to non-guest wireless stations. When a wireless station connects, a session timer is triggered. Once session time expires, wireless station has to undergo either re-authentication or re-association based on state of wireless station. By default, it is enabled.	60-604800	28800
Inactivity Timeout	Inactivity timer triggers whenever there is no communication between cnPilot device and wireless station associated to cnPilot device. Once the timer reaches the configured Inactivity timeout value, APs sends a de-authentication to that wireless station. By default, it is enabled.	60-28800	1800
Drop Multicast 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:

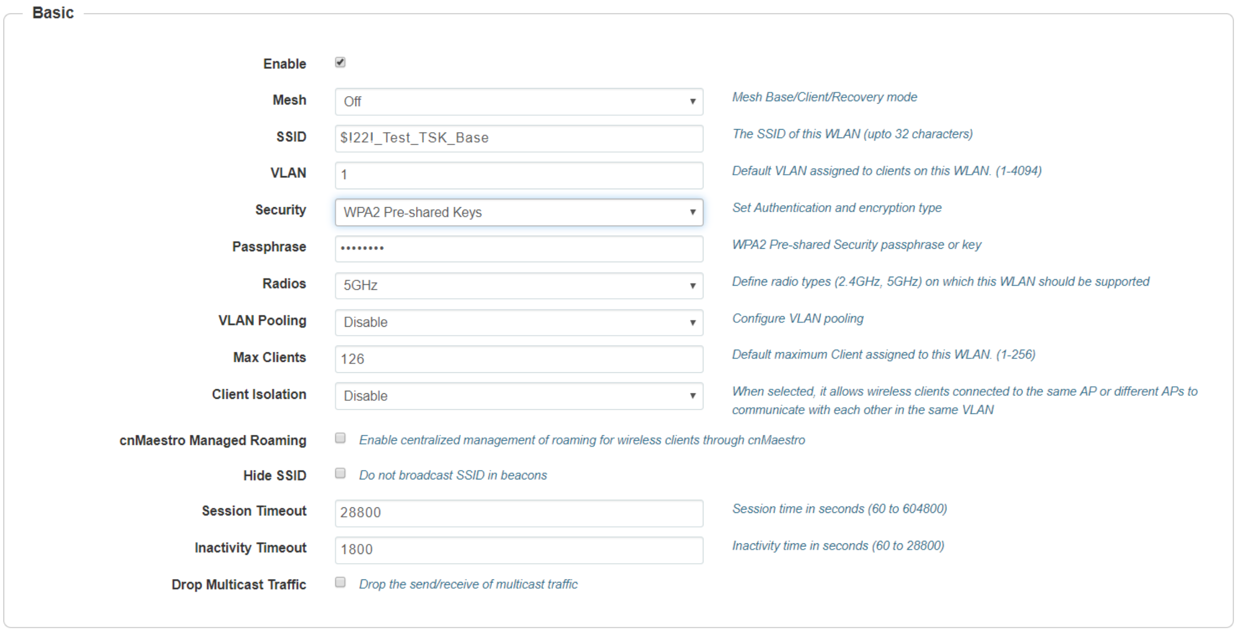
1. Select the Enable checkbox to enable a particular WLAN.
2. Select the operating parameters from the Mesh drop-down list.

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 16 WLAN (Max Clients) parameters

Number of Clients	2.4GHz	5GHz
e600 and e700	512	512
e410 and e430	256	256
E400 and E500/E501S/e502S	256	128
e425H	100	100

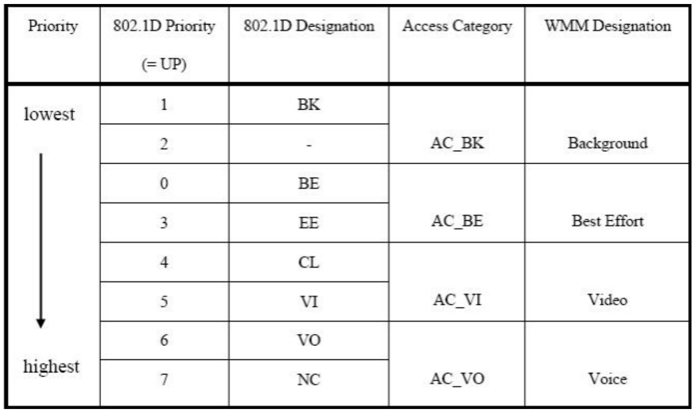
Figure 23 Configure: WLAN > Basic parameter



Basic

Enable	☑	
Mesh	Off ▾	*Mesh Base/Client/Recovery mode*
SSID	$!22!_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 ▾	*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 communicate with each other in the same VLAN*
cnMaestro Managed Roaming	☐ *Enable centralized management of roaming for wireless clients through 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*	

Table 17 Configure: WLAN > Advanced parameters

<table>
<tr><th>Parameters</th><th>Description</th><th>Range</th><th>Default</th></tr>
<tr><td colspan="4">WLAN > Advanced</td></tr>
<tr><td>UAPSD</td><td>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.

<table>
<tr><th>Priority</th><th>802.1D Priority (= UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr>
<tr><td>lowest</td><td>1</td><td>BK</td><td>AC_BK</td><td>Background</td></tr>
<tr><td></td><td>2</td><td>-</td><td></td><td></td></tr>
<tr><td></td><td>0</td><td>BE</td><td>AC_BE</td><td>Best Effort</td></tr>
<tr><td></td><td>3</td><td>EE</td><td></td><td></td></tr>
<tr><td></td><td>4</td><td>CL</td><td>AC_VI</td><td>Video</td></tr>
<tr><td></td><td>5</td><td>VI</td><td></td><td></td></tr>
<tr><td></td><td>6</td><td>VO</td><td>AC_VO</td><td>Voice</td></tr>
<tr><td>highest</td><td>7</td><td>NC</td><td></td><td></td></tr>
</table></td><td>–</td><td>Disabled</td></tr>
<tr><td>QBSS</td><td>When enabled, appends QBSS IE in Management frames. This IE provides information of channel usage by AP, so that smart wireless station can decide better AP for connectivity. Station count, Channel utilization and</td><td>–</td><td>Disabled</td></tr>
</table>

Parameters	Description	Range	Default
	Available admission capacity are the information available in this IE.		
DTIM interval	This parameter plays a key role when power save supported mobile stations are part of infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.	1-255	1
Monitored Host			
Host	This feature is required where there is interrupted backbone network. cnPilot device monitors the reachability of hostname/IP configured in this parameter and modifies the state of WLAN.	–	Disabled
Interval	The frequency of monitoring the network health based on the status of keep-alive mechanism w.r.t configured monitored host.	60-3600 Sec	300
Attempts	The number of packets in the keep-alive mechanism to determine the status.	1-20	1
DNS Logging Host	This feature is required when an Administrator requires to monitor the websites accessed by wireless stations connected to WLAN profile.	–	Disabled
Connection Logging Host	When enabled provides information of all TCP connections accessed by a wireless station that is associated to WLAN.	–	Disabled
Band Steering	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. • Low • Normal • Aggressive	–	Disabled
Proxy ARP	Provision to avoid ARP flood in wireless network. When enabled, AP responds to ARP requests for the wireless stations connected to that AP. This is for IPv4 infrastructure.	–	Enabled
Proxy ND	Provision to avoid ARP flood in wireless network. When enabled, AP responds to ARP requests for the wireless	–	Disabled

Parameters	Description	Range	Default
	stations connected to that AP. This is for IPv6 infrastructure.		
Unicast DHCP	Provision to transmit DHCP offer and ACK/NACK packets as Unicast packets to wireless stations.	–	Enabled
Insert DHCP Option 82	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: • Hostname • AP MAC • BSSID • SSID • VLAN ID • Site ID • Custom • All	–	Disabled
Tunnel Mode	This option is enabled when user traffic is tunneled to DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	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. Select any one of the following: 1. OKC 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. 2. 802.11r This is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake	–	Disabled

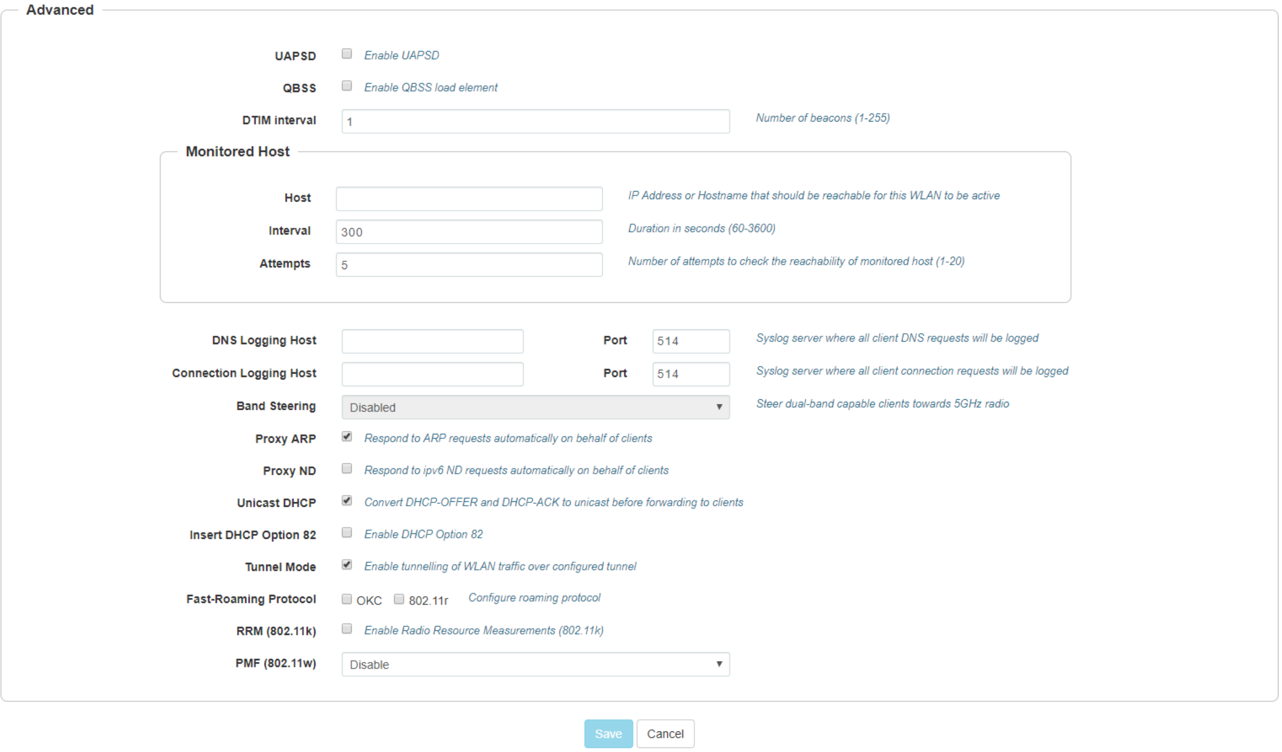
Parameters	Description	Range	Default
	with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT).		
RRM (802.11k)	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 11k clients. Following parameters needs to be enabled: • Enable OCS • Enable RRM • Support for WPA2 authentication method	–	Disabled
PMF (802.11w)	802.11w, also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames makes wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	• Optional • Mandatory • Disabled	–
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms
Association Comeback Time	This value is included in the Association Response as an Association Comeback Time information element. AP 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 hoist in the Attempts drop-down 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.

Figure 24 Configure: WLAN > Advanced parameter



Advanced

UAPSD □ Enable UAPSD

QBSS □ Enable QBSS load element

DTIM interval: 1 — Number of beacons (1-255)

Monitored Host

Host: — IP Address or Hostname that should be reachable for this WLAN to be active

Interval: 300 — Duration in seconds (60-3600)

Attempts: 5 — Number of attempts to check the reachability of monitored host (1-20)

DNS Logging Host: — Port: 514 — Syslog server where all client DNS requests will be logged

Connection Logging Host: — Port: 514 — Syslog server where all client connection requests will be logged

Band Steering: Disabled — Steer dual-band capable clients towards 5GHz radio

Proxy ARP ☑ Respond to ARP requests automatically on behalf of clients

Proxy ND □ Respond to ipv6 ND requests automatically on behalf of clients

Unicast DHCP ☑ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients

Insert DHCP Option 82 □ Enable DHCP Option 82

Tunnel Mode ☑ Enable tunnelling of WLAN traffic over configured tunnel

Fast-Roaming Protocol □ OKC □ 802.11r Configure roaming protocol

RRM (802.11k) □ Enable Radio Resource Measurements (802.11k)

PMF (802.11w): Disable

Table 18 Configure: WLAN > Radius Server parameters

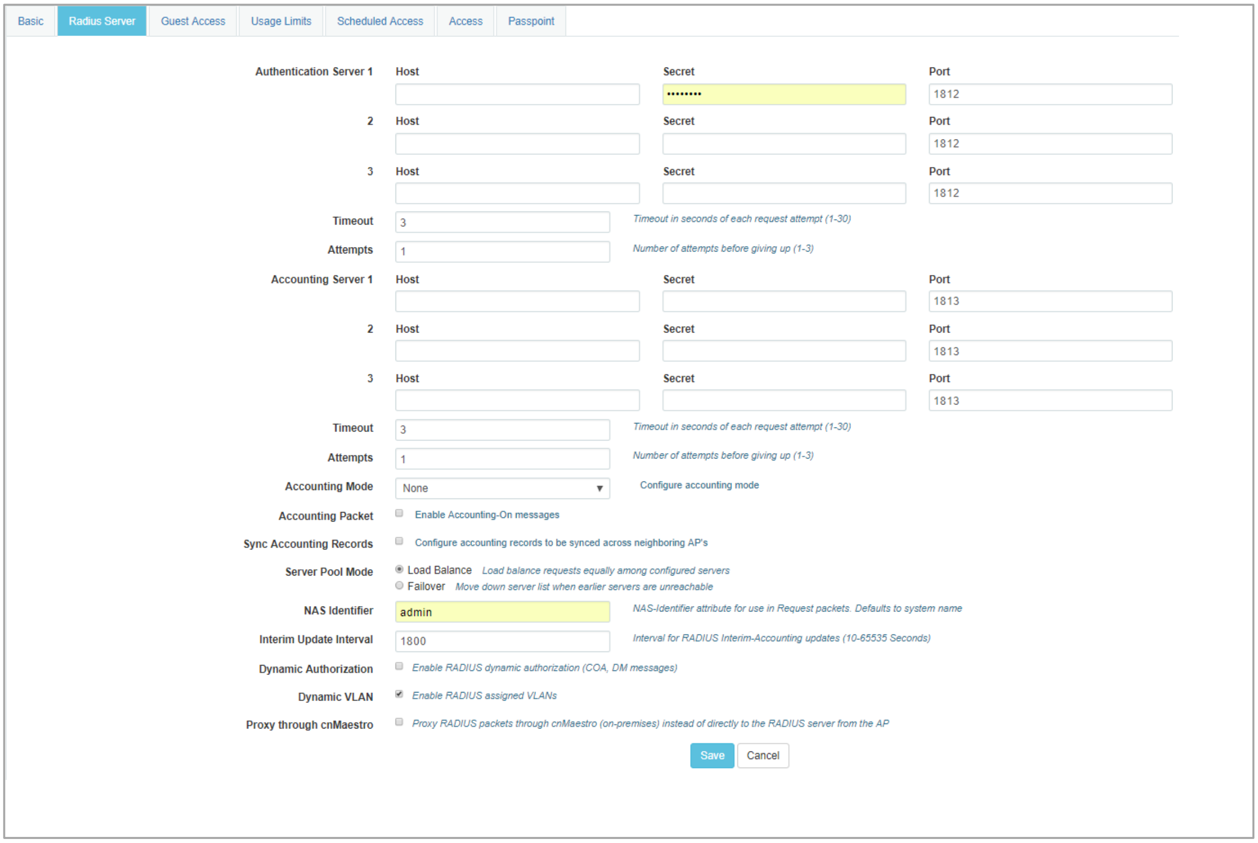
Parameters	Description	Range	Default
Authentication Server	Provision to configure RADIUS Authentication server details such as Hostname, Shared Secret, Port Number and Realm. Maximum of three RADIUS server can be configured.	–	Disabled
Accounting Server	Provision to configure Accounting server details such as Hostname, Shared Secret, Port Number. 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 Mode	This field is enabled based on customer requirement. Accounting packet is transmitted based on mode selected. 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 server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects.	–	Disabled
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	–	Disabled
Sync Accounting Records	When enabled, will share the accounting records when wireless stations move across different AP that are Layer 2 connected.	–	Disabled
Server Pool Mode	User can configure multiple Authorization and Accounting servers. Based on number of wireless stations, user can choose either Failover or Load Balance mode. 1. Load Balance AP communicates with multiple servers and ensures that authorization and accounting are equally shared across configured servers.	–	Load Balance

Parameters	Description	Range	Default
	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/ System Name
Interim Update Interval	This field is used when RADIUS accounting is enabled and mode selected as Start-Interim-Stop.	10-65535	1800
Dynamic Authorization	This option is required, where there is a CoA requests from AAA/RADIUS server.	–	Disabled
Dynamic VLAN	When enabled, AP honors the VLAN information provided in RADIUS transaction. Wireless station requests IP address from the same VLAN learnt through RADIUS.	–	Enabled
Proxy through cnMaestro	This option is enabled, whenever cnMaestro is required to act as proxy server to RADIUS authentication requests coming from cnPilot devices that are connected to cnMaestro.	–	Disabled

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. Click Save.

Figure 25 Configure: WLAN > Radius Server parameter



Authentication Server 1 Host: Secret: •••••••• Port: 1812

2 Host: Secret: Port: 1812

3 Host: Secret: Port: 1812

Timeout: 3 *Timeout in seconds of each request attempt (1-30)*

Attempts: 1 *Number of attempts before giving up (1-3)*

Accounting Server 1 Host: Secret: Port: 1813

2 Host: Secret: Port: 1813

3 Host: Secret: Port: 1813

Timeout: 3 *Timeout in seconds of each request attempt (1-30)*

Attempts: 1 *Number of attempts before giving up (1-3)*

Accounting Mode: None ▾ Configure accounting mode

Accounting Packet: □ Enable Accounting-On messages

Sync Accounting Records: □ Configure accounting records to be synced across neighboring AP's

Server Pool Mode: ● Load Balance *Load balance requests equally among configured servers*
○ Failover *Move down server list when earlier servers are unreachable*

NAS Identifier: admin *NAS-Identifier attribute for use in Request packets. Defaults to system name*

Interim Update Interval: 1800 *Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)*

Dynamic Authorization: □ *Enable RADIUS dynamic authorization (COA, DM messages)*

Dynamic VLAN: ☑ *Enable RADIUS assigned VLANs*

Proxy through cnMaestro: □ *Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP*

Table 19 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: 1. Clickthrough This mode allows the users to get access data without any authentication mechanism. User can access internet as soon as he is connected and accepts Terms and Conditions. 2. RADIUS This mode when selected, user has to provide username and password, which is then redirected to RADIUS server for authentication. If successful, user is provided with data access.	–	Clickthrough

Parameters	Description	Range	Default
	3. LDAP This mode when selected, user has to provide username and password, which is then redirected to LDAP server for authentication. If successful, user is provided with 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.		
Redirect Mode	This option helps the user to configure the HTTP or HTTPS mode of redirection URL. 1. HTTP AP sends a HTTP POSTURL to the associated client, which will be http://<Pre-defined-URL>. 2. HTTPS AP sends HTTPS POSTURL to the successful associated client, which will be https://<Pre-defined-URL>.	–	HTTP
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.	–	–
Title	User can configure a Title to the splash page. Configured text in this parameter will be displayed in the redirection page. This text is usually Bold.	Up to 255 characters	Welcome To Cambium Powered Hotspot
Contents	User can configure the contents of Splash page using this field. Displays the text configured under the Title section of redirection page.	Up to 255 characters	Please enter username and password to get Web Access
Terms	Splash page displays the text configured when user accepts Terms and Agreement.	Up to 255 characters	–
Logo	Displays the logo image updated in URL http(s)://<ipaddress>/logo.png. Either PNG or JPEG format of logo are supported.	–	–

Parameters	Description	Range	Default
Background Image	Displays the background image updated in URL http(s)://<ipaddress>/backgroundimage.png. Either PNG or JPEG format of logo are supported.	–	–
Success Action	Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL: 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 configured on device in Redirection URL 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.	–	Internal Logout page
Redirect user to External 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: ○ SSID ○ AP MAC ○ NAS ID ○ AP IP ○ Client MAC ○ Redirection URL ○ User can provide either HTTP or HTTPS URL	–	–
Redirection user to Original URL	Users will be redirected to URL that is accessed by user before successful captive portal authentication. There is additional parameter Prefix Query Strings in Redirection 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
	○ SSID ○ AP MAC ○ NAS ID ○ AP IP ○ Client MAC		
Success message	Provision to configure text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	–	–
Redirect	• If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	–	Enabled
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.	–	1.1.1.1
Proxy Redirection Port	Proxy port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.	1 - 65535	–
Session Timeout	This is the duration of time, client will be allowed to access internet if quota persists, after which AP sends de-authentication. Wireless station has to undergo Guest Access authentication after session timeout.	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
MAC Authentication Fallback	It's a mechanism in which wireless stations will be redirected to Guest Access login page after any supported type of MAC address authentication fails.	–	Disabled
Extend Interface	Provision to support Guest Access on Ethernet interface.	–	Disabled
Whitelist	Provision to configure either IPs or URLs to bypass traffic, therefor user can access those IPs or URLs without Guest Access authentication.	–	–

Parameters	Description	Range	Default
Captive Portal bypass User 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:

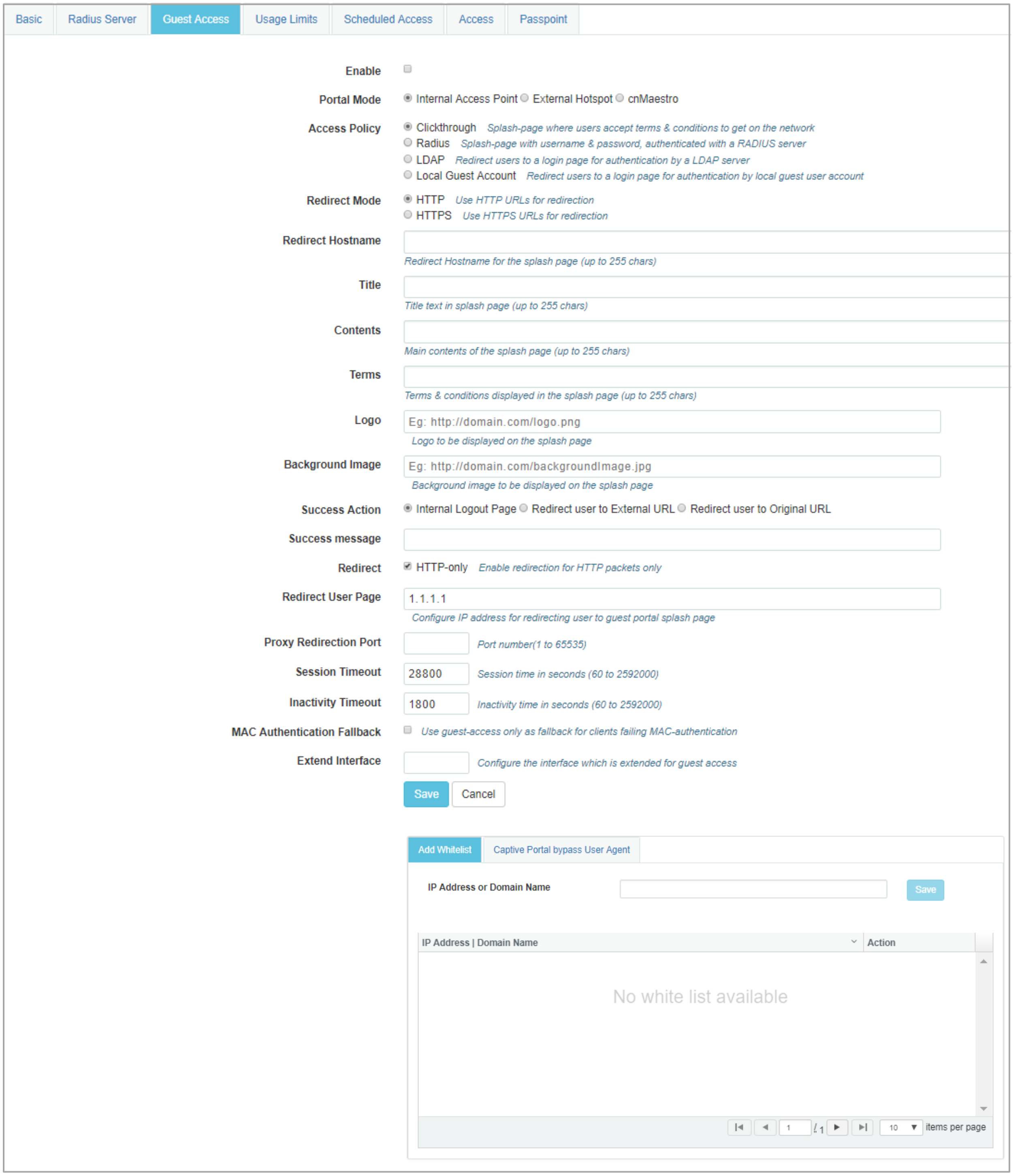
1. Enter the IP address or the domain name of the permitted domain in the IP Address or Domain Name textbox.
2. Click Save.

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.

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



Enable □

Portal Mode ● 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*
○ 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*

Redirect Mode
● HTTP *Use HTTP URLs for redirection*
○ HTTPS *Use HTTPS URLs for redirection*

Redirect Hostname
Redirect Hostname for the splash page (up to 255 chars)

Title
Title text in splash page (up to 255 chars)

Contents
Main contents of the splash page (up to 255 chars)

Terms
Terms & conditions displayed in the splash page (up to 255 chars)

Logo Eg: http://domain.com/logo.png
Logo to be displayed on the splash page

Background Image Eg: 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 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*

IP Address or Domain Name

IP Address | Domain Name	Action
No white list available	

1 / 1 10 items per page

Table 20 Configure: WLAN > Guest Access > External Hotspot parameters

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

Parameters	Description	Range	Default
	AP sends HTTPS POSTURL to the successful associated client, which will be https://<Pre-defined-URL>.		
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.	–	–
WISPr Clients External Server Login	Provision to enable re-direction of guest access portal URL obtained through WISPr.	–	Disabled
External Page URL	User can configure landing/login page which is posted to wireless stations that are not Guest Access authenticated.	–	–
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.	–	Disabled
External Portal Type	Two modes of portal types are supported by cnPilot products. 1. Standard This mode is selected, for all third-party vendors whose Guest Access services is certified and integrated with cnPilot products. 2. XWF This mode is selected for Facebook Express Wi-Fi deployment.	–	Standard
XWF Key	This is applicable when XWF portal mode is selected.	–	–
XWF Authentication API URL	This is applicable when XWF portal mode is selected. Provision to configure XWF Authentication API URL.	–	–
XWF Accounting API URL	This is applicable when XWF portal mode is selected. Provision to configure XWF Accounting API URL.	–	–
XWF Dynamic Authentication API URL	This is applicable when XWF portal mode is selected. Provision to configure XWF Dynamic Authentication API URL.	–	–

Parameters	Description	Range	Default
XWF SSE Server API URL	This is applicable when XWF portal mode is selected. Provision to configure XWF SSE Server API URL.	–	–
XWF SSE Server Timeout	This is applicable when XWF portal mode is selected. Provision to configure XWF SSE Server Timeout.	5-1800	60
Success Action	Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL: 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 configured on device in Redirection URL 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.	–	Internal Logout Page
Redirect user to External 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 o NAS ID o AP IP o Client MAC o Redirection URL User can provide either HTTP or HTTPS URL.	–	–
Redirection user to Original URL	Users will be redirected to URL that is accessed by user before successful captive portal authentication. There is additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below:	–	–

Parameters	Description	Range	Default
	• Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: ○ SSID ○ AP MAC ○ NAS ID ○ AP IP ○ Client MAC		
Success message	Provision to configure text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	–	–
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	–	Disabled
Redirect	• If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	–	Enabled
Redirect User Page	IP address configured in this field is used as logout/disconnect/redirect to captive portal URL for Guest Access sessions. IP address configured should not be reachable to internet.	–	1.1.1.1
Proxy Redirection Port	Proxy port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.	1 - 65535	–
Session Timeout	This is the duration of time, client will be allowed to access internet if quota persists, after which AP sends de-authentication. Wireless station has to undergo Guest Access authentication after session timeout.	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800

Parameters	Description	Range	Default
MAC Authentication Fallback	It's a mechanism in which wireless stations will be redirected to Guest Access login page after any supported type of MAC address authentication failures.	–	Disabled
Extend 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.	–	–
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication. This parameter is valid for standard portal type.	–	–
Captive Portal bypass User Agent	Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers. This is 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.

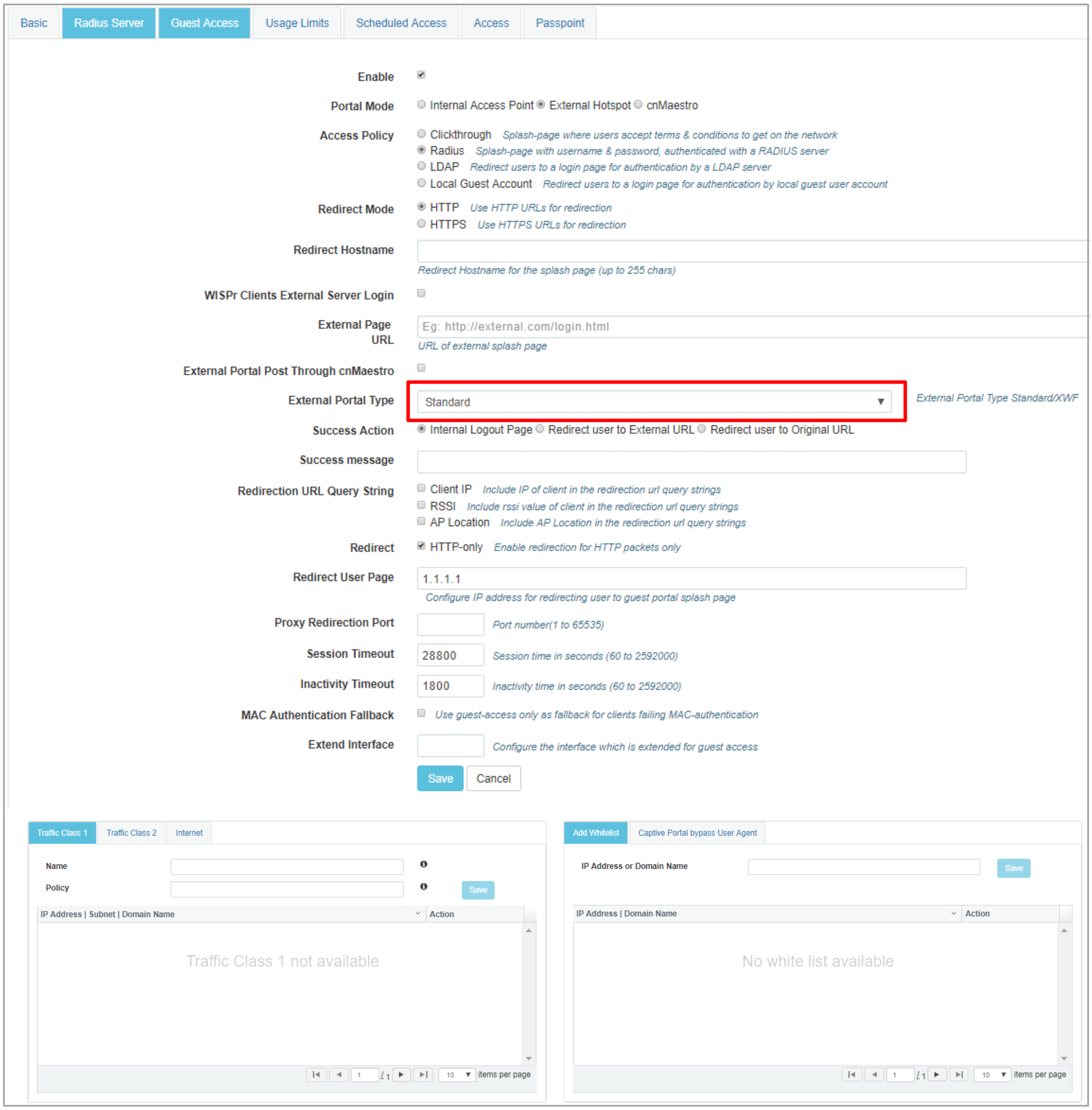
To configure Whitelist:

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:

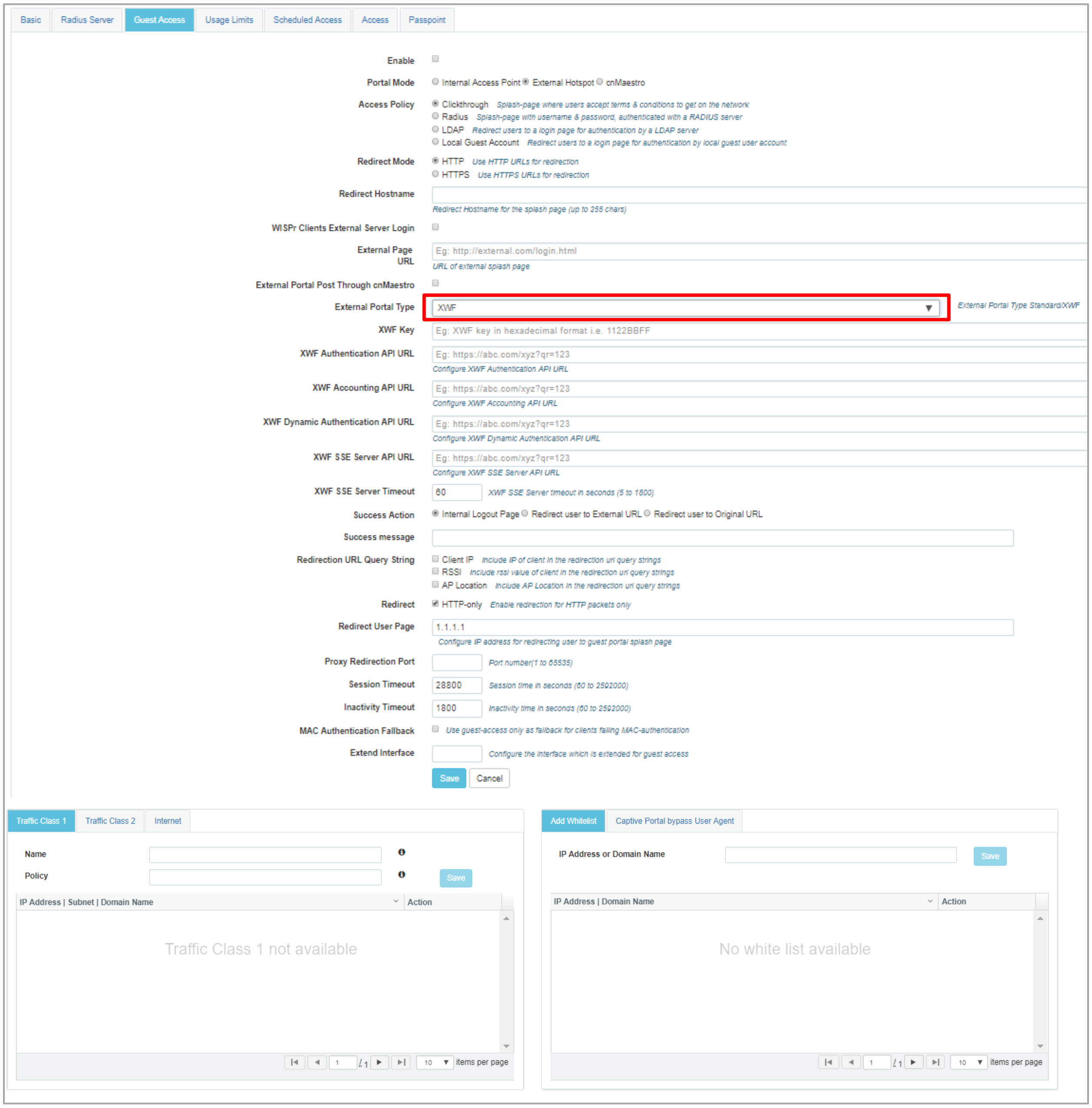
1. Select Index parameter value from the drop-down list.
2. Enter User Agent String parameter in the textbox.
3. Select Status Code from the drop-down list.
4. Enter HTML Response in the textbox.
5. Click Save.

Figure 27 Configure: WLAN > Guest Access > External Hotspot (Standard) parameter



Enable	☑
Portal Mode	○ 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* ○ 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*
Redirect Mode	● HTTP *Use HTTP URLs for redirection* ○ HTTPS *Use HTTPS URLs for redirection*
Redirect Hostname	*Redirect Hostname for the splash page (up to 255 chars)*
WISPr Clients External Server Login	□
External Page URL	Eg: http://external.com/login.html *URL of external splash page*
External Portal Post Through cnMaestro	□
External Portal Type	Standard ▼ *External Portal Type Standard/XWF*
Success Action	● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL
Success message	
Redirection URL Query String	□ Client IP *Include IP of client in the redirection url query strings* □ RSSI *Include rssi value of client in the redirection url query strings* □ AP Location *Include AP Location in the redirection url query strings*
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	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*

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



Enable □

Portal Mode ○ 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*
○ 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*

Redirect Mode
● HTTP *Use HTTP URLs for redirection*
○ HTTPS *Use HTTPS URLs for redirection*

Redirect Hostname
Redirect Hostname for the splash page (up to 255 chars)

WISPr Clients External Server Login □

External Page URL Eg: http://external.com/login.html
URL of external splash page

External Portal Post Through cnMaestro □

External Portal Type XWF ▼ *External Portal Type Standard/XWF*

XWF Key Eg: XWF key in hexadecimal format i.e. 1122BBFF

XWF Authentication API URL Eg: https://abc.com/xyz?qr=123
Configure XWF Authentication API URL

XWF Accounting API URL Eg: https://abc.com/xyz?qr=123
Configure XWF Accounting API URL

XWF Dynamic Authentication API URL Eg: https://abc.com/xyz?qr=123
Configure XWF Dynamic Authentication API URL

XWF SSE Server API URL Eg: https://abc.com/xyz?qr=123
Configure XWF SSE Server API URL

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

Redirection URL Query String
□ Client IP *Include IP of client in the redirection url query strings*
□ RSSI *Include rssi value of client in the redirection url query strings*
□ AP Location *Include AP Location in the redirection url query strings*

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 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

Name

Policy

Save

IP Address | Subnet | Domain Name	Action
Traffic Class 1 not available	

IP Address or Domain Name

Save

IP Address | Domain Name	Action
No white list available	

Table 21 Configure: WLAN > Guest Access > cnMaestro parameters

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	–	–

Parameters	Description	Range	Default
Redirect	• If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	–	Enabled
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.	–	1.1.1.1
Proxy Redirection Port	Proxy port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.	1 - 65535	–
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
MAC Authentication Fallback	It's a mechanism in which wireless stations will be redirected to Guest Access login page after any supported type of MAC address authentication fails.	–	Disabled
Extend Interface	Provision to support Guest Access on Ethernet interface.	–	Disabled
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that 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.	–	–

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.

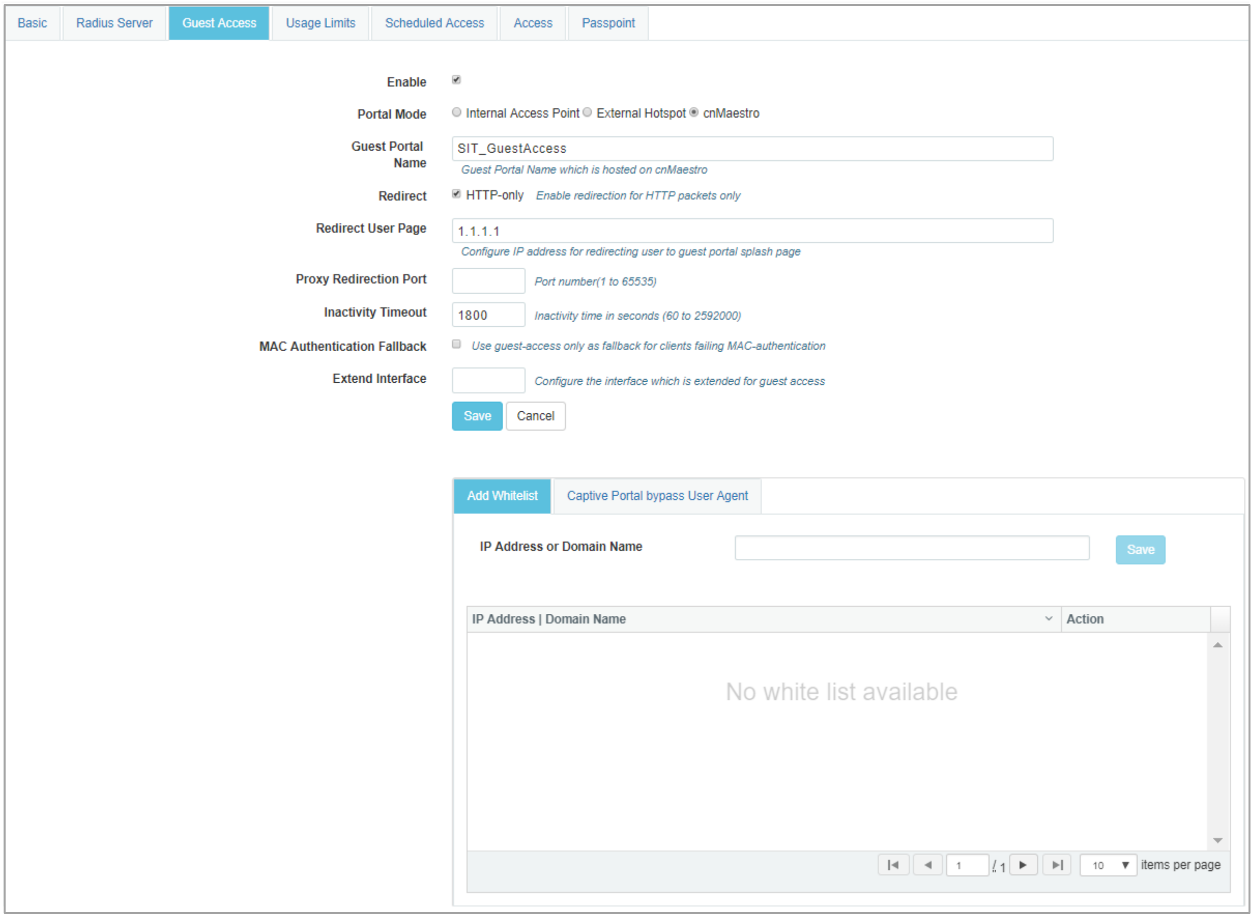
To configure the Whitelist parameter:

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



Enable ☑

Portal Mode ○ Internal Access Point ○ External Hotspot ● cnMaestro

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 page

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-authentication

Extend Interface: Configure the interface which is extended for guest access

No white list available

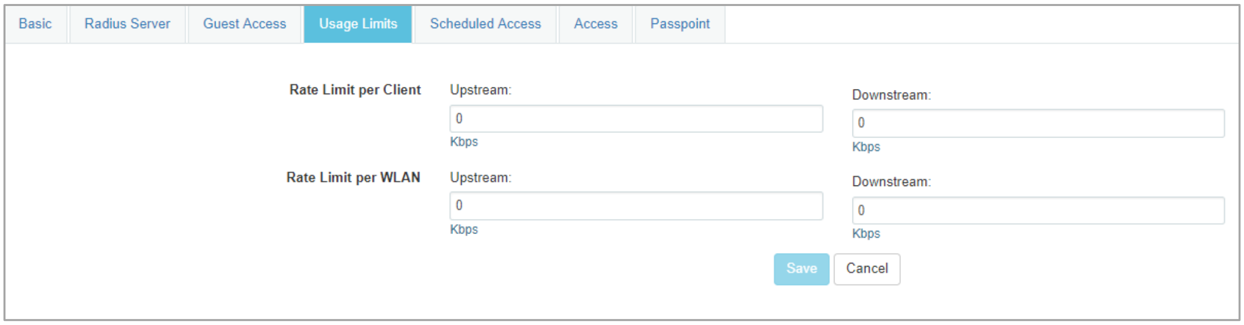
Table 22 Configure: WLAN > Usage Limits parameters

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

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.

Figure 30 Configure: WLAN > Usage Limits parameters



Rate Limit per Client
Upstream: 0 Kbps
Downstream: 0 Kbps

Rate Limit per WLAN
Upstream: 0 Kbps
Downstream: 0 Kbps

Table 23 Configure: WLAN > Scheduled Access parameters

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

Figure 31 Configure: WLAN > Scheduled Access parameters

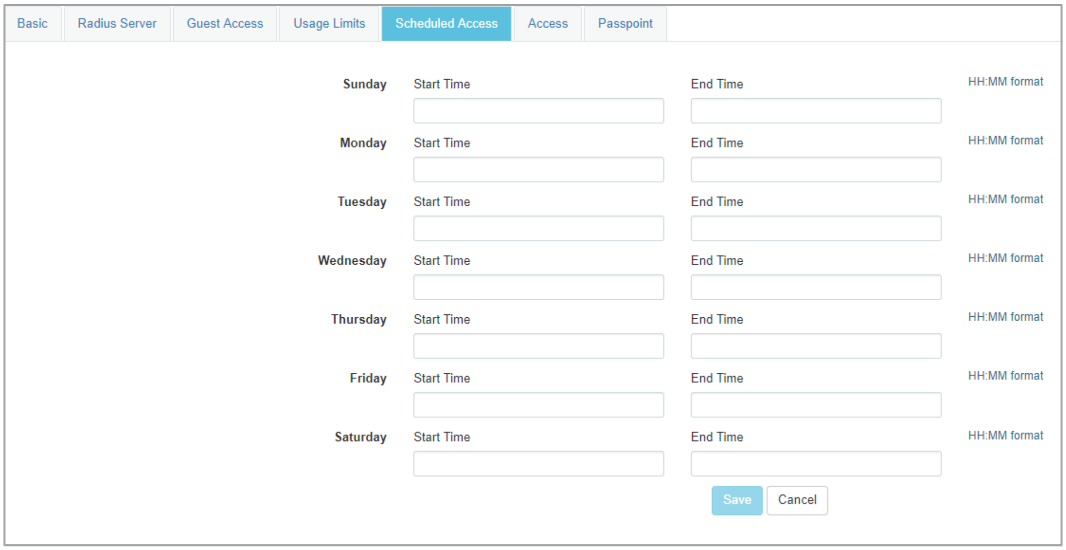


Table 24 Configure: WLAN > Access parameters

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 or deny traffic.	Allow/deny	Deny
Direction	Provision to apply the ACLs rules configured either in any direction or specific direction.	–	–

Parameters	Description	Range	Default
Type	cnPilot devices support three layers of ACLs. A rule can be configured as below: • MAC • IP • Proto	–	IP
Source IP/Mask	This option is available when ACL type is configured to an IP address. This field helps user to configure if rule needs to be applied for a single IP address or range of IP addresses.	–	–
Destination IP/Mask	This option is available when ACL type is configured to an IP address. This field helps user to configure if rule needs to be applied for a single IP address or range of IP addresses.	–	–
Source MAC/Mask	This option is available when ACL type is configured to a MAC address. This field helps user to configure if rule needs to be applied for a single device MAC address or range of MAC addresses.	–	–
Destination MAC/Mask	This option is available when ACL type is configured to MAC address. This field helps user to configure if rule needs to be applied for a single device MAC address or range of MAC addresses.	–	–
Protocol	This option is available when user selects ACL type as proto. User can select following protocols: • TCP • UDP • ICMP • Any	–	TCP
Source Port	Provision to apply ACL with combination of protocol and port.	–	–
Destination 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.	–	–
DNS-ACL			

Parameters	Description	Range	Default
Precedence	Provision to configure index of ACL rule. Packets are validated and processed based on Precedence 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 Authentication			
MAC Authentication Policy	cnPilot supports multiple methods of MAC authentication. Following are details of each mode: 1. Permit Wireless station MAC addresses listed will be allowed to associate to AP. 2. Deny When user configures a MAC address, those wireless station shall be denied to associate and the non-listed MAC address will be allowed. 3. Radius For every wireless authentication, cnPilot sends a radius request and if radius accept is received, then wireless station is allowed to associate. 4. cnMaestro This option is preferable when administrator prefers centralized MAC authentication policy. For every wireless authentication, AP sends query to cnMaestro if it allowed or disallowed to connect. Based on the configuration, wireless stations are either allowed or denied.	–	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.

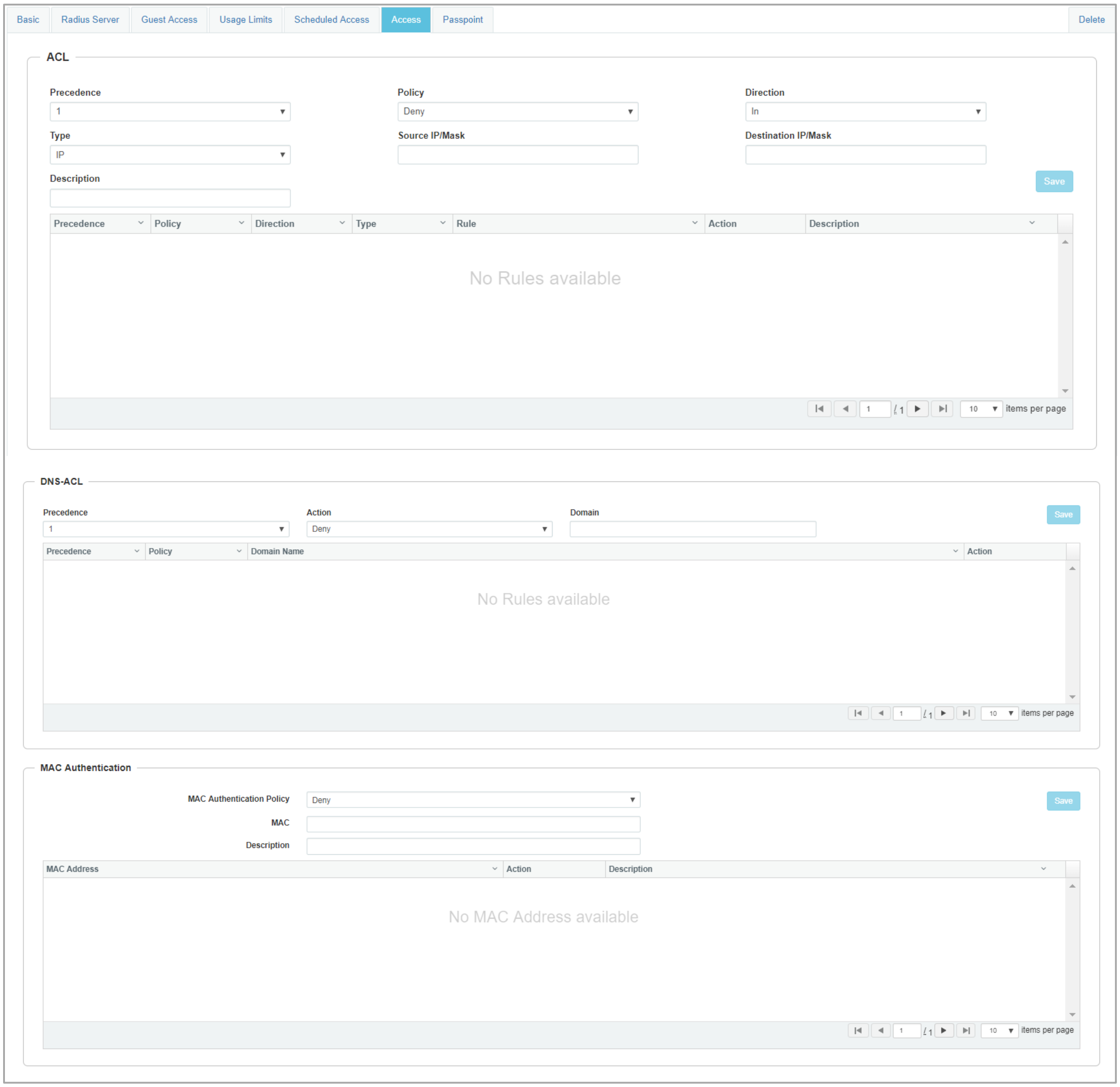
To configure DNS ACL:

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.

Figure 32 Configure: WLAN > Access parameters



ACL

Precedence: 1
Policy: Deny
Direction: In
Type: IP
Source IP/Mask:
Destination IP/Mask:
Description:

Precedence	Policy	Direction	Type	Rule	Action	Description

No Rules available

DNS-ACL

Precedence: 1
Action: Deny
Domain:

Precedence	Policy	Domain Name	Action

No Rules available

MAC Authentication

MAC Authentication Policy: Deny
MAC:
Description:

MAC Address	Action	Description

No MAC Address available

Table 25 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

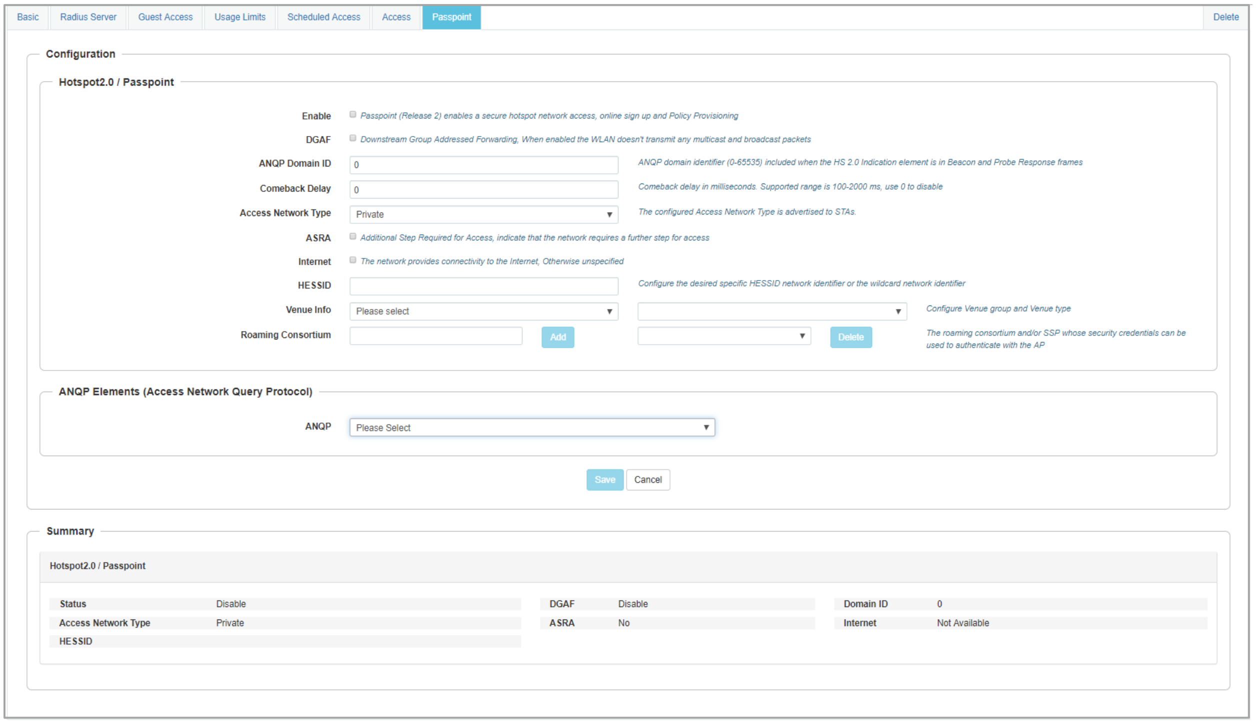
Parameters	Description	Range	Default
DGAF	Downstream Group Addressed Forwarding, when enabled the WLAN doesn't transmit any multicast and broadcast packets.	–	Disabled
ANQP Domain ID	ANQP domain identifier included when the HS 2.0 indication element is in Beacon and Probe Response frames.	0-65535	0
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with Guest • Test • Wildcard	–	Private
ASRA	Indicates that the network requires a further step for 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 Consortium	The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.	–	–
ANQP Elements	Select any one of the following: • 3GPP Cellular Network Information • Connection Capability • Domain Name List • Icons	–	–

Parameters	Description	Range	Default
	• IP Address Type information • 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.

Figure 33 Configure: WLAN > Passpoint parameters



Configuration

Hotspot2.0 / Passpoint

Enable □ *Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning*

DGAF □ *Downstream Group Addressed Forwarding, When enabled the WLAN doesn't transmit any multicast and broadcast packets*

ANQP Domain ID: 0 — *ANQP domain identifier (0-65535) included when the HS 2.0 Indication element is in Beacon and Probe Response frames*

Comeback Delay: 0 — *Comeback delay in milliseconds. Supported range is 100-2000 ms, use 0 to disable*

Access Network Type: Private — *The configured Access Network Type is advertised to STAs.*

ASRA □ *Additional Step Required for Access, indicate that the network requires a further step for access*

Internet □ *The network provides connectivity to the Internet, Otherwise unspecified*

HESSID: — *Configure the desired specific HESSID network identifier or the wildcard network identifier*

Venue Info: Please select — *Configure Venue group and Venue type*

Roaming Consortium: — *The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP*

ANQP Elements (Access Network Query Protocol)

ANQP: Please Select

Summary

Hotspot2.0 / Passpoint

Status	Disable	**DGAF**	Disable	**Domain ID**	0
Access Network Type	Private	**ASRA**	No	**Internet**	Not Available
HESSID					

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

Table 26 Configure: Network > VLAN parameters

Parameters	Description	Range	Default
VLAN			
Edit	Provision to select the VLAN interface that user is intended to view/update configuration.	–	VLAN 1
IP Address	Provision to configure mode of IP address configuration for an interface selected. Two modes are supported: 1. DHCP This is the default mode in which cnPilot device tries to obtain IP address from DHCP server. 2. Static User has to explicitly configure IP address and Netmask for a VLAN selected.	–	DHCP

Parameters	Description	Range	Default
NAT	This option is preferable when you defined local DHCP servers. This option when selected, traffic from wireless stations are NAT'ed to the default gateway interface IP.		Disabled
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only on VLAN1 configuration section. If VLAN 1 is not allowed in Ethernet interfaces, this IP will not be accessible.	–	Enabled
Management Access	Provision to restrict the access of device either using CLI or UI and to restrict SNMP access. User can configure restriction of device access as follows: • Block • Allow from Wired • Allow from both wired and wireless	–	Allow from both Wired and Wireless
DHCP Relay 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: 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	–	Disabled
Request Option All	This configuration decides the interface on which cnPilot AP will learn the following:	–	Enabled on VLAN1

Parameters	Description	Range	Default
	• IP default gateway • DHCP client options like Option 43 (Controller discovery like controller host name / IP address) • DNS Servers • Domain Name		
Routing & DNS			
Default Gateway	Provision to configure default gateway. If this is provided, cnPilot device installs this gateway as this is the highest priority.	–	–
Domain Name	Provision to configure Domain Name. If this is provided, cnPilot device installs this Domain Name as this is highest priority.	–	–
DNS Server	Provision to configure Static DNS server on cnPilot device. Maximum of two DNS servers can be configured.	–	–
DNS Proxy	cnPilot device can acts as DNS proxy server when this parameter is enabled.	–	Disabled

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

To configure VLAN:

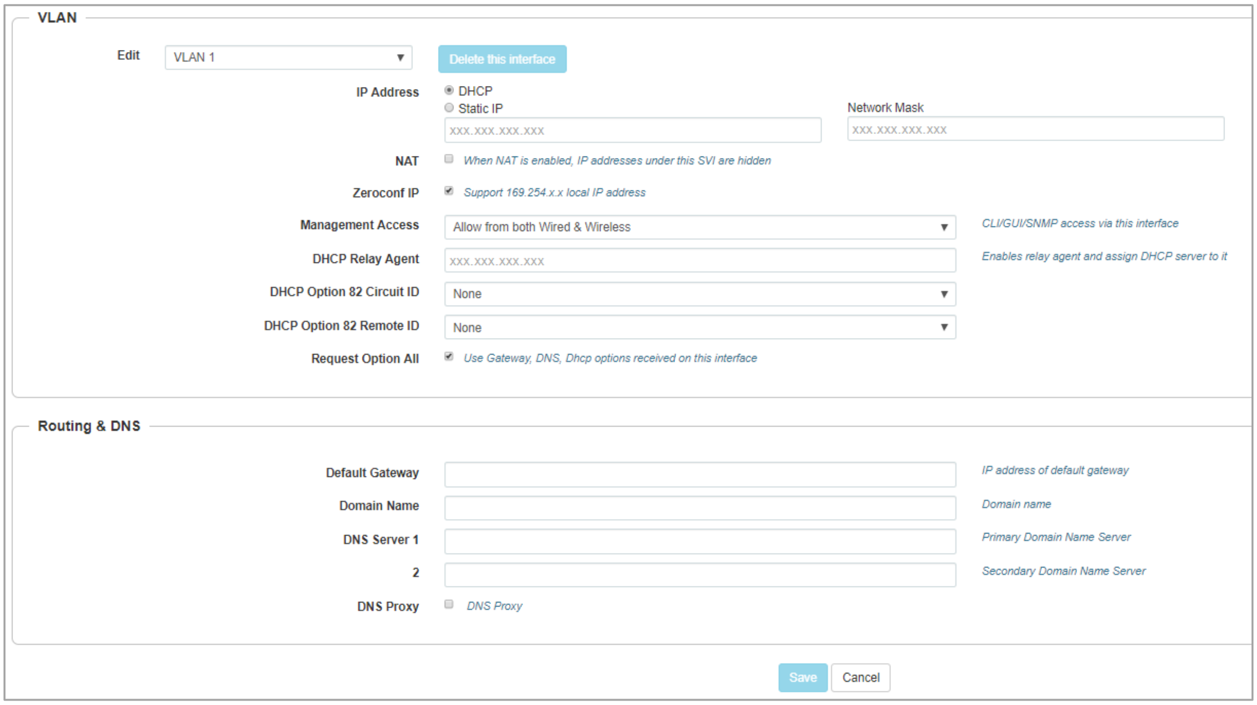
1. Select Edit checkbox to enable VLAN1 functionality.
2. Enable DHCP or Static IP mode of IP address configuration from the IP Address checkbox.
3. Enable NAT checkbox.
4. Enable Zeroconf IP checkbox.
5. Select Management Access to configure restriction of device from the drop-down list.
6. Enter DHCP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

To configure Routing & DNS:

1. Enter Default Gateway IP 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 34 Configure: Network > VLAN parameters



VLAN

Edit: VLAN 1 ▾ [Delete this interface]

IP Address: ● DHCP ○ Static IP xxx.xxx.xxx.xxx; Network Mask xxx.xxx.xxx.xxx

NAT: □ *When NAT is enabled, IP addresses under this SVI are hidden*

Zeroconf IP: ☑ *Support 169.254.x.x local IP address*

Management Access: Allow from both Wired & Wireless ▾ *CLI/GUI/SNMP access via this interface*

DHCP Relay Agent: xxx.xxx.xxx.xxx *Enables relay agent and assign DHCP server to it*

DHCP Option 82 Circuit ID: None ▾

DHCP Option 82 Remote ID: None ▾

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] [Cancel]

Table 27 Configure: Network > Routes parameters

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

Parameters	Description	Range	Default
	• IP Address • Type		

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 IP address in the textbox.
3. Enter Gateway IP 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.

Figure 35 Configure: Network > Routes parameters

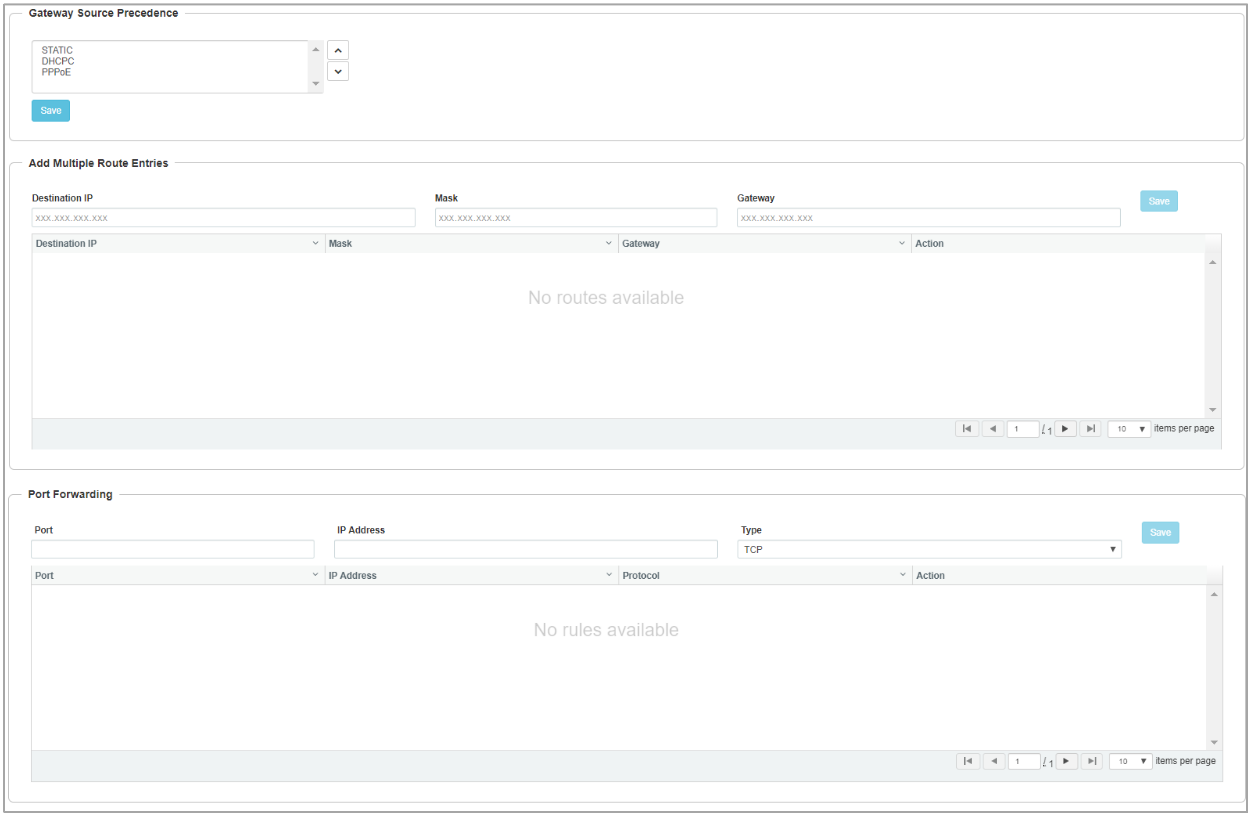


Table 28 Configure: Network > Ethernet Ports parameters

Parameters	Description	Range	Default
Ethernet	cnPilot devices Ethernet port is provisioned to operate in following modes: 1. Access Single VLAN Single VLAN traffic is allowed in this mode. 2. Trunk Multiple VLANs Multiple VLANs are supported in this mode.	–	Access
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 or deny traffic.	Allow/ deny	Deny

Parameters	Description	Range	Default
Direction	Provision to apply the ACLs rules configured either in any direction or specific direction.	–	–
Type	cnPilot devices support three layers of ACLs. A rule can be configured as below: • IP • MAC • Proto	–	IP
Source IP/Mask	This option is available when ACL type is configured to an IP address. This field helps user to configure if rule needs to be applied for a single IP address or range of IP addresses.	–	–
Destination IP/Mask	This option is available when ACL type is configured to an IP address. This field helps user to configure if rule needs to be applied for a single IP address or range of IP addresses.	–	–
Source MAC/Mask	This option is available when ACL type is configured to a MAC address. This field helps user to configure if rule needs to be applied for a single device MAC address or range of MAC addresses.	–	–
Destination MAC/Mask	This option is available when ACL type is configured to MAC address. This field helps user to configure if rule needs to be applied for a single device MAC address or range of MAC addresses.	–	–
Protocol	This option is available when user selects ACL type as proto. User can select following protocols: • TCP • UDP • ICMP • Any	–	TCP
Source Port	Provision to apply ACL with combination of protocol and port.	–	–
Destination 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.	–	–

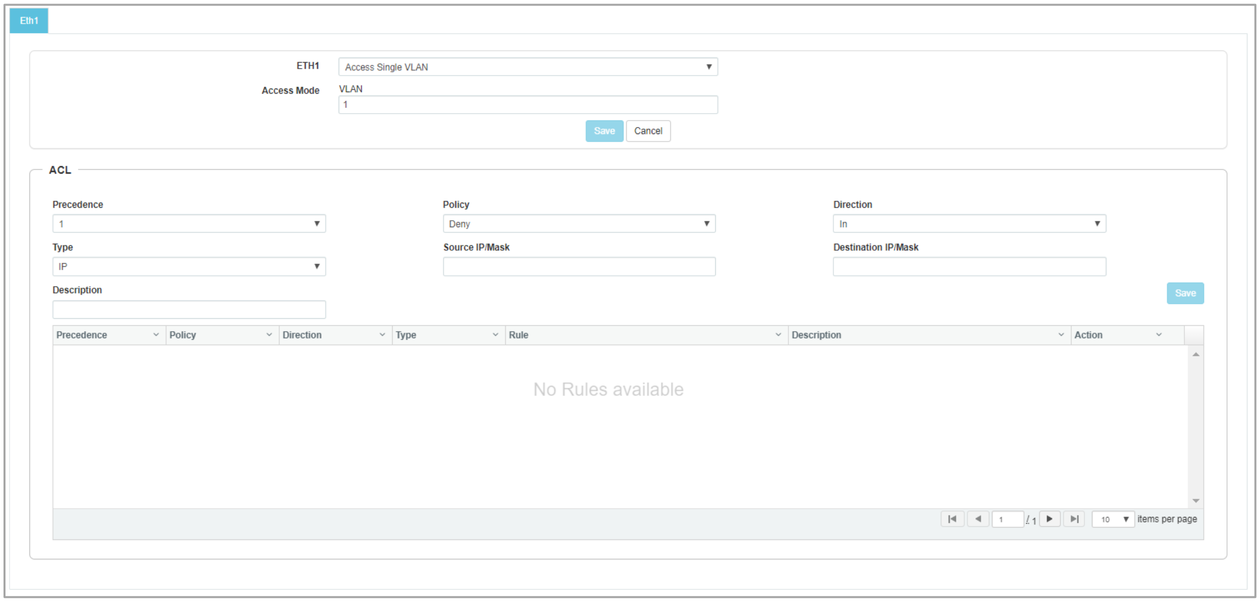
To configure the above parameter, navigate to the Configure > Network > Ethernet Ports tab and provide the details as given below:

1. Select Access Single VLAN or Trunk Multiple VLANs from the ETH1 drop-down list.
2. Enter Access Mode in the textbox.
3. 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.

Figure 36 Configure: Network > Ethernet Ports parameters



ETH1: Access Single VLAN

Access Mode: VLAN 1

Precedence: 1

Policy: Deny

Direction: In

Type: IP

Source IP/Mask

Destination IP/Mask

Description

Precedence	Policy	Direction	Type	Rule	Description	Action
No Rules available						

1 / 1 10 items per page

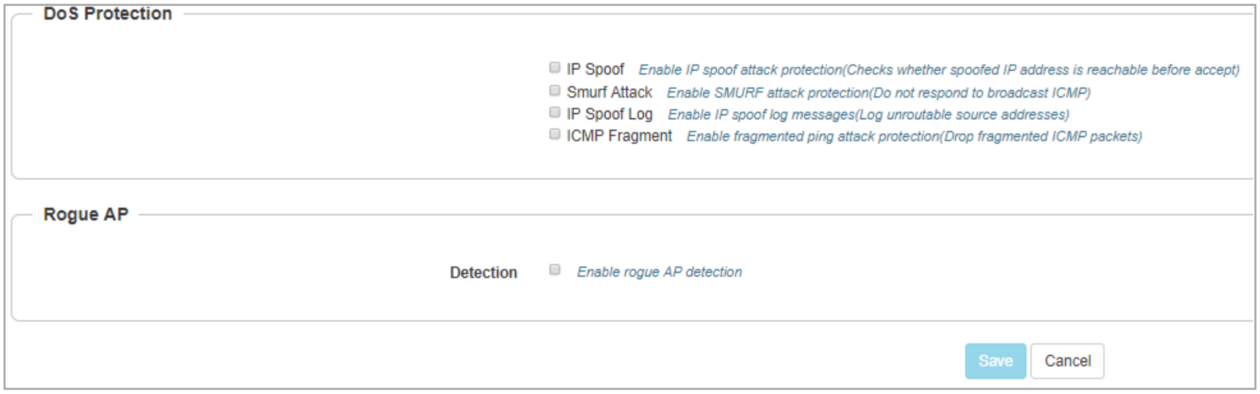
Table 29 Configure: Network > Security parameters

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

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.

Figure 37 Configure: Network > Security parameters



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)*

Rogue AP

Detection □ *Enable rogue AP detection*

Table 30 Configure: Network > DHCP parameters

Parameters	Description	Range	Default
Edit	Provision to select DHCP Pool if multiple Pools are defined on cnPilot device.	–	–
Address 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 IP from the address pool defined, so that wireless station gets same IP address every time they connect. Following parameters are required to bind IP address: • MAC Address • IP Address	–	–

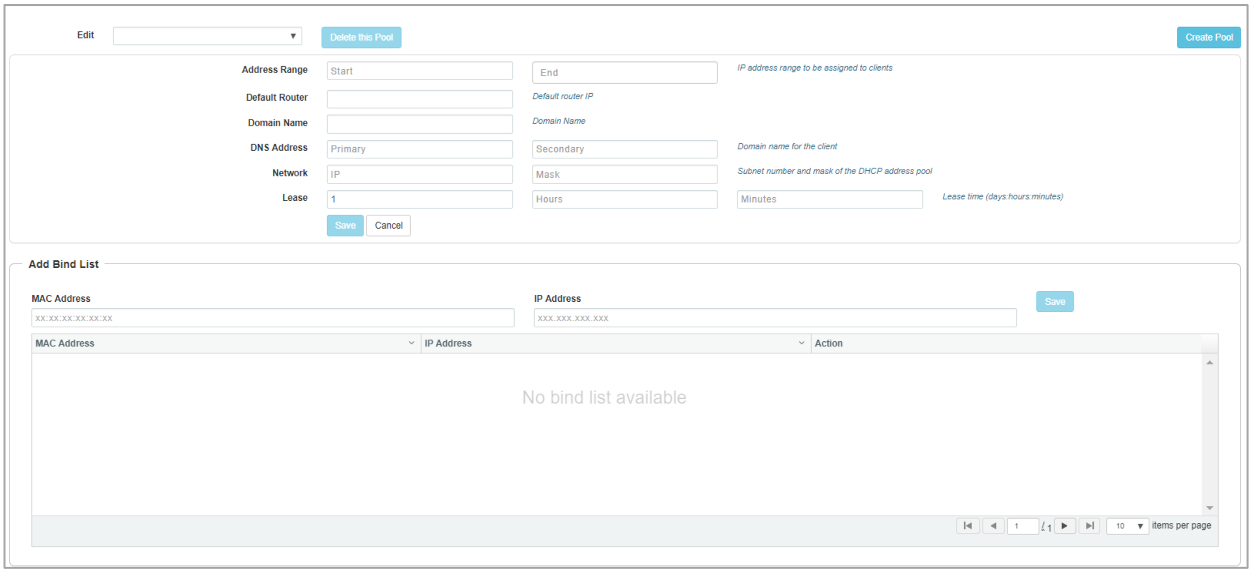
To configure the above parameter, navigate to the Configure > Network > DHCP tab and provide the details as given below:

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.

Figure 38 Configure: Network > DHCP parameters



Address Range: Start | End — IP address range to be assigned to clients

Default Router: — Default router IP

Domain Name: — Domain Name

DNS Address: Primary | Secondary — Domain name for the client

Network: IP | Mask — Subnet number and mask of the DHCP address pool

Lease: 1 | Hours | Minutes — Lease time (days:hours:minutes)

Add Bind List

MAC Address: xx:xx:xx:xx:xx:xx

IP Address: xxx.xxx.xxx.xxx

MAC Address	IP Address	Action

No bind list available

1 / 1 | 10 items per page

Table 31 Configure: Network > Tunnel parameters

Parameters	Description	Range	Default
Tunnel Encapsulation	Provision to enable tunnel type. Following tunnel types are supported by cnPilot devices: • L2TP • L2GRE	–	Disabled
L2TP			
Remote Host	Configure L2TP end point. Either IP or hostname of endpoint is supported.	–	–
Authentication Info	Provision to configure credentials required for L2TP authentication.	–	–
Auth Type	Provision to select the PPP authentication method. Following are the options available: • Auto • CHAP • MS-CHAP	–	Auto

Parameters	Description	Range	Default
	• MS-CHAP v2 • PAP		
TCP MSS	Provision to configure TCP Maximum Segment Size.	–	1400
PMTU Discovery	Provision to enable to discover PMTU in network.	–	Disabled
L2GRE			
Remote Host	Configure L2GRE end point. Either IP address or hostname of endpoint is supported.	–	–
DSCP	User can configure priority of GRE packets.	–	0
TCP MSS	Configure L2TP end point. Either IP address or hostname of endpoint is supported.	–	1410
PMTU Discovery	Provision to enable to discover PMTU in network.	–	Disabled
MTU	Maximum Transmission Unit.	–	1500

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.

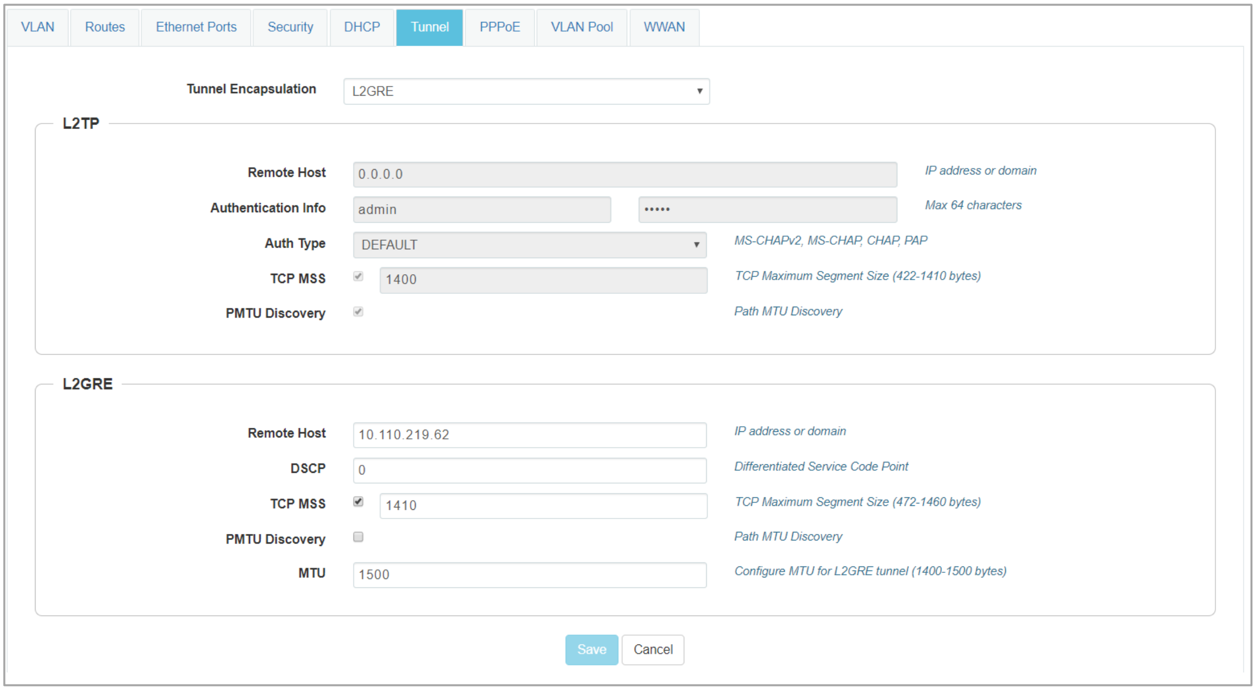
To configure L2TP:

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

To configure L2GRE:

1. Enter IP address or domain name in the Remote Host textbox.
2. Enter DSCP in the textbox.
3. Enter TCP Maximum Segment Size in the TCP MSS textbox.
4. Enable PMTU Discovery checkbox.
5. Enter Maximum Transmission Unit in the MTU textbox.
6. Click Save.

Figure 39 Configure: Network > Tunnel parameters



Tunnel Encapsulation: L2GRE

L2TP

Remote Host	0.0.0.0	IP address or domain
Authentication Info	admin / •••••	Max 64 characters
Auth Type	DEFAULT	MS-CHAPv2, MS-CHAP, CHAP, PAP
TCP MSS	☑ 1400	TCP Maximum Segment Size (422-1410 bytes)
PMTU Discovery	☑	Path MTU Discovery

L2GRE

Remote Host	10.110.219.62	IP address or domain
DSCP	0	Differentiated Service Code Point
TCP MSS	☑ 1410	TCP Maximum Segment Size (472-1460 bytes)
PMTU Discovery	☐	Path MTU Discovery
MTU	1500	Configure MTU for L2GRE tunnel (1400-1500 bytes)

Table 32 Configure: Network > PPPoE parameters

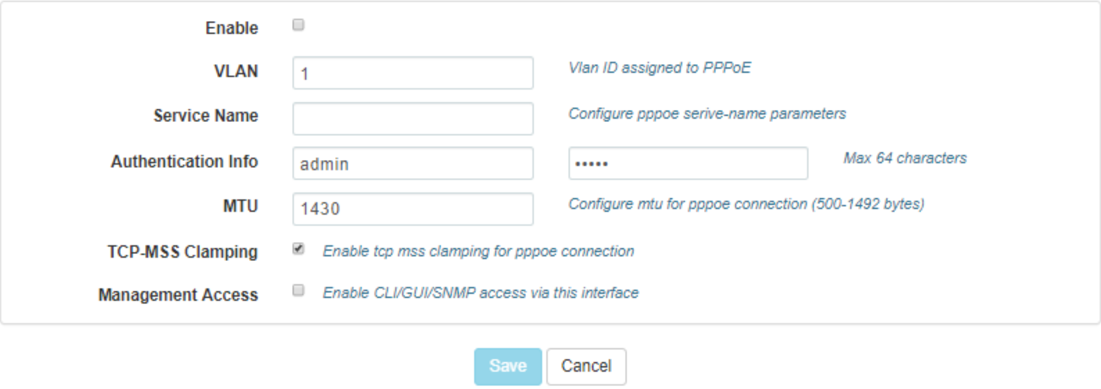
Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disable
VLAN	User can configure VLAN ID where PPPoE client should obtain IP address.	–	–
Service Name	Configure PPPoE service name	–	–
Authentication Info	Provision to configure credentials required for PPPoE authentication.	–	–
MTU	Maximum Transmission Unit.	500-1492	1430
TCP MSS Clamping	Configure PPPoE end point. Either IP or hostname of endpoint is supported.	–	Enabled
Management 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 in the TCP-MSS Clamping textbox.
7. Enable Management Access in the textbox.
8. Click Save.

Figure 40 Configure: Network > PPPoE parameters



Enable ☐

VLAN: 1 — Vlan ID assigned to PPPoE

Service Name: — Configure pppoe serive-name parameters

Authentication Info: admin ••••• — Max 64 characters

MTU: 1430 — Configure mtu for pppoe connection (500-1492 bytes)

TCP-MSS Clamping ☑ Enable tcp mss clamping for pppoe connection

Management Access ☐ Enable CLI/GUI/SNMP access via this interface

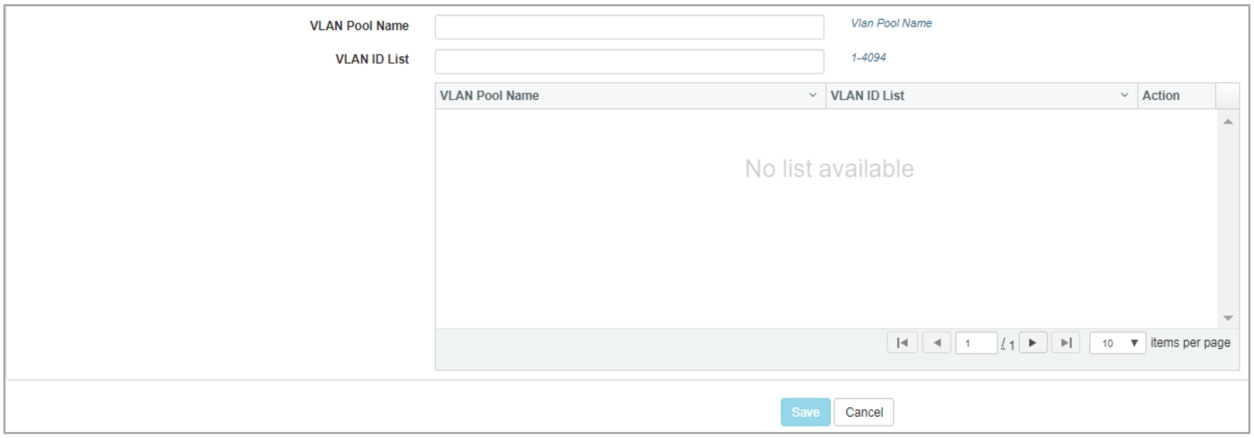
Table 33 Configure: Network > VLAN Pool parameters

Parameters	Description	Range	Default
VLAN Pool 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 configure either single VLAN ID or multiple VLAN ID. Multiple VLAN IDs can be configured either separated by 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.

Figure 41 Configure: Network > VLAN Pool parameters



VLAN Pool Name — Vlan Pool Name

VLAN ID List — 1-4094

VLAN Pool Name	VLAN ID List	Action

No list available

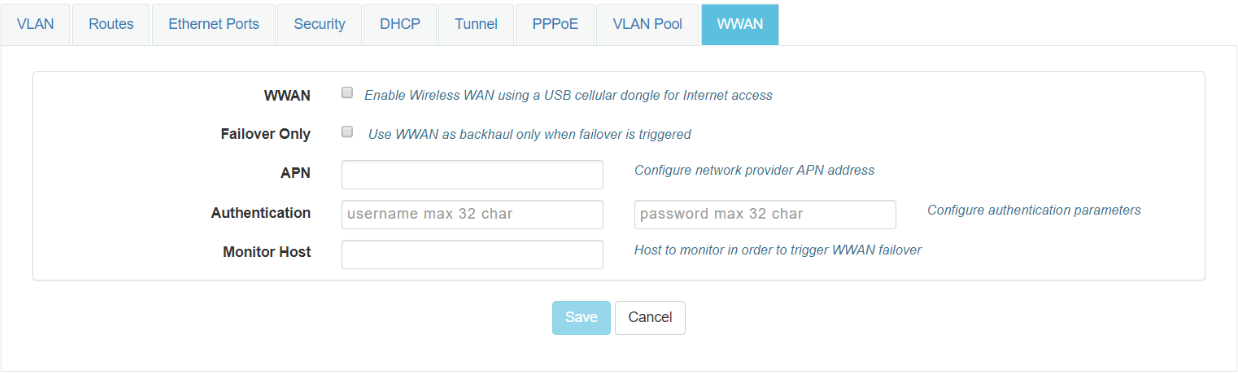
Table 34 Configure: Network > WWAN parameters

Parameters	Description	Range	Default
WWAN	Enables wireless WAN using a USB cellular dongle for Internet access.	–	Disabled
Failover Only	Enables to use WWAN as backhaul only when failover is triggered.	–	Disabled
APN	Provision to configure network provider APN address.	–	–
Authentication	Provision to configure authentication parameters.	–	–
Monitor Host	Provision to configure as server to monitor with ping to decide for internet failover.	–	–

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

1. Enable WWAN checkbox.
2. Enable Failover Only checkbox.
3. Enter APN address in the textbox.
4. Enter username and password in the Authentication textbox.
5. Enter Monitor Hoist parameter in the textbox.
6. Click Save.

Figure 42 Configure: Network > WWAN parameters



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	username max 32 char	password max 32 char	*Configure authentication parameters*
Monitor Host		*Host to monitor in order to trigger WWAN failover*	

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

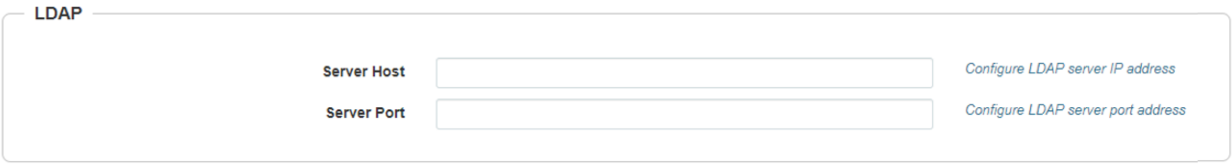
Table 35 Configure: Services > LDAP parameters

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 43 Configure: Services > LDAP parameters


LDAP
Server Host
Configure LDAP server IP address
Server Port
Configure LDAP server port address

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 36 PDU type code: 0x82

Type	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 37 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	The protocol type. The supported protocol types are: • 0x06 TCP • 0x11 UDP
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.
4 Bytes	The IP address of the visited server.
2 Bytes	The port address of the visited server.

Table 37 lists the fields that are displayed in Configuration > Services > NAT Logging tab:

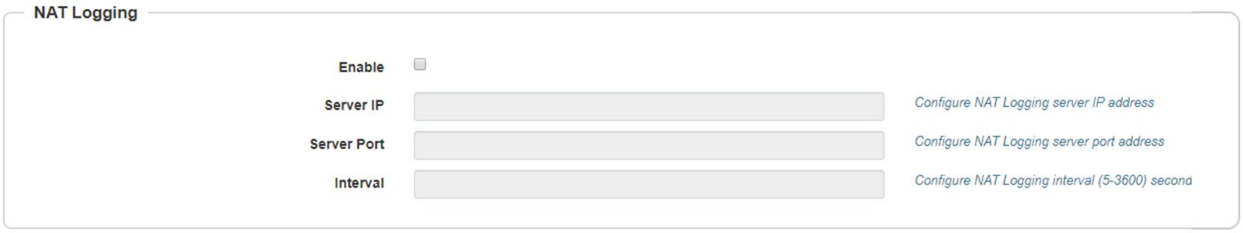
Table 38 Configure: Services > NAT Logging parameters

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 44 Configure: Services > NAT Logging parameters


NAT Logging
Enable ☐
Server IP
Configure NAT Logging server IP address
Server Port
Configure NAT Logging server port address
Interval
Configure NAT Logging interval (5-3600) second

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. Discovered client entries are deleted from the list if the entry is aged out. Age timeout is five minutes. If there are no new probe requests for the client within 5 minutes, entry is deleted.

Table 39 lists the fields that are displayed in Configuration > Services > Location API tab:

Table 39 Configure: Services > Location API parameters

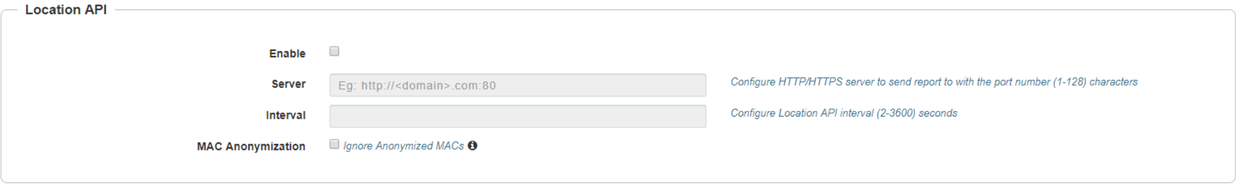
Parameters	Description	Range	Default
Enable	Provision to enable/disable Location API services.	–	–

Parameters	Description	Range	Default
Server	Provision to configure HTTP/HTTPs server to send report with the pot number.	–	–
Interval	Provision to configure custom frequency of information to be shared to server.	5-3600	–
MAC Anonymization	Provision to detect fake clients and avoid populating it in Location API client list.	–	–

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 45 Configure: Services > Location API parameters



Location API

Enable □

Server Eg: http://<domain>.com:80 Configure HTTP/HTTPS server to send report to with the port number (1-128) characters

Interval Configure Location API interval (2-3600) seconds

MAC Anonymization □ Ignore Anonymized MACs ℹ

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.

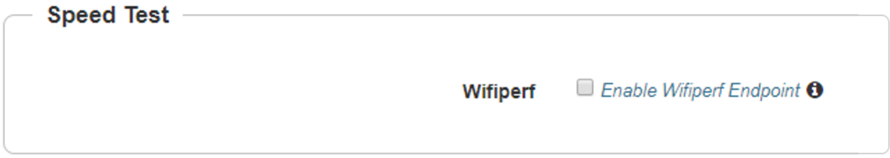
Table 40 lists the fields that are displayed in the Configuration > Services > Speed Test tab:

Table 40 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.

Figure 46 Configure: Services > Speed Test parameters



Speed Test

Wifiperf □ Enable Wifiperf 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 41 lists the fields that are displayed in the Configuration > Services > DHCP Option 82 tab:

Table 41 Configure: Services > DHCP Option 82 parameters

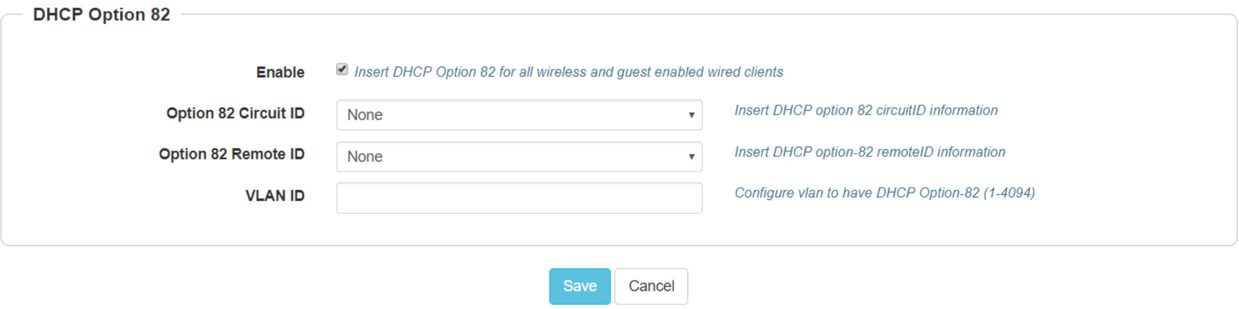
Parameters	Description	Range	Default
Enable	Provision to enable/disable DHCP Option 82 as global services.	–	–
Option 82 Circuit ID	When enabled, DHCP packets generated from wireless stations that are associated to APs are appended with Option 82 parameters. Option 82 provides provision to append Circuit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

Parameters	Description	Range	Default
	• BSSID • SSID • VLAN ID • SITEID • Custom • All		
VLAN ID	User can configure VLAN IDs where DHCP Option 82 has to be enabled.	–	–

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 drop-down list.
4. Enter VLAN ID parameter to configure VLAN to have DHCP Option 82.
5. Click Save.

Figure 47 Configure: Services > DHCP Option 82 parameters



DHCP Option 82

Enable ☑ *Insert DHCP Option 82 for all wireless and guest enabled wired clients*

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)*

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

Table 42 Configure: Operations > Firmware update parameters

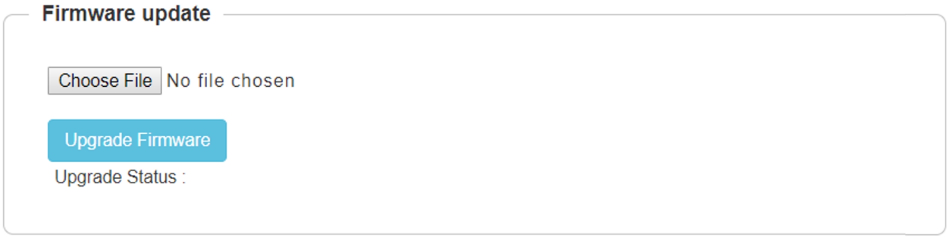
Parameters	Description	Range	Default
Choose File	Provisions to select upgrade file.	–	–
Upgrade Firmware	Provision to initiate upgrade once file is selected.	–	–

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.

Figure 48 Configure: Operations > Firmware update parameters



System

This section provides multiple troubleshooting tools provided by cnPilot Enterprises.

Table 43 lists the fields that are displayed in the Operations > System tab:

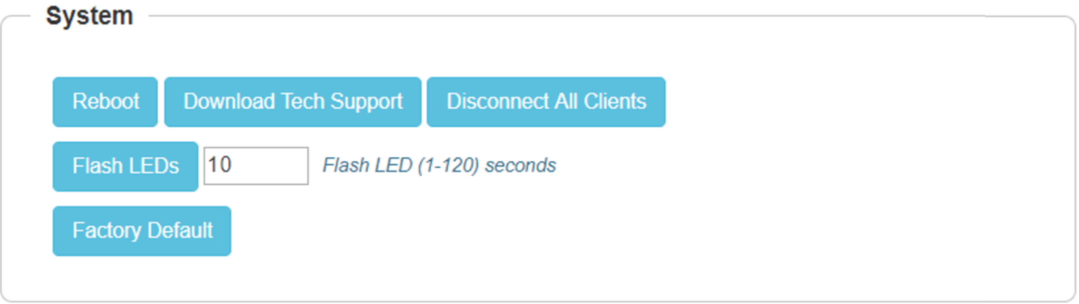
Table 43 Configure: Operations > System parameters

Parameters	Description	Range	Default
Reboot	User will be prompted with Reboot pop-up requesting for reboot. If Yes, device will go for reboot.	–	–
Download Tech Support	User will be prompted with permission to download tech-support from AP. If yes, file will be saved in your default download path configured on your system.	–	–
Disconnect All Clients	All clients connected to both the radios will be terminated by sending de-authentication packet to each client connected to radios.	–	–
Flash LEDs	LEDs on the device will toggle for configured time period.	1-120	10
Factory 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.

Figure 49 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 44 lists the fields that are displayed in the Operations > Configuration tab:

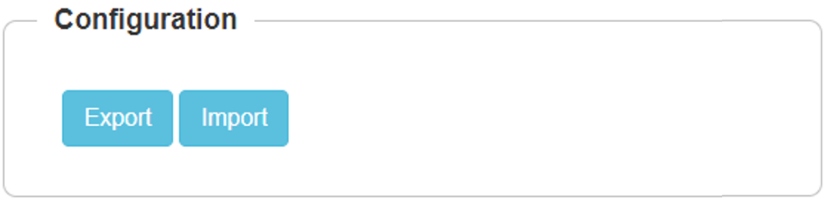
Table 44 Configure: Operations > Configuration parameters

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 50 Configure: Operations > Configuration parameters



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

Logging

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

Events

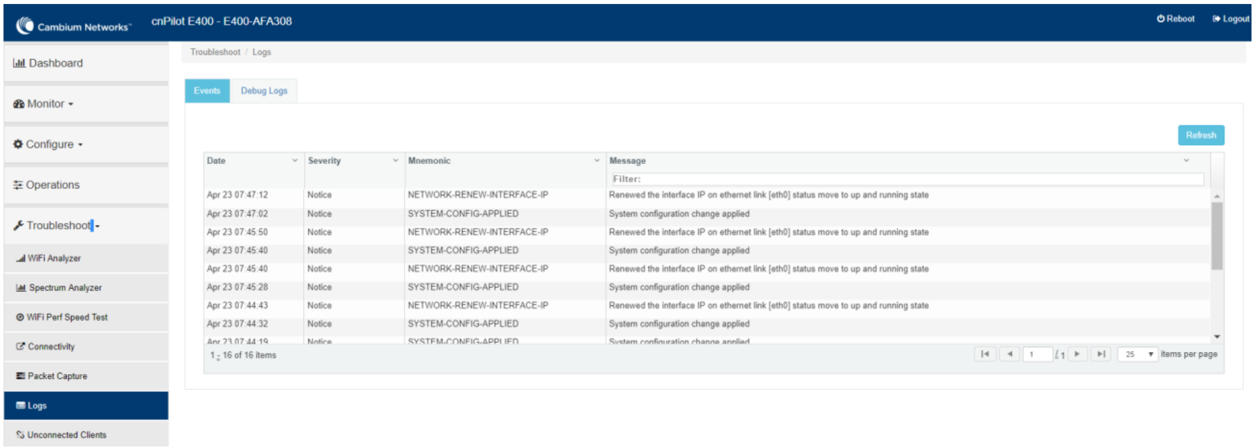
cnPilot devices generates events that are necessary for troubleshooting across various modules. Below is the list of modules, cnPilot device generates events for troubleshoot.

- Wireless station
    - Connectivity
- Configuration updates
- LDAP
    - Authentication
- RADIUS
    - Authentication
    - Accounting
    - CoA
- Mesh
- Roaming
    - Enhanced roaming
- Auto-RF

  - ○ Channel change
- Tunnel state
- Reboot
- Guest Access
- Autopilot

Events are available at Troubleshoot > Logs > Events.

Figure 51 Troubleshoot > Logs > Events



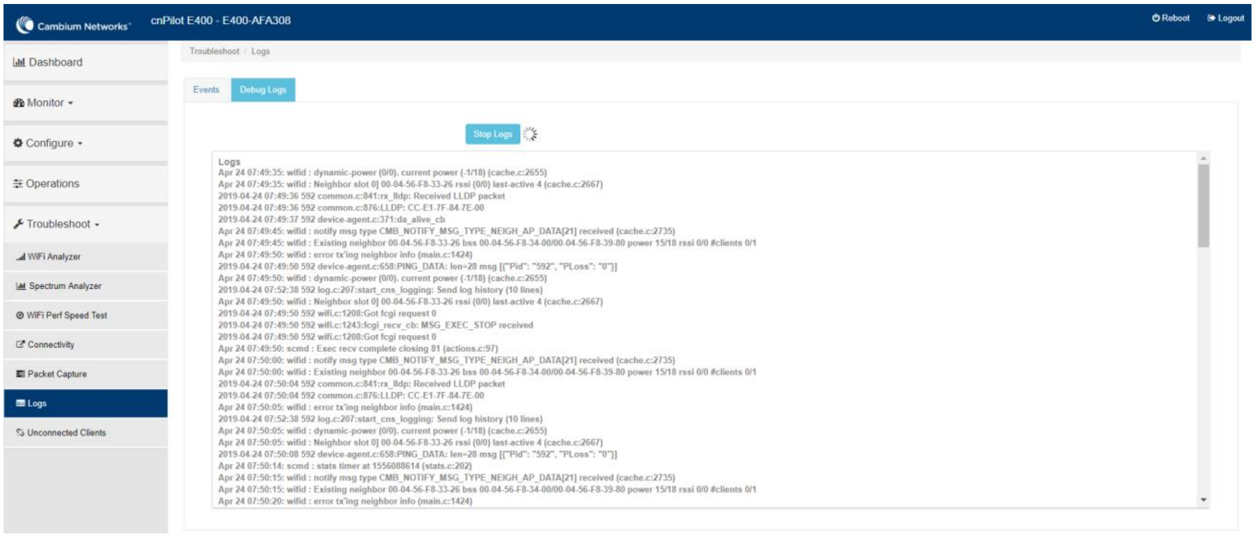
Date	Severity	Mnemonic	Message
Apr 23 07:47:12	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:47:02	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:45:50	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:45:40	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
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
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
Apr 23 07:44:32	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:44:19	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied

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 52 Troubleshoot > Logs > Debug Logs



```
Logs
Apr 24 07:49:35: wifid : dynamic-power (0/0). current power (-1/18) (cache.c:2655)
Apr 24 07:49:35: wifid : Neighbor slot 0] 00-04-56-F8-33-26 rssi (0/0) last-active 4 (cache.c:2667)
2019-04-24 07:49:36 592 common.c:841:rx_lldp: Received LLDP packet
2019-04-24 07:49:36 592 common.c:876:LLDP: CC-E1-7F-84-7E-00
2019-04-24 07:49:37 592 device-agent.c:371:da_alive_cb
Apr 24 07:49:45: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2735)
Apr 24 07:49:45: wifid : Existing neighbor 00-04-56-F8-33-26 bss 00-04-56-F8-34-00/00-04-56-F8-39-80 power 15/18 rssi 0/0 #clients 0/1
Apr 24 07:49:50: wifid : error tx'ing neighbor info (main.c:1424)
2019-04-24 07:49:50 592 device-agent.c:658:PING_DATA: len=28 msg [{"Pid": "592", "PLoss": "0"}]
Apr 24 07:49:50: wifid : dynamic-power (0/0). current power (-1/18) (cache.c:2655)
2019-04-24 07:52:38 592 log.c:207:start_cns_logging: Send log history (10 lines)
Apr 24 07:49:50: wifid : Neighbor slot 0] 00-04-56-F8-33-26 rssi (0/0) last-active 4 (cache.c:2667)
2019-04-24 07:49:50 592 wifi.c:1208:Got fcgi request 0
2019-04-24 07:49:50 592 wifi.c:1243:fcgi_recv_cb: MSG_EXEC_STOP received
2019-04-24 07:49:50 592 wifi.c:1208:Got fcgi request 0
Apr 24 07:49:50: scmd : Exec recv complete closing 81 (actions.c:97)
Apr 24 07:50:00: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2735)
Apr 24 07:50:00: wifid : Existing neighbor 00-04-56-F8-33-26 bss 00-04-56-F8-34-00/00-04-56-F8-39-80 power 15/18 rssi 0/0 #clients 0/1
2019-04-24 07:50:04 592 common.c:841:rx_lldp: Received LLDP packet
2019-04-24 07:50:04 592 common.c:876:LLDP: CC-E1-7F-84-7E-00
Apr 24 07:50:05: wifid : error tx'ing neighbor info (main.c:1424)
2019-04-24 07:52:38 592 log.c:207:start_cns_logging: Send log history (10 lines)
Apr 24 07:50:05: wifid : dynamic-power (0/0). current power (-1/18) (cache.c:2655)
Apr 24 07:50:05: wifid : Neighbor slot 0] 00-04-56-F8-33-26 rssi (0/0) last-active 4 (cache.c:2667)
2019-04-24 07:50:08 592 device-agent.c:658:PING_DATA: len=28 msg [{"Pid": "592", "PLoss": "0"}]
Apr 24 07:50:14: scmd : stats timer at 1556088614 (stats.c:202)
Apr 24 07:50:15: wifid : notify msg type CMB_NOTIFY_MSG_TYPE_NEIGH_AP_DATA[21] received (cache.c:2735)
Apr 24 07:50:15: wifid : Existing neighbor 00-04-56-F8-33-26 bss 00-04-56-F8-34-00/00-04-56-F8-39-80 power 15/18 rssi 0/0 #clients 0/1
Apr 24 07:50:20: wifid : error tx'ing neighbor info (main.c:1424)
```

RF

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:

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

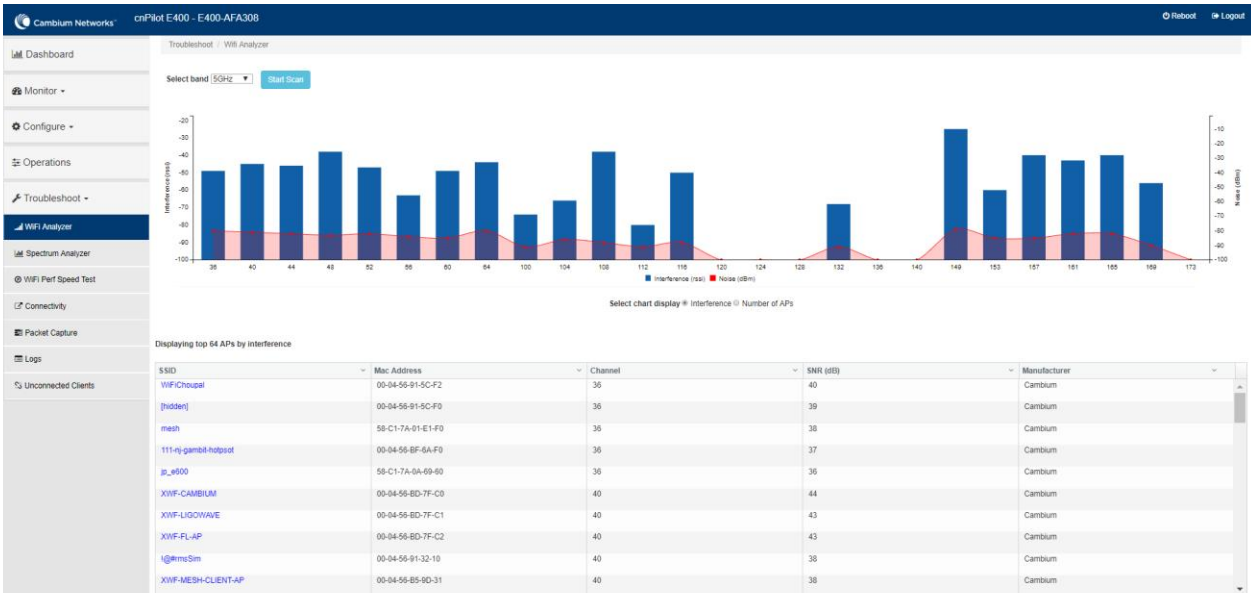
- Number of APs

  This tool shares more information of each channel as below:

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

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

Figure 53 Troubleshoot > Wi-Fi Analyzer > Interference Mode



Select band 5GHz

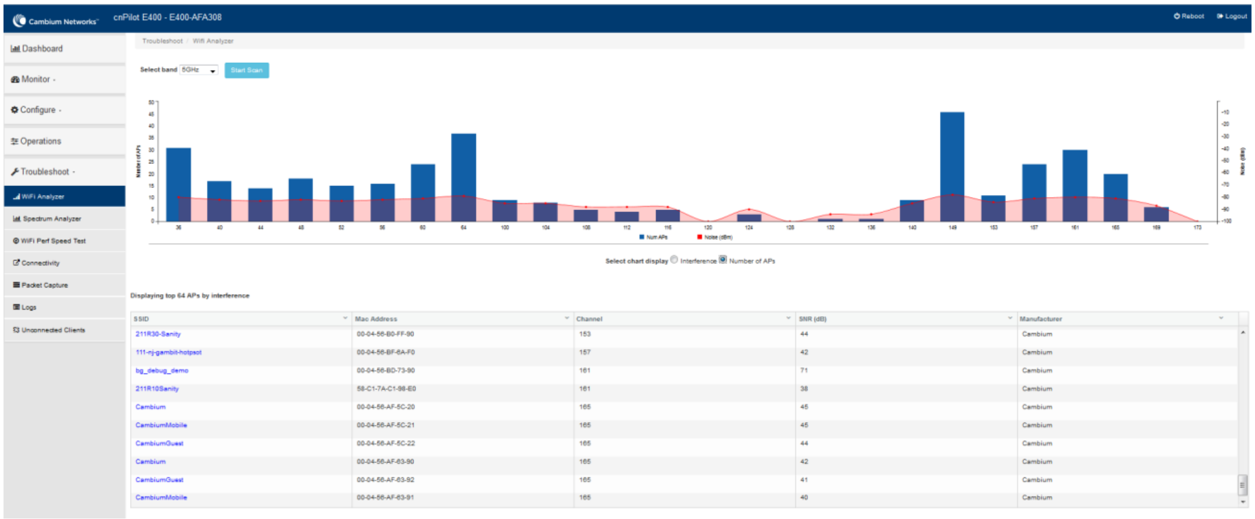
Select chart display ● Interference ○ Number of APs

Displaying top 64 APs by interference

SSID	Mac Address	Channel	SNR (dB)	Manufacturer
WiFiChoupal	00-04-56-91-5C-F2	36	40	Cambium
[hidden]	00-04-56-91-5C-F0	36	39	Cambium
mesh	58-C1-7A-01-E1-F0	36	38	Cambium
111-nj-gambit-hotpsot	00-04-56-BF-6A-F0	36	37	Cambium
jp_e600	58-C1-7A-0A-69-60	36	36	Cambium
XWF-CAMBIUM	00-04-56-BD-7F-C0	40	44	Cambium
XWF-LIGOWAVE	00-04-56-BD-7F-C1	40	43	Cambium
XWF-FL-AP	00-04-56-BD-7F-C2	40	43	Cambium
!@#rmsSim	00-04-56-91-32-10	40	38	Cambium
XWF-MESH-CLIENT-AP	00-04-56-B5-9D-31	40	38	Cambium

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

Figure 54 Troubleshoot > Wi-Fi Analyzer > Number of APs Mode



Displaying top 64 APs by interference

SSID	Mac Address	Channel	SNR (dB)	Manufacturer
211R30-Sanity	00-04-56-B0-FF-90	153	44	Cambium
111-nj-gambit-hotpsot	00-04-56-BF-6A-F0	157	42	Cambium
bg_debug_demo	00-04-56-BD-73-90	161	71	Cambium
211R10Sanity	58-C1-7A-C1-98-E0	161	38	Cambium
Cambium	00-04-56-AF-5C-20	165	45	Cambium
CambiumMobile	00-04-56-AF-5C-21	165	45	Cambium
CambiumGuest	00-04-56-AF-5C-22	165	44	Cambium
Cambium	00-04-56-AF-63-90	165	42	Cambium
CambiumGuest	00-04-56-AF-63-92	165	41	Cambium
CambiumMobile	00-04-56-AF-63-91	165	40	Cambium

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

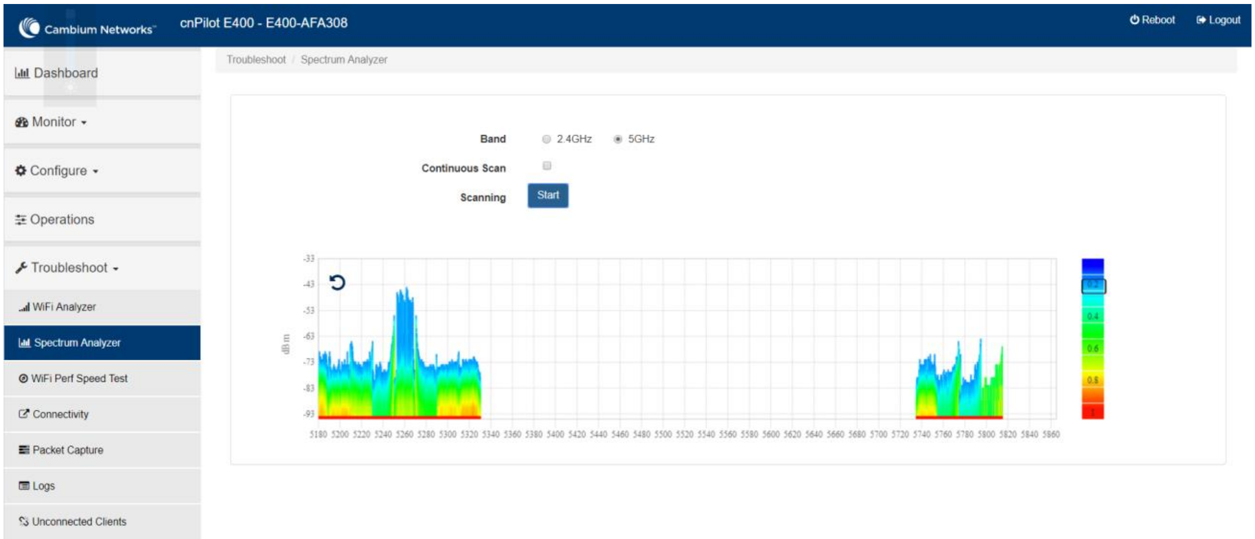
  If user is looking for continuous scan until stopped, this field has to be enabled.

- Scanning

  Option to start and stop the scan process.

Spectrum analyzer is available at Troubleshoot > Spectrum Analyzer.

Figure 55 Troubleshoot > Spectrum Analyzer



Band ○ 2.4GHz ● 5GHz

Continuous Scan □

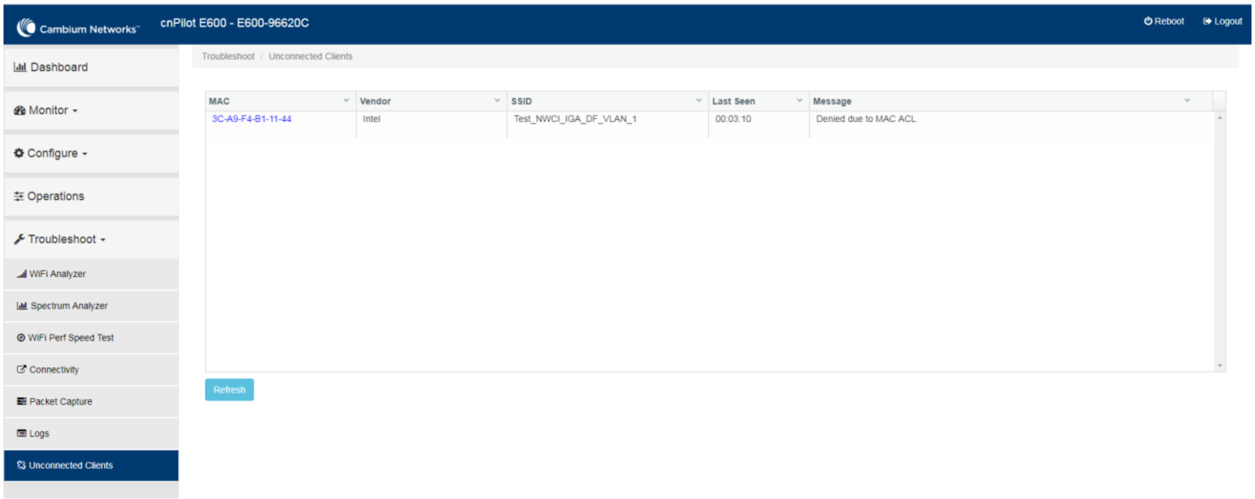
Scanning Start

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 56 Unconnected clients



MAC	Vendor	SSID	Last Seen	Message
3C-A9-F4-B1-11-44	Intel	Test_NWCI_IGA_DF_VLAN_1	00:03:10	Denied due to MAC ACL

Packet capture

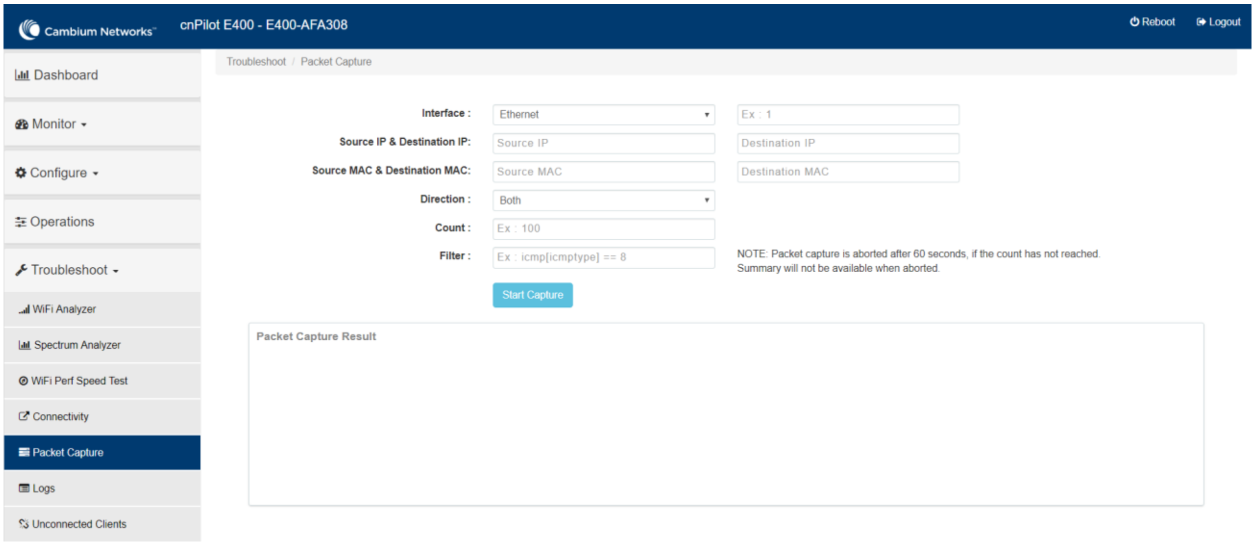
Allows the administrator to capture all packets on a specified interface. A decode of the packet indicating the network addresses, protocol types etc is displayed. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, port number etc. The number of 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:

Figure 57 Troubleshoot > Packet Capture page



Interface : Ethernet | Ex : 1

Source IP & Destination IP: Source IP | Destination IP

Source MAC & Destination MAC: Source MAC | Destination MAC

Direction : Both

Count : Ex : 100

Filter : Ex : icmp[icmptype] == 8

NOTE: Packet capture is aborted after 60 seconds, if the count has not reached. Summary will not be available when aborted.

Performance

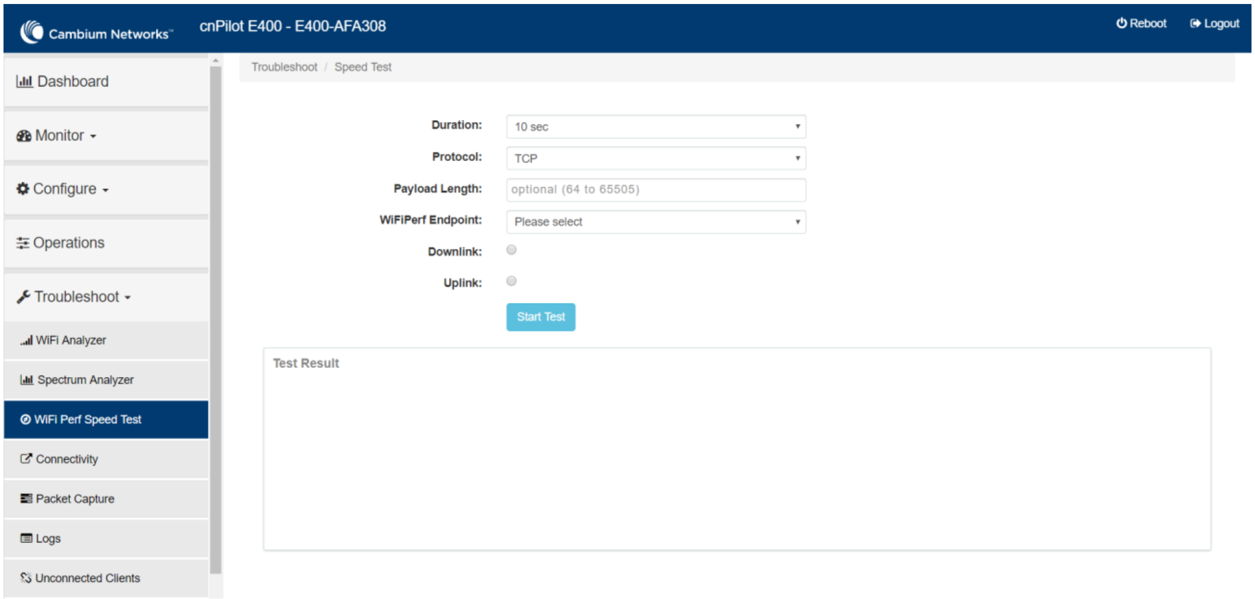
Wi-Fi Perf speed test

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.
- Click on Start Test.

Figure 58 Troubleshoot > Wi-Fi Perf Speed Test



Duration: 10 sec

Protocol: TCP

Payload Length: optional (64 to 65505)

WiFiPerf Endpoint: Please select

Downlink: ○

Uplink: ○

Test Result

Connectivity

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

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

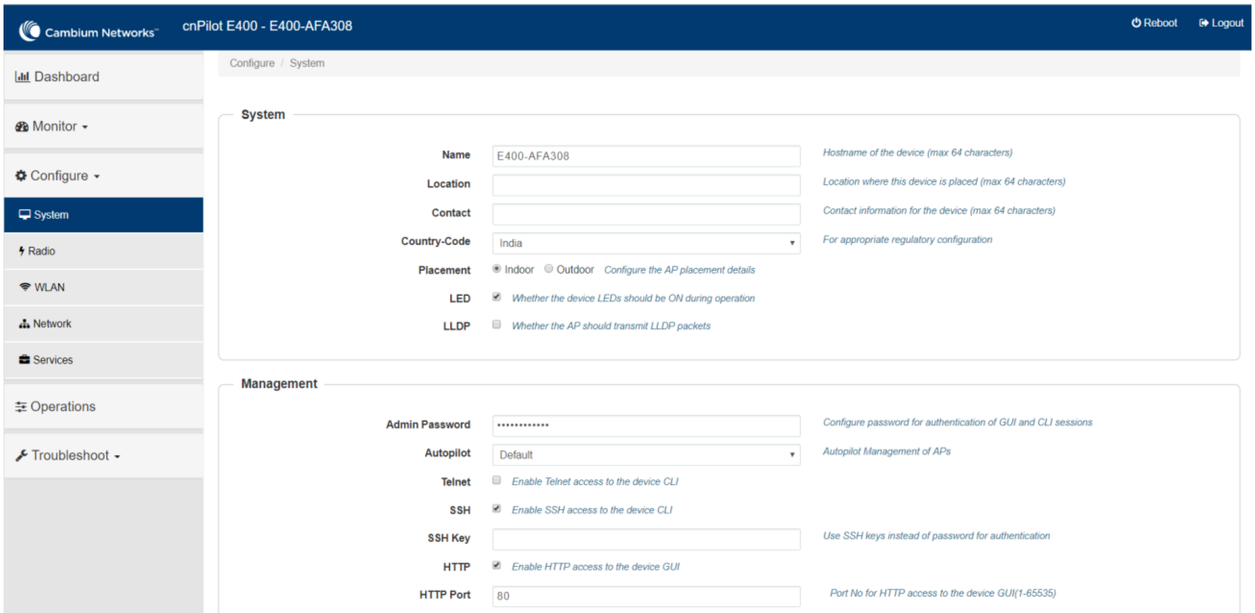
This is the default authentication mode enabled on device. Only one username is supported which is “admin”. Default password for “admin” username is “admin”. User has provision to configure/update password.

Device configuration

Figure 59 shows how to configure/update default password of admin user.

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

Figure 59 configure/update default password of admin user



System

Name	E400-AFA308	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	India	For appropriate regulatory configuration
Placement	● Indoor ○ Outdoor	Configure the AP placement details
LED	☑	Whether the device LEDs should be ON during operation
LLDP	□	Whether the AP should transmit LLDP packets

Management

Admin Password	••••••••••••	Configure password for authentication of GUI and CLI sessions
Autopilot	Default	Autopilot Management of APs
Telnet	□	Enable Telnet access to the device CLI
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	Port No for HTTP access to the device GUI(1-65535)

SSH-Key authentication

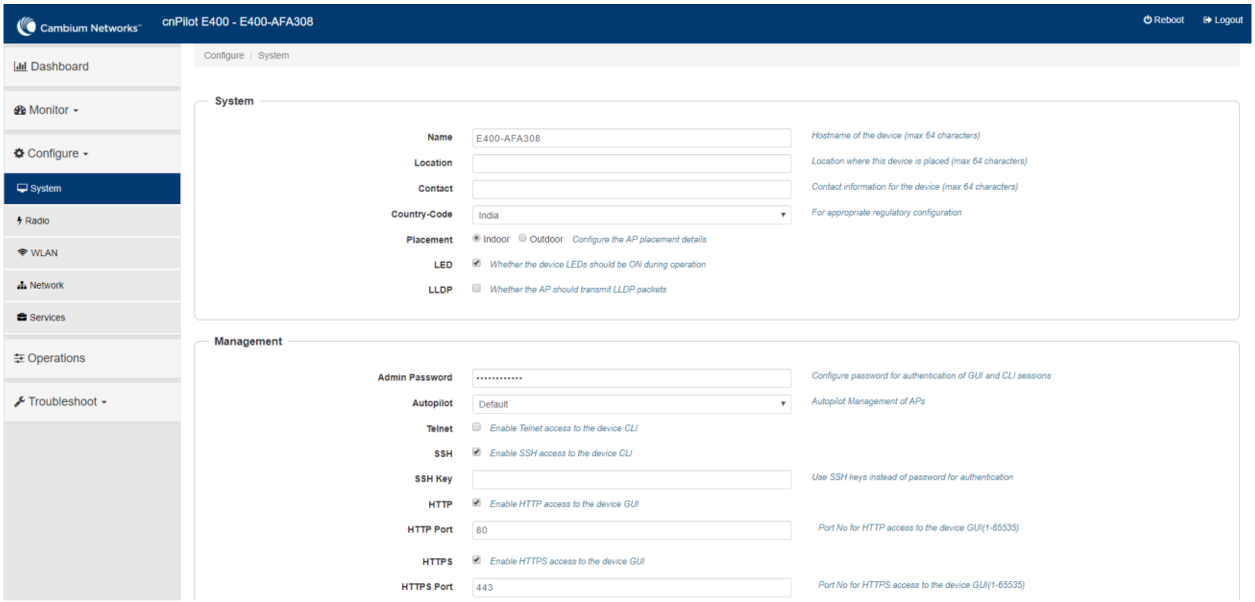
SSH keys are also used to connect remote machines securely. They are based on the SSH cryptographic network protocol, which is responsible for the encryption of the information stream between two machines. Ultimately, using SSH keys user can connect to remote devices without even entering a password 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.

Figure 60 System > Management



System

Name	E400-AFA308	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	India ▾	For appropriate regulatory configuration
Placement	● Indoor ○ Outdoor	Configure the AP placement details
LED	☑	Whether the device LEDs should be ON during operation
LLDP	□	Whether the AP should transmit LLDP packets

Management

Admin Password	············	Configure password for authentication of GUI and CLI sessions
Autopilot	Default ▾	Autopilot Management of APs
Telnet	□	Enable Telnet access to the device CLI
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	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)

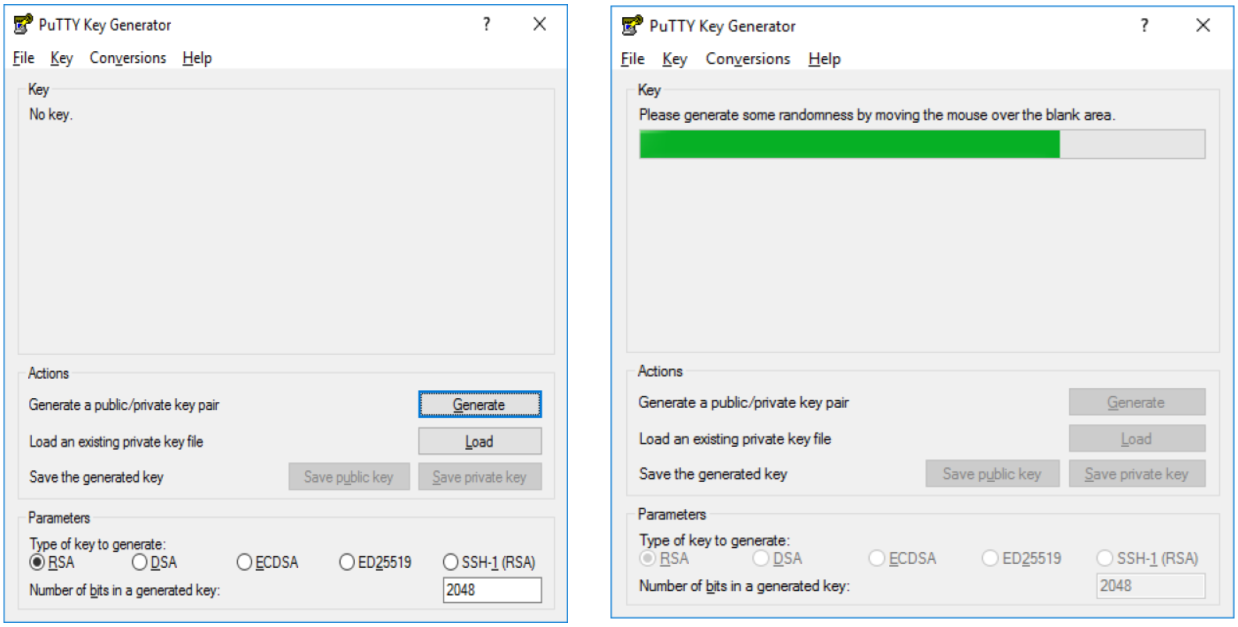
SSH Key Generation

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 61) and save private and public key as shown in Figure 62.

Figure 61 Generating public/private Key



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA

Number of bits in a generated key: 2048

Please generate some randomness by moving the mouse over the blank area.

Generate a public/private key pair

Load an existing private key file

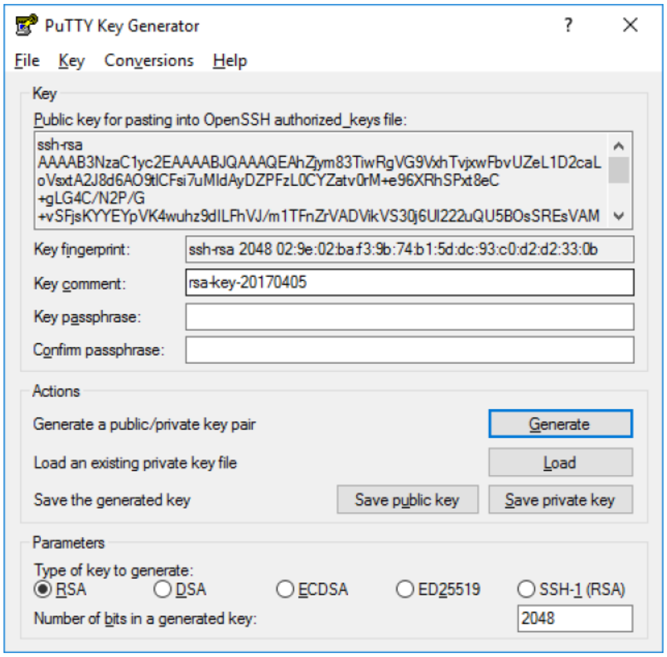
Save the generated key

Type of key to generate:

Number of bits in a generated key: 2048

2. Save the Public key and Private key once key pair is generated as shown in Figure 62.

Figure 62 Public and Private Key



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAhZjym83TiwRgVG9VxhTvjxwFbvUZeL1D2caL
oVsxtA2J8d6AO9tICFsi7uMIdAyDZPFzL0CYZatv0rM+e96XRhSPxt8eC
+gLG4C/N2P/G
+vSFjsKYYEYpVK4wuhz9dILFhVJ/m1TFnZrVADVikVS30j6UI222uQU5BOsSREsVAM
```

Key fingerprint: ssh-rsa 2048 02:9e:02:ba:f3:9b:74:b1:5d:dc:93:c0:d2:d2:33:0b

Key comment: rsa-key-20170405

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
● RSA

Number of bits in a generated key: 2048

3. Save the Public key generated in step above as described in Device configuration section.

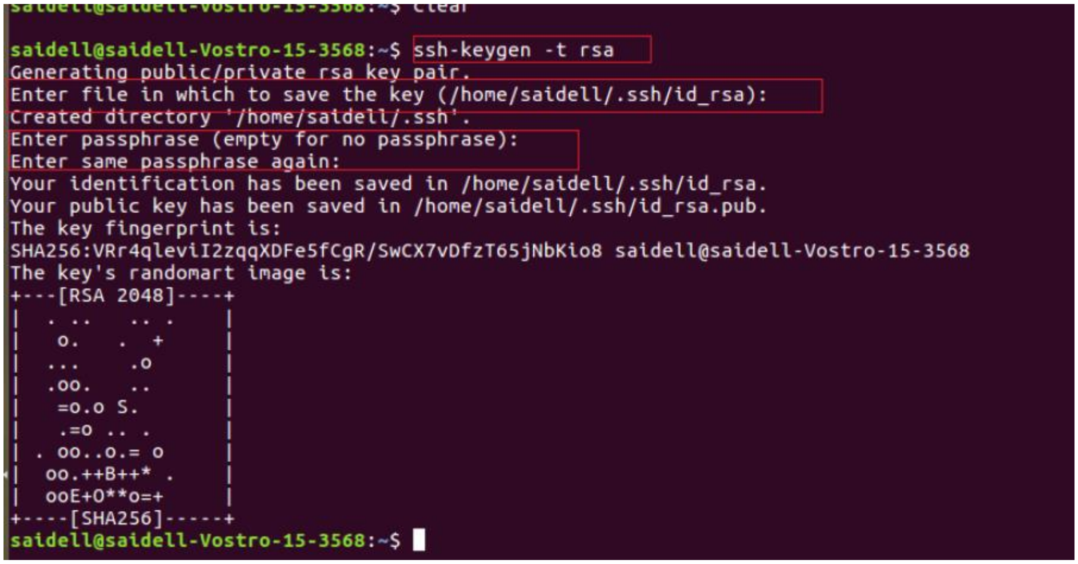
4. Login to device using Private key generated above with username as “admin”.

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 63.

Figure 63 Public Key location path

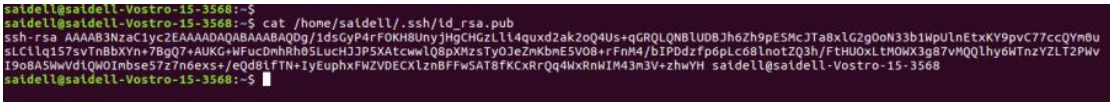


```
saidell@saidell-Vostro-15-3568:~$ clear

saidell@saidell-Vostro-15-3568:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/saidell/.ssh/id_rsa):
Created directory '/home/saidell/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/saidell/.ssh/id_rsa.
Your public key has been saved in /home/saidell/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:VRr4qleviI2zqqXDFe5fCgR/SwCX7vDfzT65jNbKio8 saidell@saidell-Vostro-15-3568
The key's randomart image is:
+---[RSA 2048]----+
|   . ..    .. .  |
|    o.    .  +   |
|   ...     .o    |
|   .oo.    ..    |
|    =o.o S.      |
|    .=o .. .     |
|  . oo..o.= o    |
|   oo.++B++* .   |
|   ooE+O**o=+    |
+----[SHA256]-----+
saidell@saidell-Vostro-15-3568:~$ 
```

2. The Public key is now located in PATH mentioned in Figure 63.
   - PATH = "Enter the file to which to save the key"
3. The private key (identification) is now saved in PATH as mentioned in Figure 64.
   - PATH = "Your identification has saved in <>"

Figure 64 Private Key saved path



```
saidell@saidell-Vostro-15-3568:~$
saidell@saidell-Vostro-15-3568:~$ cat /home/saidell/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDg/1dsGyP4rFOKH8UnyjHgCHGzLli4quxd2ak2oQ4Us+qGRQLQNBlUDBJh6Zh9pESMcJTa8xlG2gOoN33b1WpUlnEtxKY9pvC77ccQYm0u
sLCilq157svTnBbXYn+7BgQ7+AUKG+WFucDmhRh05LucHJJP5XAtcwwlQ8pXMzsTyOJeZmKbmE5VO8+rFnM4/bIPDdzfp6pLc68lnotZQ3h/FtHUOxLtMOWX3g87vMQQlhy6WTnzYZLT2PWv
I9o8A5WwVdiQWOImbse57z7n6exs+/eQd8ifTN+IyEuphxFWZVDECXlznBFFwSAT8fKCxRrQq4WxRnWIM43m3V+zhwYH saidell@saidell-Vostro-15-3568
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.

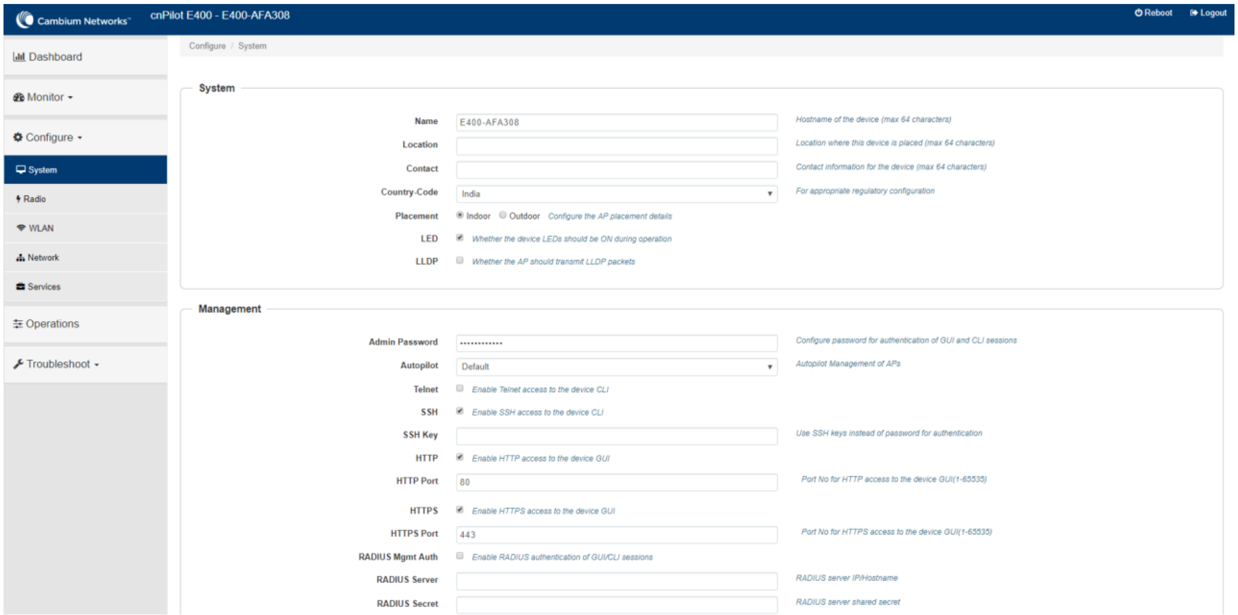
Device configuration

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 IP/Hostname and shared secret in RADIUS Server and RADIUS Secret parameters respectively.
3. Click Save.

Figure 65 System > Management: RADIUS Server and RADIUS Secret parameters



System

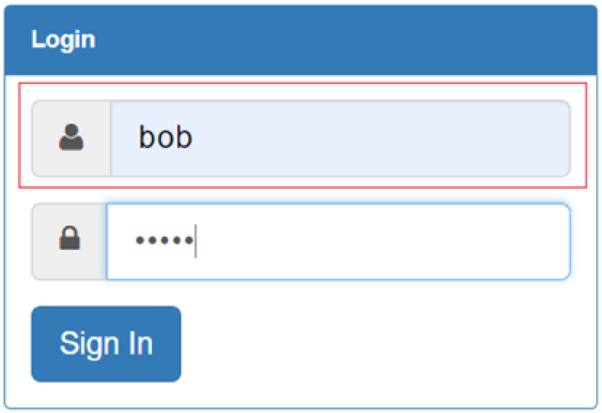
Name: E400-AFA308 — Hostname of the device (max 64 characters)
Location: — Location where this device is placed (max 64 characters)
Contact: — Contact information for the device (max 64 characters)
Country-Code: India — For appropriate regulatory configuration
Placement: ● Indoor ○ Outdoor — Configure the AP placement details
LED: ☑ Whether the device LEDs should be ON during operation
LLDP: □ Whether the AP should transmit LLDP packets

Management

Admin Password: •••••••••••• — Configure password for authentication of GUI and CLI sessions
Autopilot: Default — Autopilot Management of APs
Telnet: □ Enable Telnet access to the device CLI
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 — 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)
RADIUS Mgmt Auth: □ Enable RADIUS authentication of GUI/CLI sessions
RADIUS Server: — RADIUS server IP/Hostname
RADIUS Secret: — RADIUS server shared secret

4. Login to device using appropriate credentials as shown in Figure 66.

Figure 66 UI Login page


Login

bob

•••••

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 45 lists the configurable parameters that are exclusive to mesh:

Table 45 Configure: WLAN > Mesh parameters

Parameters	Description	Range	Default
Enable	Option to enable a WLAN profile. Once enabled, a Beacon is broadcasted with SSID and respective configured parameters in a WLAN profile.	–	–
Mesh	This parameter is required when a WDS connection is established with cnPilot devices. Four options are available under this parameter: 1. Base 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.	–	Off

Parameters	Description	Range	Default
	2. Client A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-based AP to connect. 3. Recovery A WLAN profile configured as mesh-recovery will broadcast pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on mesh-base device. Mesh-client will auto scan for mesh-recovery 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 based on selected algorithm. Following security methods are supported by cnPilot devices: 1. Open This method is preferred when Layer 2 authentication is built in the network. With this configured on cnPilot 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.	–	Open
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 • 5GHz	–	2.4GHz

Parameters	Description	Range	Default
Max Clients	This specifies the maximum number of mesh clients that can be associated to a mesh WLAN profile. This varies based on cnPilot device model number. Refer Table 16 for more details.	1-512 (Refer Table 16)	128
Client Isolation	This feature needs to be enabled when there is a need for prohibition of inter mesh devices communication either over the network or on an AP. Three options are available to configure based on requirement: 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 client isolation feature. It prevents mesh client communications connected to different AP deployed in same network.	–	Disabled
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	–	Disabled
Mesh Vlan Tagging	Enable the VLAN tagging over mesh link. This is applicable only for Cambium mesh topology.	–	Enabled
Mesh Auto Detect Backhaul	1. Single Hop MC is configured on MB with same WLAN parameters. When enabled, this feature triggers when a MB losses Ethernet connectivity. MB profile will get disabled and MC profile will get enable and establishes mesh link with nearest MB. For MB profile to get auto disabled, uncheck Mesh Multi Hop. 2. Multi Hop MC is configured on MB with same WLAN parameters. When enabled, this feature triggers when a MB losses Ethernet connectivity. MB profile and MC profile will get enable and establishes mesh link with nearest MB.	–	Disabled
Drop Multicast Traffic	When enabled, will drop all multicast flowing in or out of that WLAN.	–	Disabled

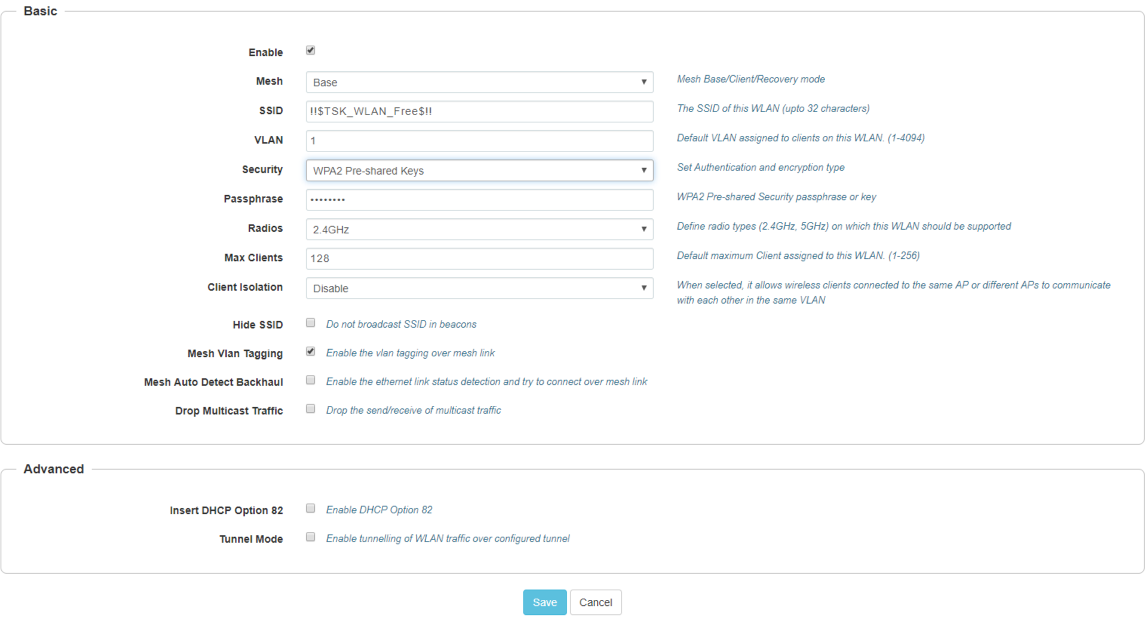
Parameters	Description	Range	Default
Insert DHCP Option 82	Enabling this option appends Option 82 in the DHCP packets. Following information is allowed to configure: 1. DHCP Option 82 Circuit ID Configurable parameters under this option are as follows: • Hostname • APMAC • Site ID • BSSID • SSID • Custom 2. DHCP Option 82 Remote ID Configurable parameters under this option are as follows: • Hostname • APMAC • Site ID • BSSID • SSID • Custom		Disabled
Tunnel Mode	This option is enabled when user traffic is tunneled to central network either using L2TP or L2GRE.	–	Disabled
Mesh Monitored Host	This parameter is exclusive to MC device. Configure IP or Hostname to check the link status.	–	–
Mesh Monitor Duration	Configure the interval at which the ping is sent for the configured mesh monitored host.	5-60 Min	30
Mesh Recovery Interval	Configure the interval for the consecutive ping loss seen after which the mesh link is considered to be down and a reconnect is attempted. One can configure the duration and interval both to be the same at which case the first 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 67 Configure > Mesh > Base parameters



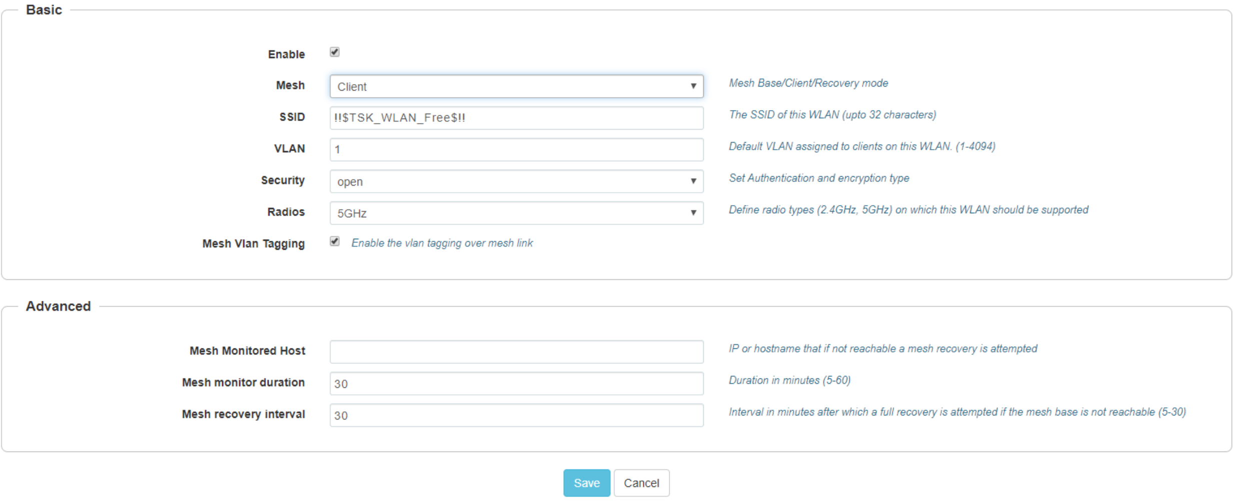
Basic

Enable	☑	
Mesh	Base ▾	*Mesh Base/Client/Recovery mode*
SSID	!!TSK_WLAN_Free!!	*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	2.4GHz ▾	*Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported*
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 SSID	☐ *Do not broadcast SSID in beacons*	
Mesh Vlan Tagging	☑ *Enable the vlan tagging over mesh link*	
Mesh Auto Detect Backhaul	☐ *Enable the ethernet link status detection and 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 configured tunnel*

Figure 68 Configure > Mesh > Client parameters



Basic

Enable ☑

Mesh: Client ▾ — *Mesh Base/Client/Recovery mode*

SSID: !!TSK_WLAN_Free!! — *The SSID of this WLAN (upto 32 characters)*

VLAN: 1 — *Default VLAN assigned to clients on this WLAN. (1-4094)*

Security: open ▾ — *Set Authentication and encryption type*

Radios: 5GHz ▾ — *Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported*

Mesh Vlan Tagging ☑ *Enable the vlan 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)*

Mesh link

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

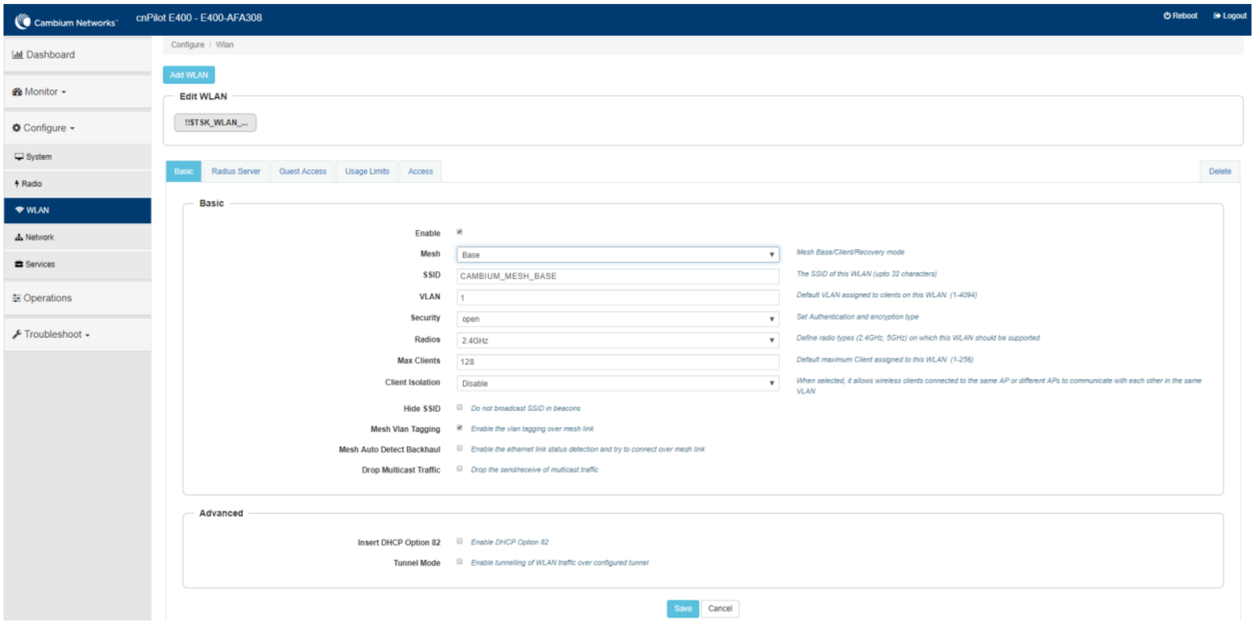
VLAN 1 as management interface

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

Figure 69 Mesh Base configuration with native VLAN 1



Edit WLAN: !!$TSK_WLAN_...

Basic

Enable ☑

Mesh: Base ▾ — *Mesh Base/Client/Recovery mode*

SSID: CAMBIUM_MESH_BASE — *The SSID of this WLAN (upto 32 characters)*

VLAN: 1 — *Default VLAN assigned to clients on this WLAN. (1-4094)*

Security: open ▾ — *Set Authentication and encryption type*

Radios: 2.4GHz ▾ — *Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported*

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 SSID ☐ *Do not broadcast SSID in beacons*

Mesh Vlan Tagging ☑ *Enable the vlan tagging over mesh link*

Mesh Auto Detect Backhaul ☐ *Enable the ethernet link status detection and try to connect over mesh link*

Drop Multicast Traffic ☐ *Drop the send/receive of multicast traffic*

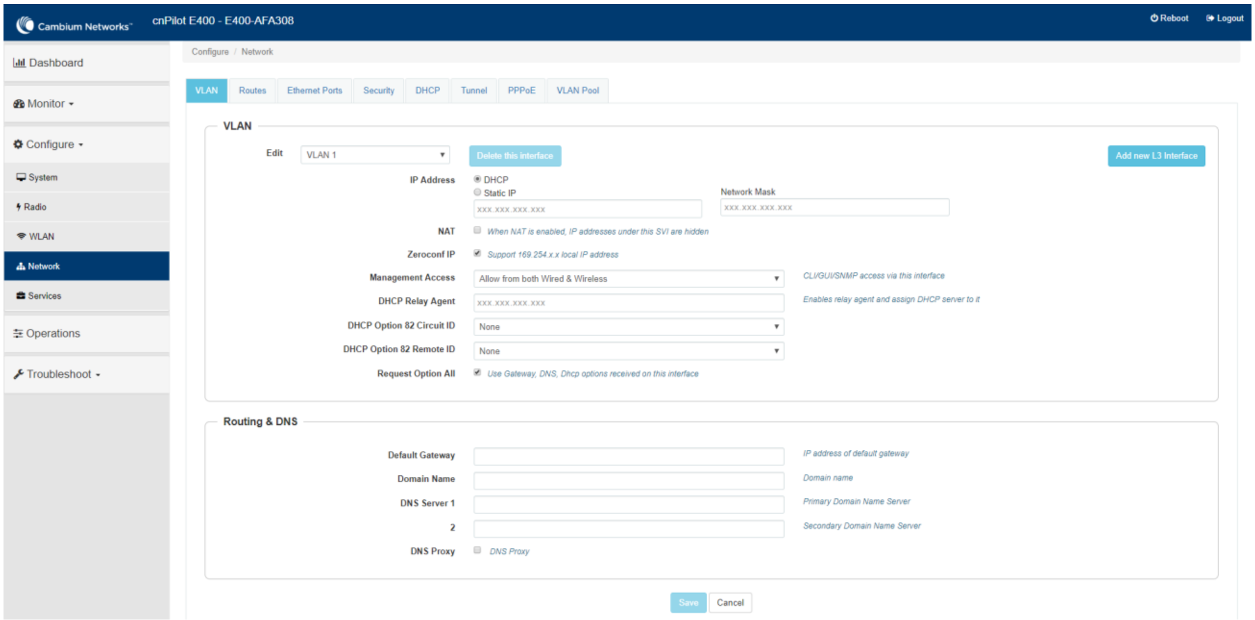
Advanced

Insert DHCP Option 82 ☐ *Enable DHCP Option 82*

Tunnel Mode ☐ *Enable tunnelling of WLAN traffic over configured tunnel*

   b. Management VLAN Interface

Figure 70 Mesh Base configuration > Management VLAN 1



VLAN

Edit: VLAN 1

IP Address: ● DHCP ○ Static IP xxx.xxx.xxx.xxx

Network Mask: xxx.xxx.xxx.xxx

NAT: □ When NAT is enabled, IP addresses under this SVI are hidden

Zeroconf IP: ☑ Support 169.254.x.x local IP address

Management Access: Allow from both Wired & Wireless — CLI/GUI/SNMP access via this interface

DHCP Relay Agent: xxx.xxx.xxx.xxx — Enables relay agent and assign DHCP server to it

DHCP Option 82 Circuit ID: None

DHCP Option 82 Remote ID: None

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

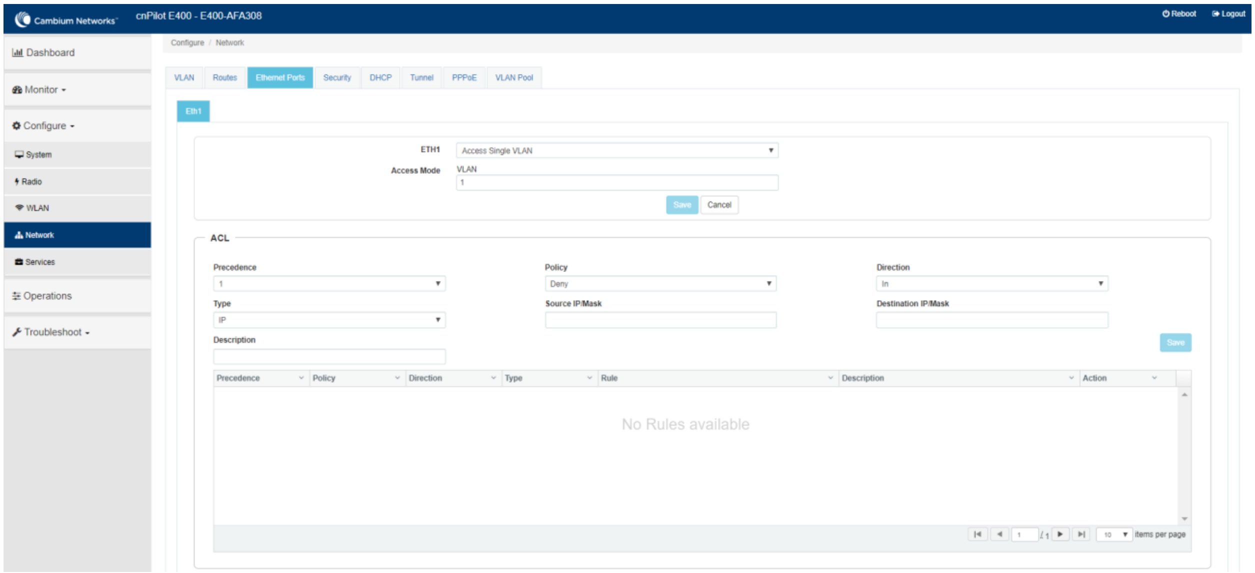
DNS Server 1: — Primary Domain Name Server

2: — Secondary Domain Name Server

DNS Proxy: □ DNS Proxy

c. Ethernet Interface

Figure 71 Mesh Base Ethernet configuration > Access VLAN 1



ETH1: Access Single VLAN

Access Mode: VLAN 1

ACL

Precedence: 1

Policy: Deny

Direction: In

Type: IP

Source IP/Mask:

Destination IP/Mask:

Description:

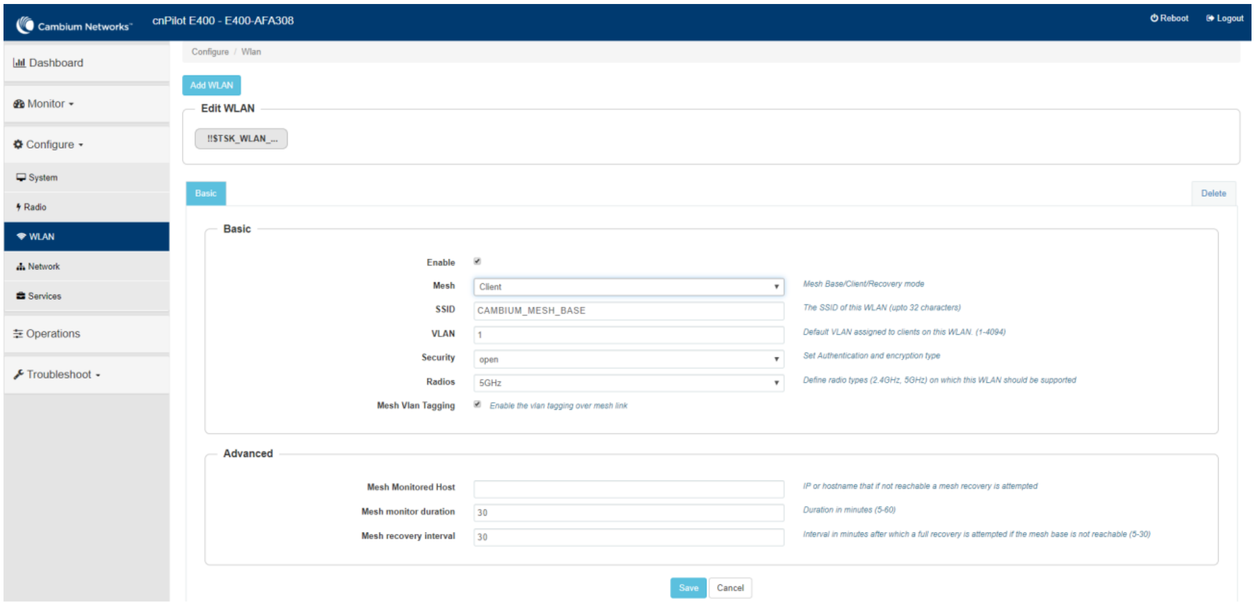
Precedence	Policy	Direction	Type	Rule	Description	Action

No Rules available

2. Configure MC as below:

a. WLAN Profile

Figure 72 Mesh Client configuration with VLAN 1



Edit WLAN

Basic

Enable ☑

Mesh: Client ▾ — *Mesh Base/Client/Recovery mode*

SSID: CAMBIUM_MESH_BASE — *The SSID of this WLAN (upto 32 characters)*

VLAN: 1 — *Default VLAN assigned to clients on this WLAN. (1-4094)*

Security: open ▾ — *Set Authentication and encryption type*

Radios: 5GHz ▾ — *Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported*

Mesh Vlan Tagging ☑ *Enable the vlan tagging over mesh link*

Advanced

Mesh Monitored Host: — *IP or hostname that if not reachable a mesh recovery is attempted*

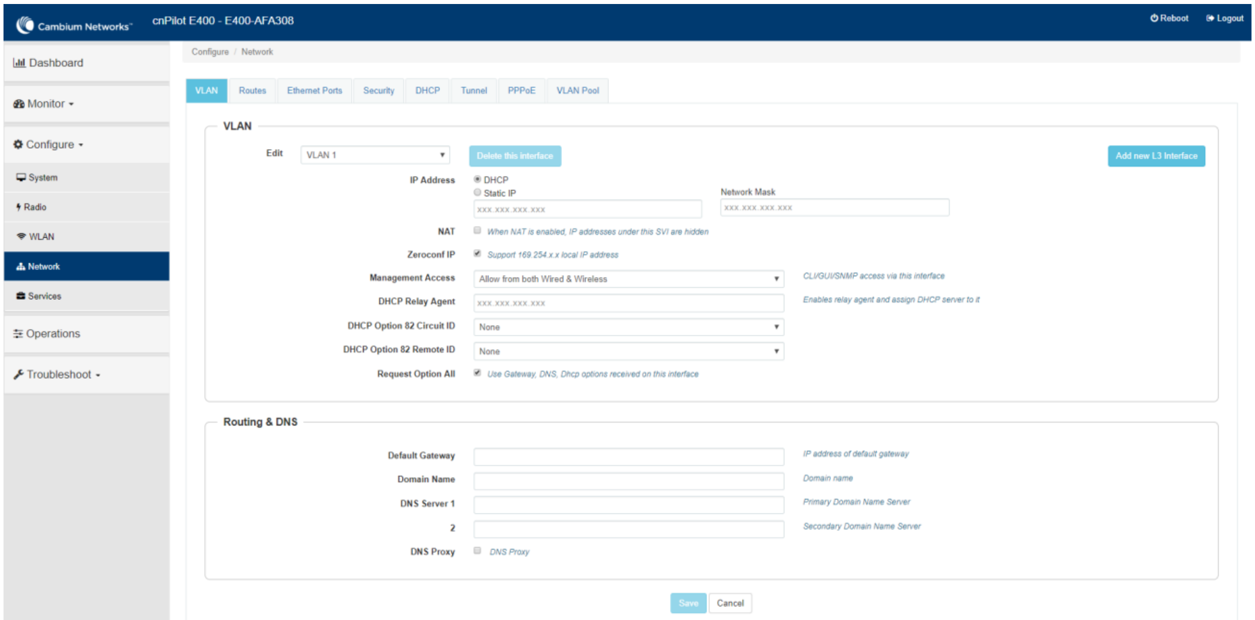
Mesh monitor duration: 30 — *Duration in minutes (5-60)*

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

Figure 73 Mesh Client configuration > Management VLAN 1



VLAN

Edit: VLAN 1 ▾

IP Address: ● DHCP ○ Static IP xxx.xxx.xxx.xxx — Network Mask xxx.xxx.xxx.xxx

NAT ☐ *When NAT is enabled, IP addresses under this SVI are hidden*

Zeroconf IP ☑ *Support 169.254.x.x local IP address*

Management Access: Allow from both Wired & Wireless ▾ — *CLI/GUI/SNMP access via this interface*

DHCP Relay Agent: xxx.xxx.xxx.xxx — *Enables relay agent and assign DHCP server to it*

DHCP Option 82 Circuit ID: None ▾

DHCP Option 82 Remote ID: None ▾

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*

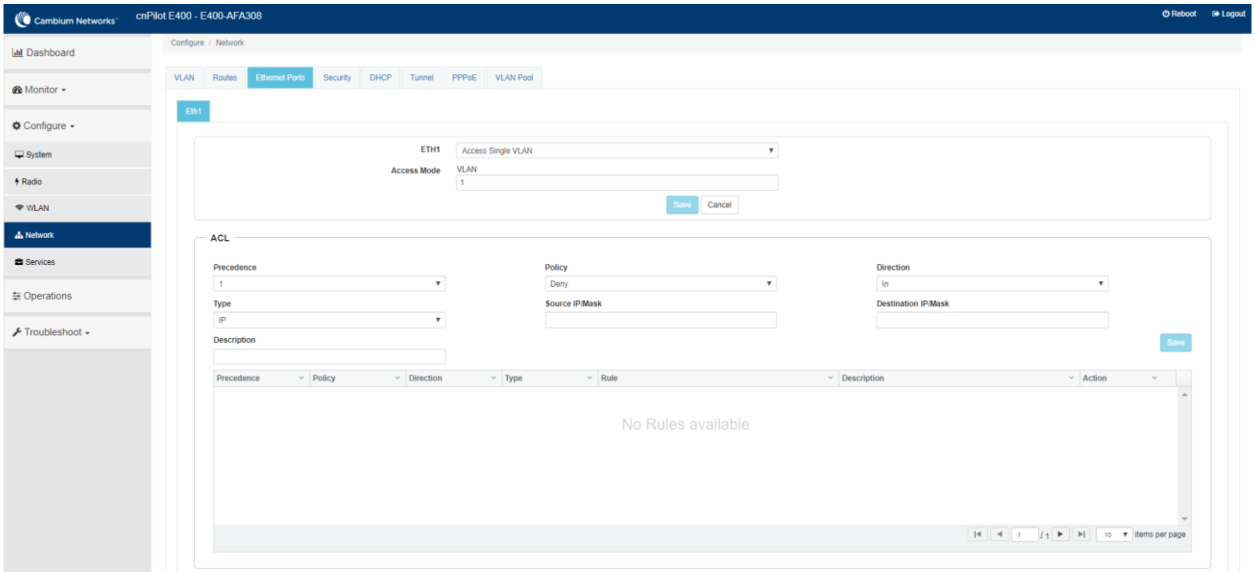
2: — *Secondary Domain Name Server*

DNS Proxy ☐ *DNS Proxy*

Save Cancel

c. Ethernet Interface

Figure 74 Mesh Client Ethernet configuration > Access VLAN 1



ETH1: Access Single VLAN

Access Mode: VLAN 1

Precedence	Policy	Direction
1	Deny	In

Type	Source IP/Mask	Destination IP/Mask
IP		

Description:

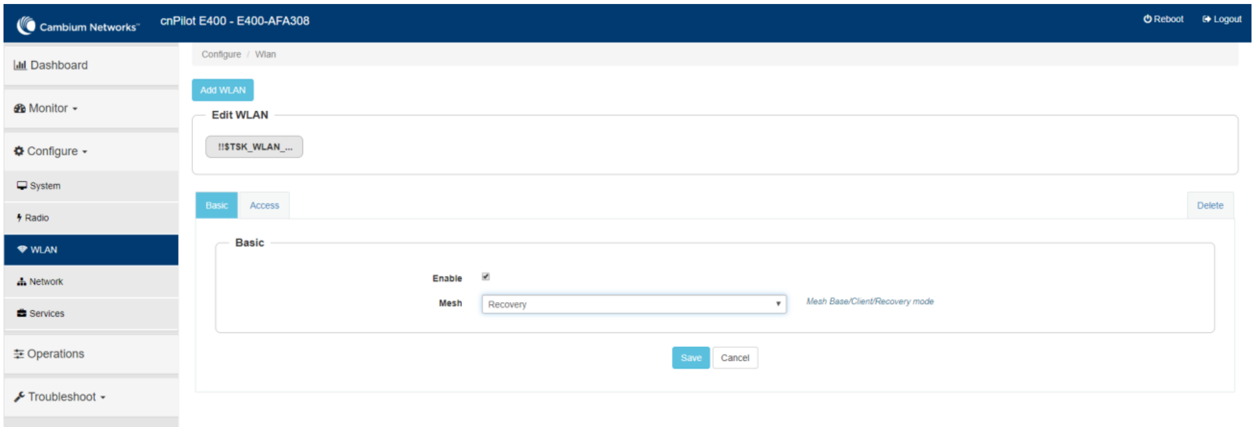
Precedence	Policy	Direction	Type	Rule	Description	Action

No Rules available

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

   a. WLAN Profile

Figure 75 Configure > WLAN > Mesh Recovery



Edit WLAN: !!$TSK_WLAN_...

Basic

Enable: ☑

Mesh: Recovery — *Mesh Base/Client/Recovery mode*

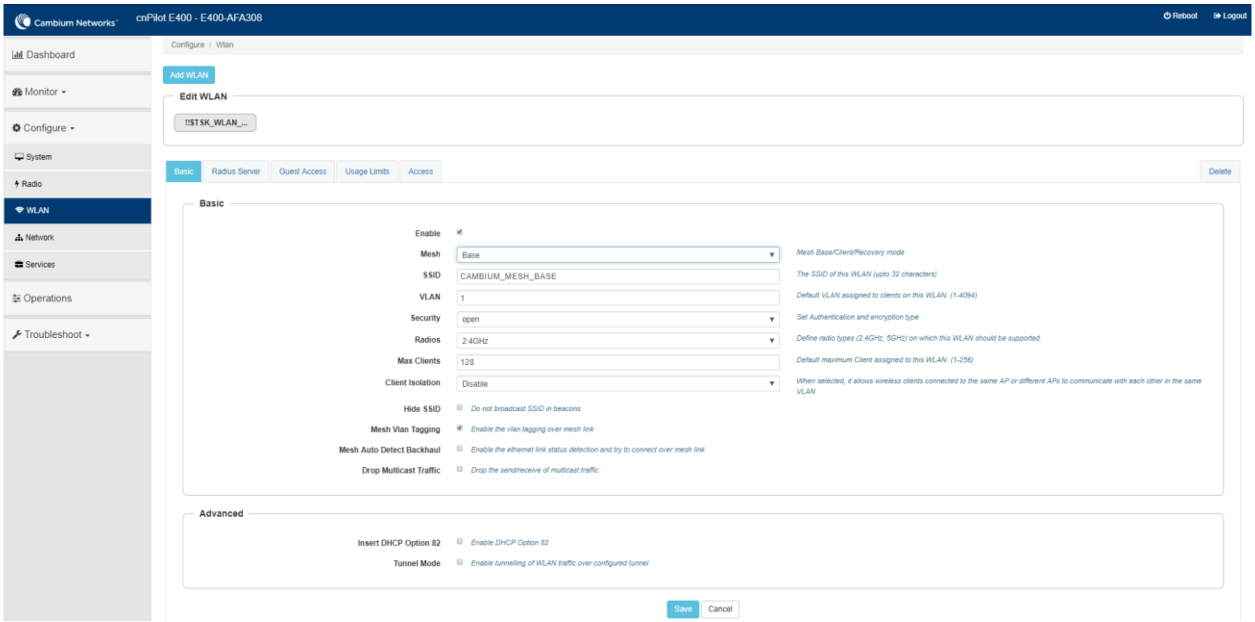
Non-VLAN 1 as management interface

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

Figure 76 Mesh Base configuration with non-VLAN 1



Edit WLAN

!!$TSK_WLAN_...

Basic

Enable ☑

Mesh: Base — *Mesh Base/Client/Recovery mode*

SSID: CAMBIUM_MESH_BASE — *The SSID of this WLAN (upto 32 characters)*

VLAN: 1 — *Default VLAN assigned to clients on this WLAN. (1-4094)*

Security: open — *Set Authentication and encryption type*

Radios: 2.4GHz — *Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported*

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 SSID ☐ *Do not broadcast SSID in beacons*

Mesh Vlan Tagging ☑ *Enable the vlan tagging over mesh link*

Mesh Auto Detect Backhaul ☐ *Enable the ethernet link status detection and try to connect over mesh link*

Drop Multicast Traffic ☐ *Drop the send/receive of multicast traffic*

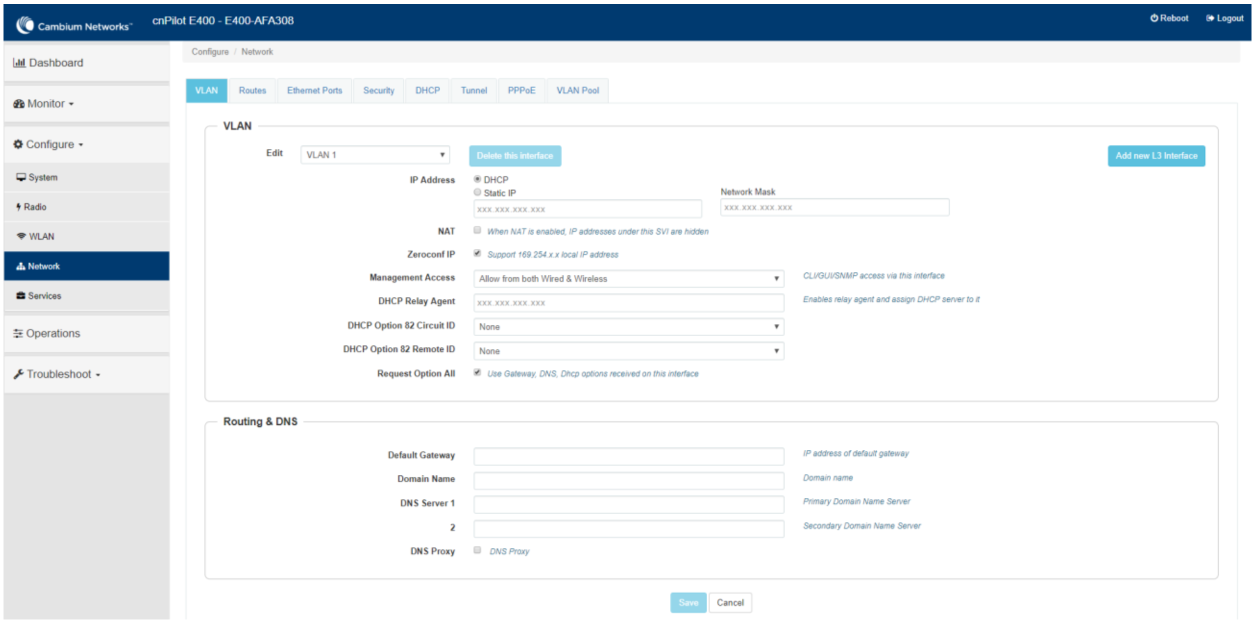
Advanced

Insert DHCP Option 82 ☐ *Enable DHCP Option 82*

Tunnel Mode ☐ *Enable tunnelling of WLAN traffic over configured tunnel*

b. Management VLAN Interface

Figure 77 Mesh Base configuration > Management non-VLAN 1



VLAN

Edit: VLAN 1

IP Address: ● DHCP ○ Static IP xxx.xxx.xxx.xxx Network Mask xxx.xxx.xxx.xxx

NAT ☐ *When NAT is enabled, IP addresses under this SVI are hidden*

Zeroconf IP ☑ *Support 169.254.x.x local IP address*

Management Access: Allow from both Wired & Wireless — *CLI/GUI/SNMP access via this interface*

DHCP Relay Agent: xxx.xxx.xxx.xxx — *Enables relay agent and assign DHCP server to it*

DHCP Option 82 Circuit ID: None

DHCP Option 82 Remote ID: None

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*

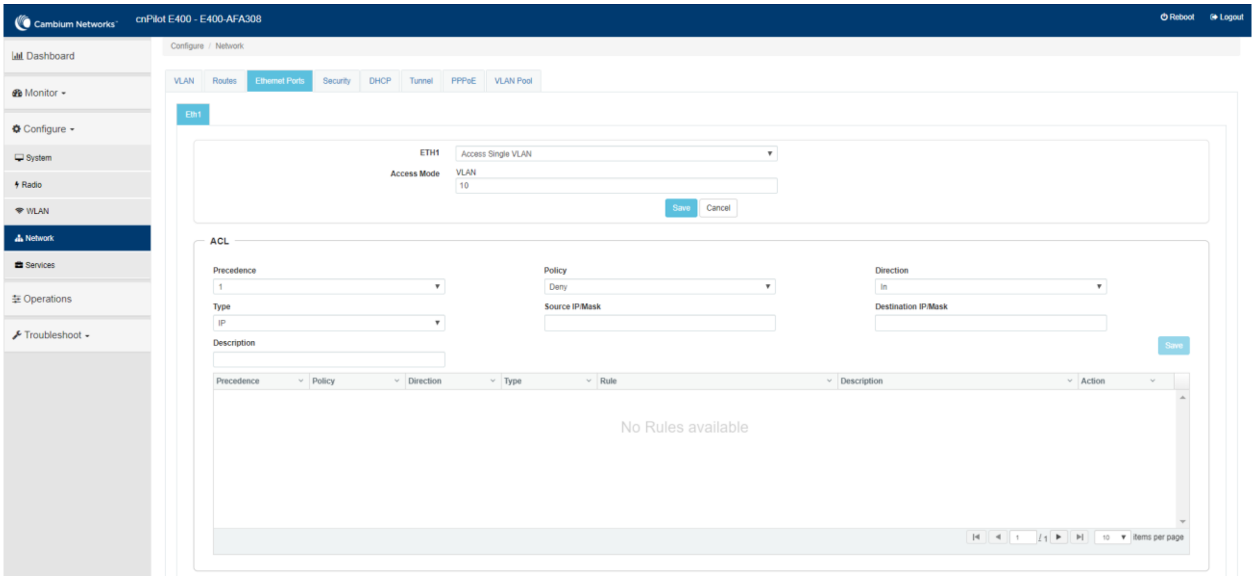
DNS Server 1 — *Primary Domain Name Server*

2 — *Secondary Domain Name Server*

DNS Proxy ☐ *DNS Proxy*

c. Ethernet Interface

Figure 78 Mesh Base Ethernet configuration > Access non-VLAN 1



ETH1: Access Single VLAN

Access Mode: VLAN 10

ACL

Precedence: 1

Policy: Deny

Direction: In

Type: IP

Source IP/Mask:

Destination IP/Mask:

Description:

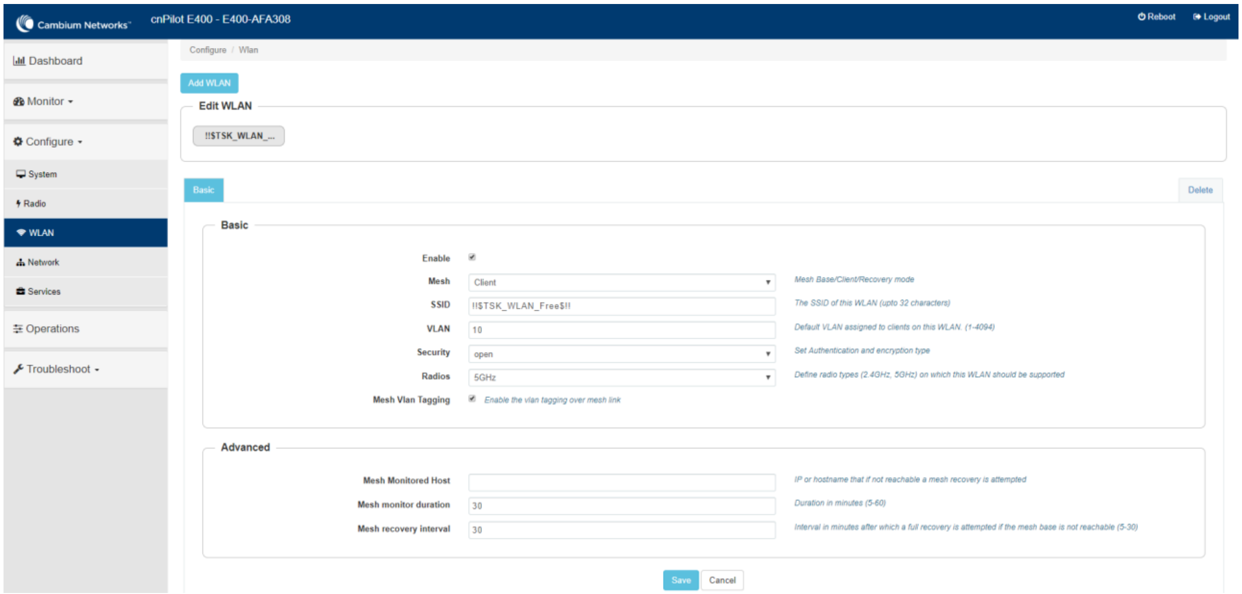
Precedence	Policy	Direction	Type	Rule	Description	Action

No Rules available

2. Configure MC as below:

   a. WLAN Profile

Figure 79 Mesh Client configuration with non-VLAN 1



Basic

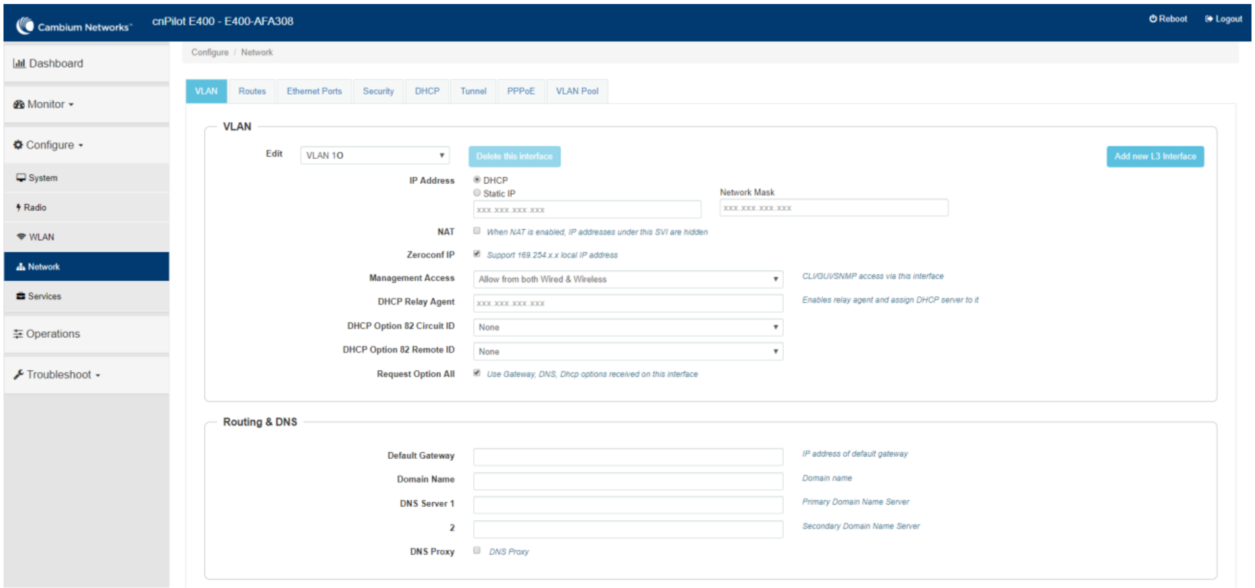
Enable	☑	
Mesh	Client	Mesh Base/Client/Recovery mode
SSID	!!TSK_WLAN_Free!!	The SSID of this WLAN (upto 32 characters)
VLAN	10	Default VLAN assigned to clients on this WLAN. (1-4094)
Security	open	Set Authentication and encryption type
Radios	5GHz	Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported
Mesh Vlan Tagging	☑ Enable the vlan 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)

   b. Management Interface

Figure 80 Mesh Client configuration > Management non-VLAN 1



VLAN

Edit: VLAN 10

IP Address: ● DHCP ○ Static IP xxx.xxx.xxx.xxx Network Mask xxx.xxx.xxx.xxx

NAT: □ When NAT is enabled, IP addresses under this SVI are hidden

Zeroconf IP: ☑ Support 169.254.x.x local IP address

Management Access: Allow from both Wired & Wireless — CLI/GUI/SNMP access via this interface

DHCP Relay Agent: xxx.xxx.xxx.xxx — Enables relay agent and assign DHCP server to it

DHCP Option 82 Circuit ID: None

DHCP Option 82 Remote ID: None

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

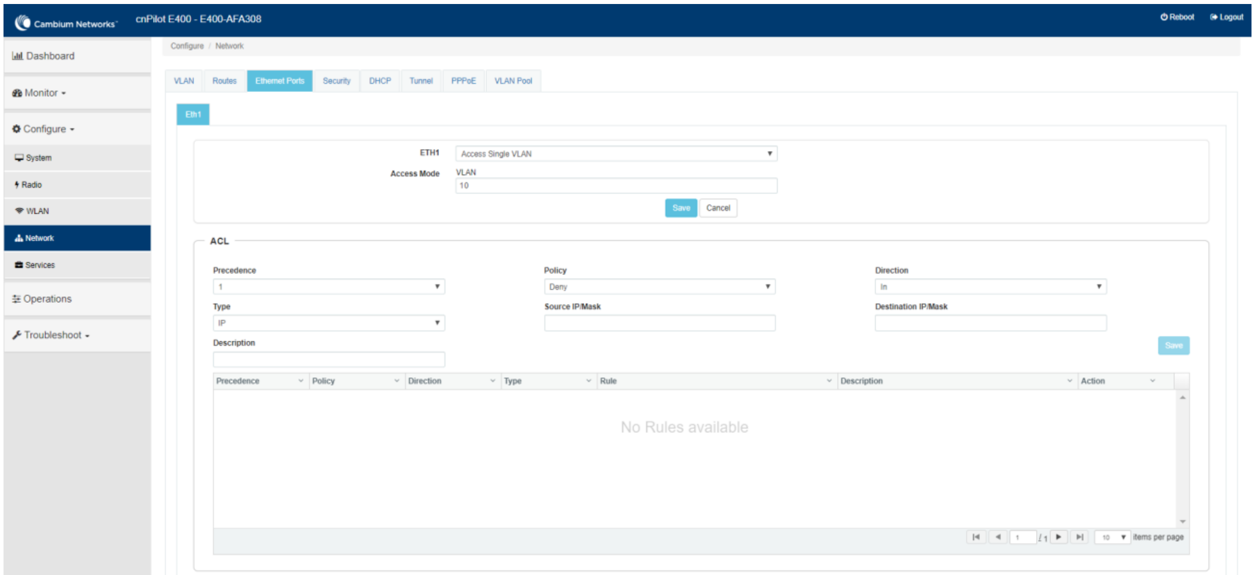
DNS Server 1: — Primary Domain Name Server

2: — Secondary Domain Name Server

DNS Proxy: □ DNS Proxy

c. Ethernet Interface

Figure 81 Mesh Client Ethernet configuration > Access non-VLAN 1



ETH1: Access Single VLAN

Access Mode: VLAN 10

ACL

Precedence: 1

Policy: Deny

Direction: In

Type: IP

Source IP/Mask:

Destination IP/Mask:

Description:

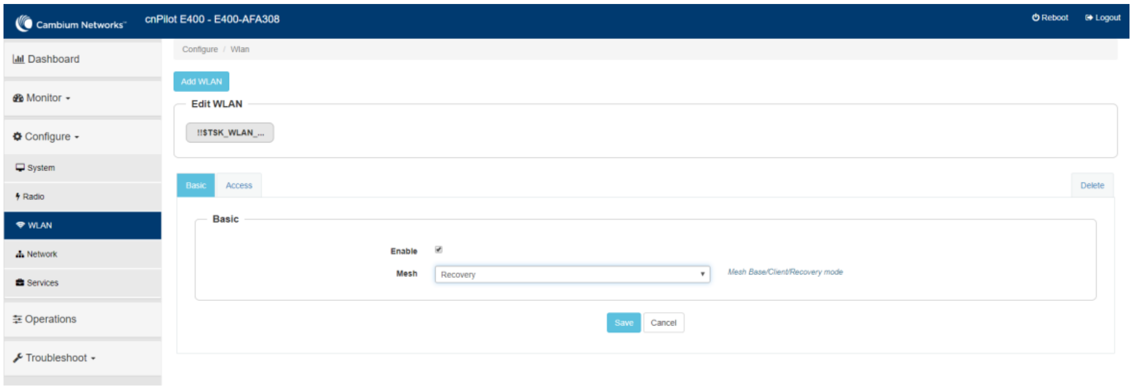
Precedence	Policy	Direction	Type	Rule	Description	Action

No Rules available

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

a. WLAN Profile

Figure 82 Configure > WLAN > Mesh Recovery



Edit WLAN

!!$TSK_WLAN_...

Basic

Enable ☑

Mesh: Recovery — *Mesh Base/Client/Recovery mode*

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

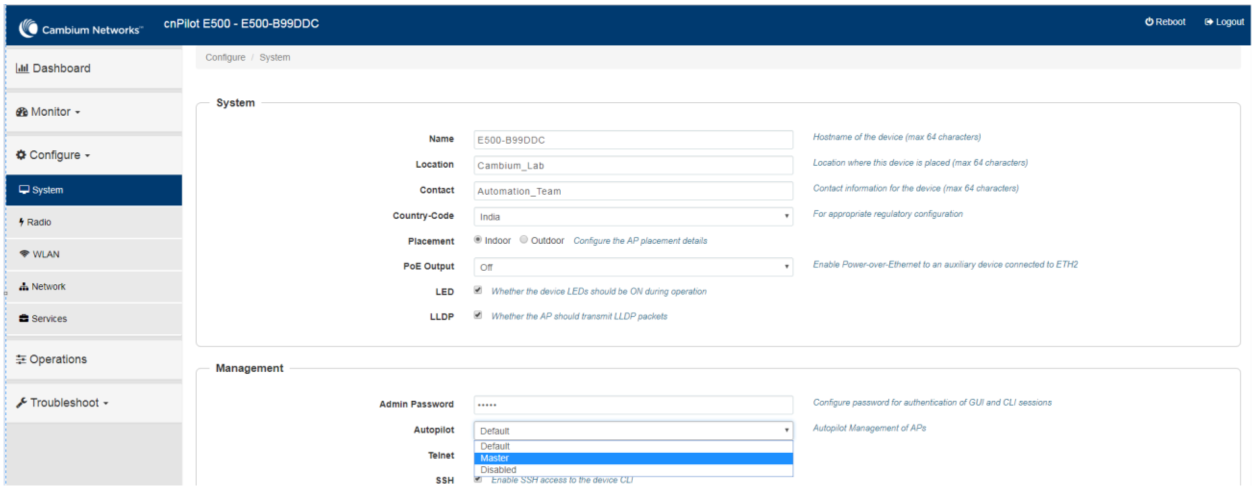
To configure member APs to a Master:

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

> Note The AP needs to be upgraded with autopilot firmware.

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

Figure 83 Configure > System > Management > Autopilot



System

Name: E500-B99DDC — *Hostname of the device (max 64 characters)*

Location: Cambium_Lab — *Location where this device is placed (max 64 characters)*

Contact: Automation_Team — *Contact information for the device (max 64 characters)*

Country-Code: India — *For appropriate regulatory configuration*

Placement: ● Indoor ○ Outdoor — *Configure the AP placement details*

PoE Output: Off — *Enable Power-over-Ethernet to an auxiliary device connected to ETH2*

LED: ☑ *Whether the device LEDs should be ON during operation*

LLDP: ☑ *Whether the AP should transmit LLDP packets*

Management

Admin Password: ••••• — *Configure password for authentication of GUI and CLI sessions*

Autopilot: Default — *Autopilot Management of APs*

Default
Master
Disabled

Telnet

SSH: ☑ *Enable SSH access to the device CLI*

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:

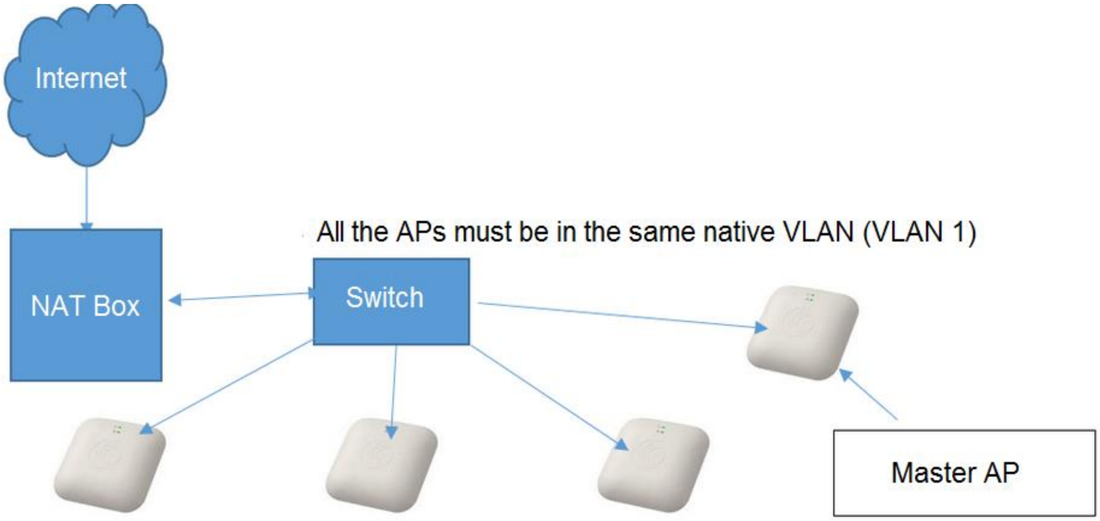
- Configuring an AP with Internal DHCP server
- Configuring an AP with External DHCP Server

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 84.

Figure 84 Configuring an AP with Internal DHCP server



Configure an AP with default WLAN group

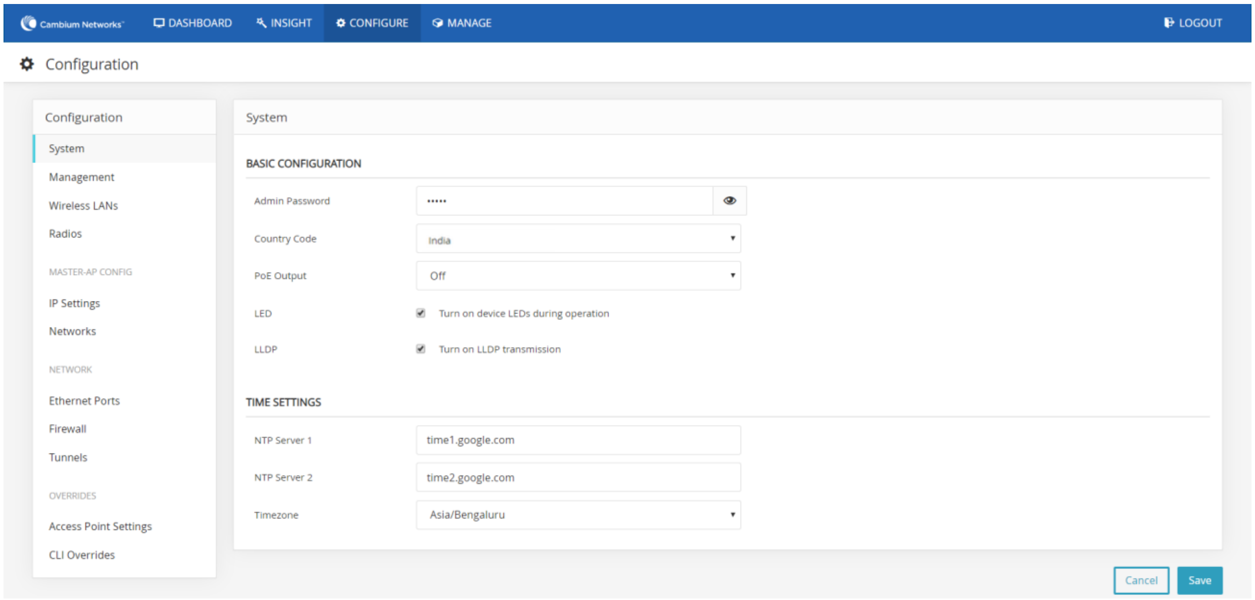
To configure an AP with default WLAN group:

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 85 Configure > Systems



System

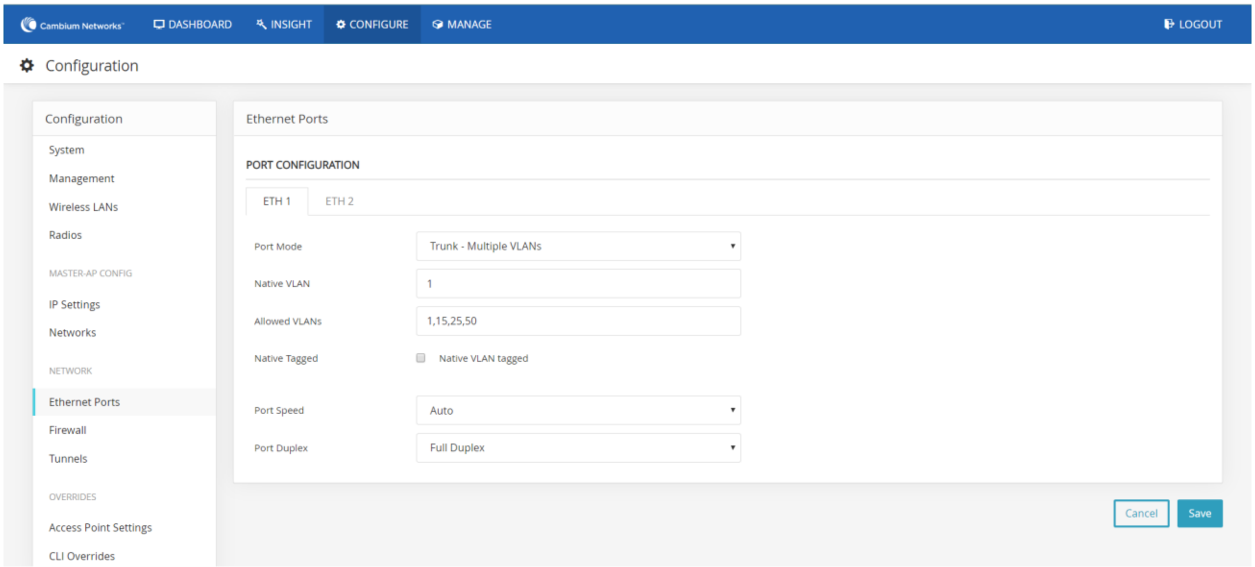
BASIC CONFIGURATION

Admin Password	•••••
Country Code	India
PoE Output	Off
LED	☑ Turn on device LEDs during operation
LLDP	☑ Turn on LLDP transmission

TIME SETTINGS

NTP Server 1	time1.google.com
NTP Server 2	time2.google.com
Timezone	Asia/Bengaluru

Figure 86 Configure > Ethernet Ports



Port Mode: Trunk - Multiple VLANs

Native VLAN: 1

Allowed VLANs: 1,15,25,50

Native Tagged: □ Native VLAN tagged

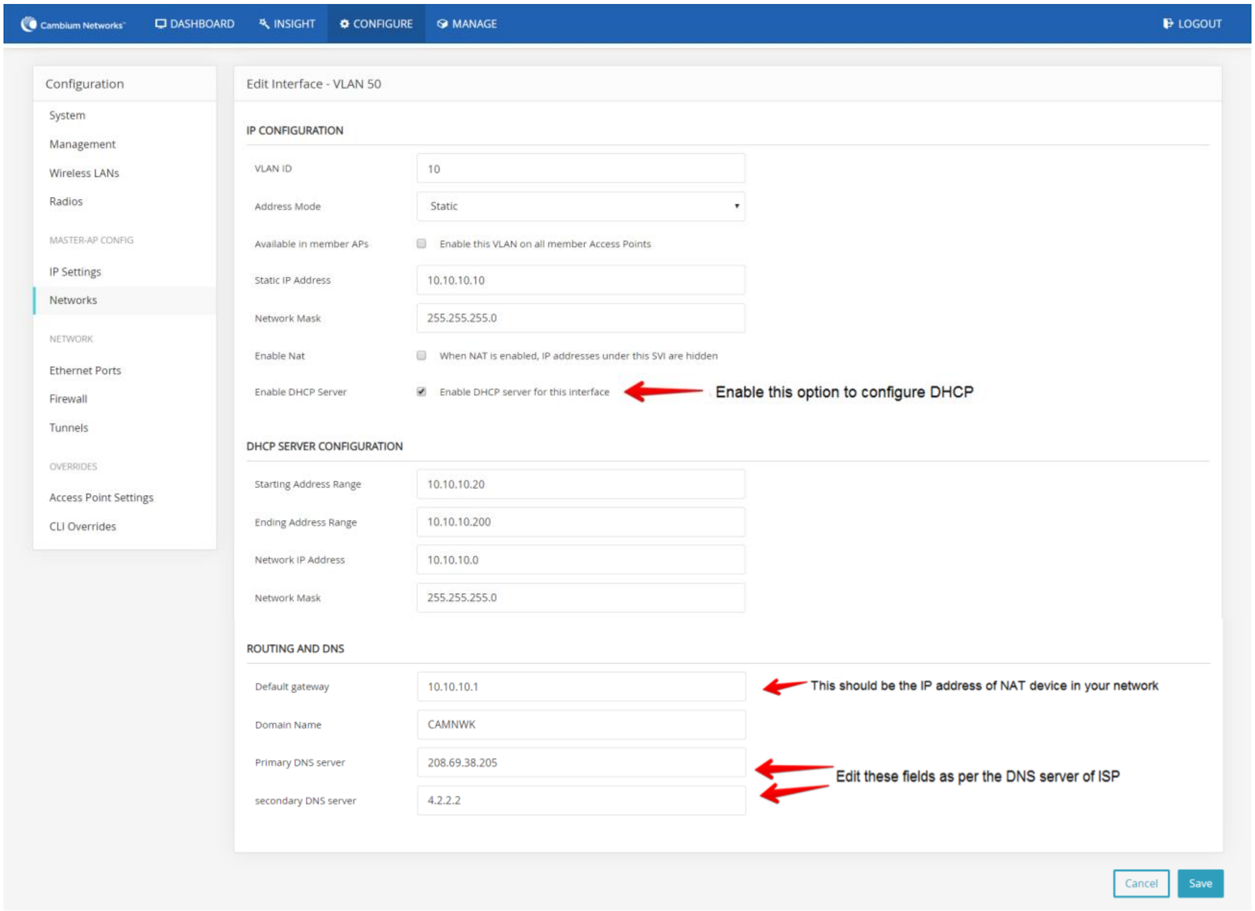
Port Speed: Auto

Port Duplex: Full Duplex

2. Go to CONFIGURE > MASTER AP CONFIG > Networks and configure the Static IP Address and the DHCP Server for VLAN 1 (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.

Figure 87 Configure > Networks



Edit Interface - VLAN 50

IP CONFIGURATION

VLAN ID	10
Address Mode	Static
Available in member APs	□ Enable this VLAN on all member Access Points
Static IP Address	10.10.10.10
Network Mask	255.255.255.0
Enable Nat	□ When NAT is enabled, IP addresses under this SVI are hidden
Enable DHCP Server	☑ Enable DHCP server for this interface

Enable this option to configure DHCP

DHCP SERVER CONFIGURATION

Starting Address Range	10.10.10.20
Ending Address Range	10.10.10.200
Network IP Address	10.10.10.0
Network Mask	255.255.255.0

ROUTING AND DNS

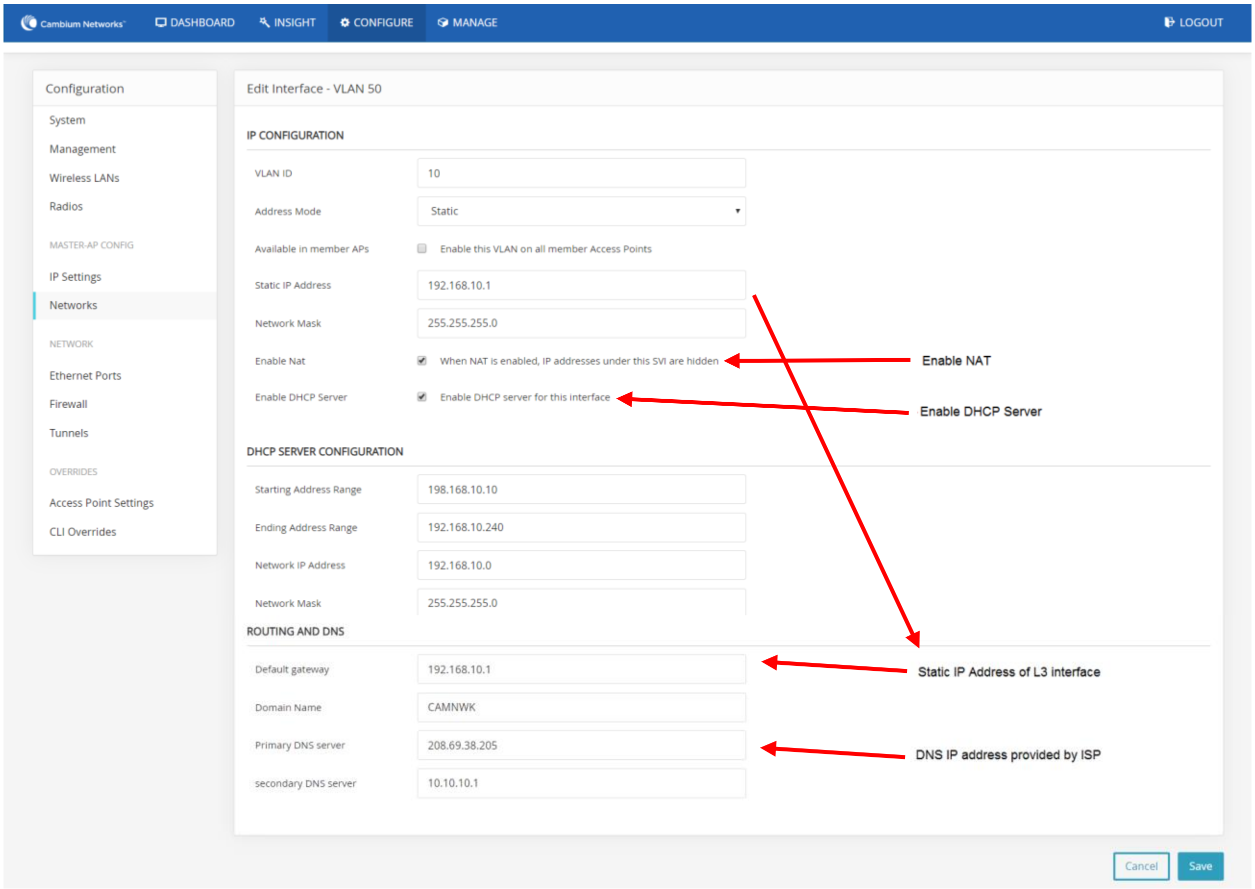
Default gateway	10.10.10.1
Domain Name	CAMNWK
Primary DNS server	208.69.38.205
secondary DNS server	4.2.2.2

This should be the IP address of NAT device in your network

Edit these fields as per the DNS server of ISP

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.

Figure 88 Configure > Networks > VLAN 10



Edit Interface - VLAN 50

IP CONFIGURATION

VLAN ID	10
Address Mode	Static
Available in member APs	☐ Enable this VLAN on all member Access Points
Static IP Address	192.168.10.1
Network Mask	255.255.255.0
Enable Nat	☑ When NAT is enabled, IP addresses under this SVI are hidden
Enable DHCP Server	☑ Enable DHCP server for this interface

DHCP SERVER CONFIGURATION

Starting Address Range	198.168.10.10
Ending Address Range	192.168.10.240
Network IP Address	192.168.10.0
Network Mask	255.255.255.0

ROUTING AND DNS

Default gateway	192.168.10.1
Domain Name	CAMNWK
Primary DNS server	208.69.38.205
secondary DNS server	10.10.10.1

Enable NAT

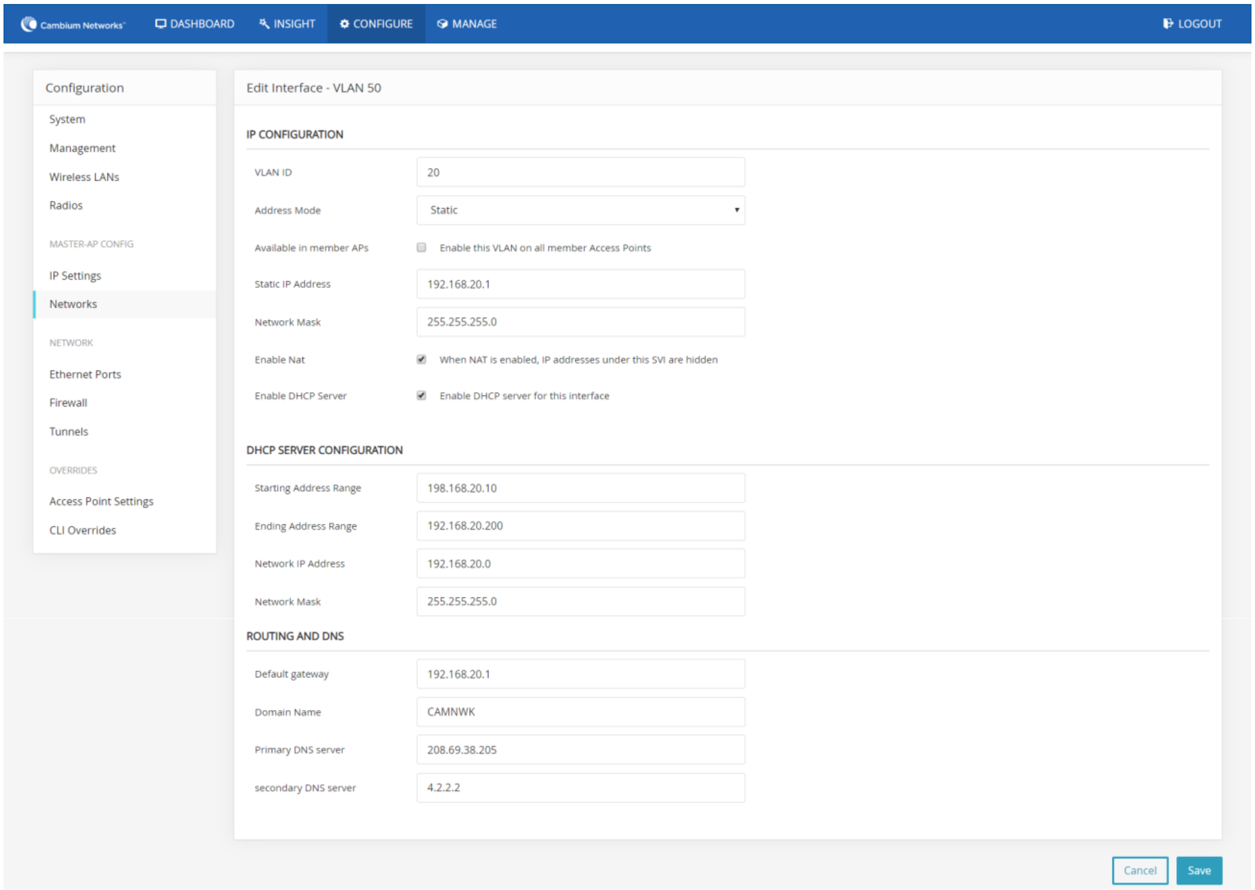
Enable DHCP Server

Static IP Address of L3 interface

DNS IP address provided by ISP

5. Add L3 interface of VLAN 20 and enable DHCP server and NAT as shown in Figure 89.

Figure 89 Configure > Networks > VLAN 20



Edit Interface - VLAN 50

IP CONFIGURATION

VLAN ID	20
Address Mode	Static ▾
Available in member APs	□ Enable this VLAN on all member Access Points
Static IP Address	192.168.20.1
Network Mask	255.255.255.0
Enable Nat	☑ When NAT is enabled, IP addresses under this SVI are hidden
Enable DHCP Server	☑ Enable DHCP server for this interface

DHCP SERVER CONFIGURATION

Starting Address Range	198.168.20.10
Ending Address Range	192.168.20.200
Network IP Address	192.168.20.0
Network Mask	255.255.255.0

ROUTING AND DNS

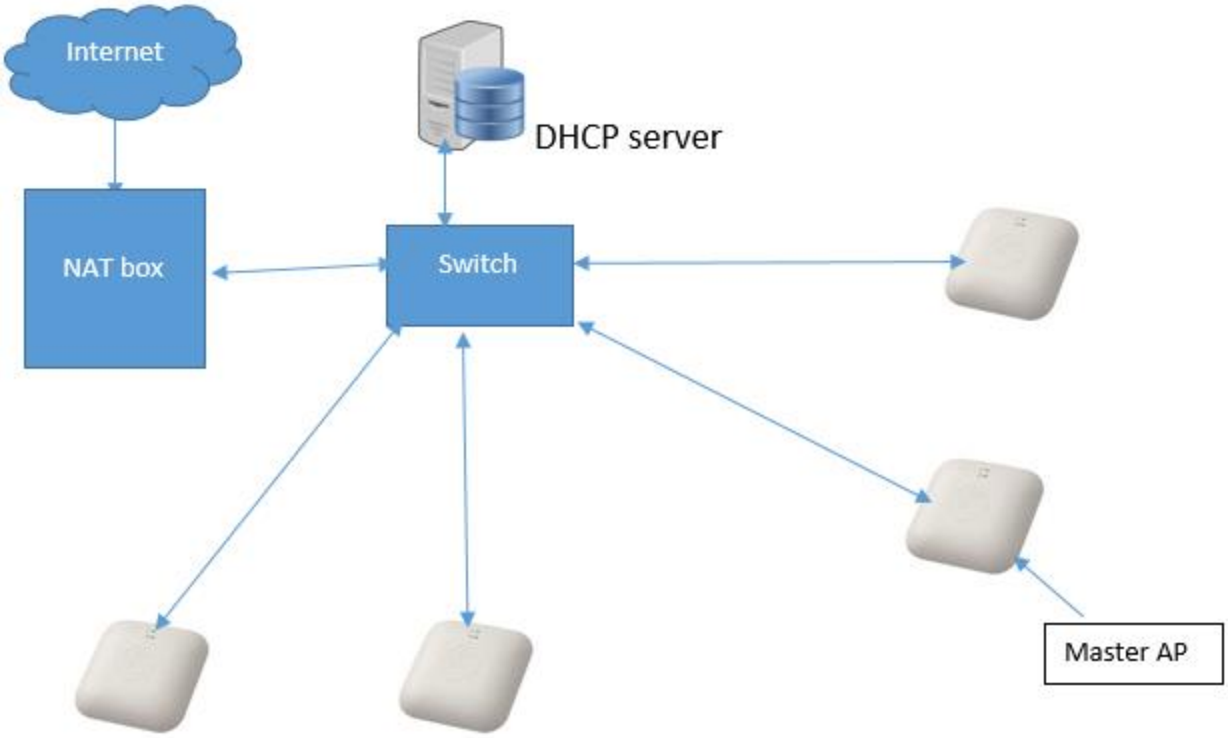
Default gateway	192.168.20.1
Domain Name	CAMNWK
Primary DNS server	208.69.38.205
secondary DNS server	4.2.2.2

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 90 Configuring an AP with External DHCP server

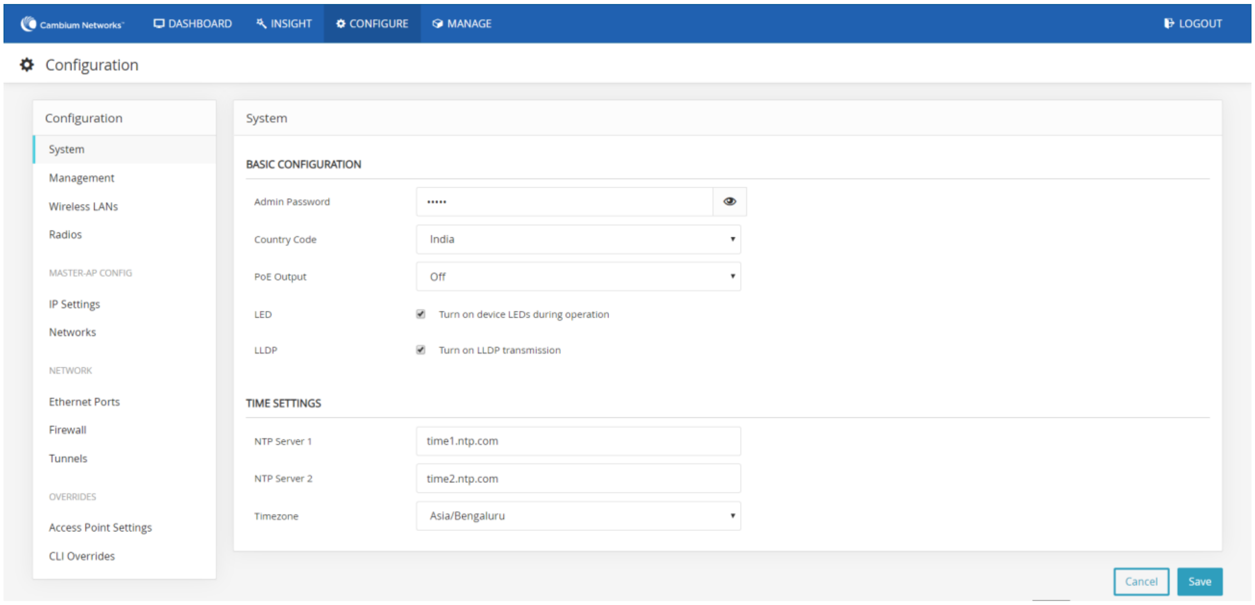


All the member APs are connected to ports of Switch. All the ports are mapped to VLAN 1.

To configure Master AP:

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

Figure 91 Configure > Systems



System

BASIC CONFIGURATION

Admin Password: •••••

Country Code: India

PoE Output: Off

LED: ☑ Turn on device LEDs during operation

LLDP: ☑ Turn on LLDP transmission

TIME SETTINGS

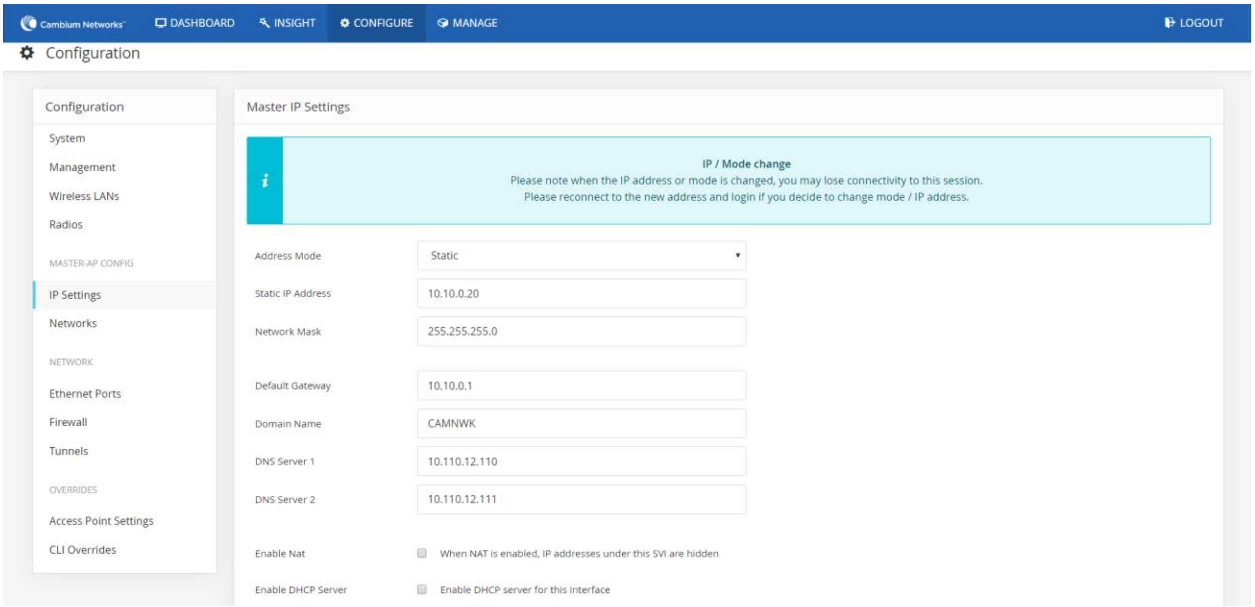
NTP Server 1: time1.ntp.com

NTP Server 2: time2.ntp.com

Timezone: Asia/Bengaluru

2. Configure static IP on Master.

Figure 92 Configure > IP Settings



Master IP Settings

IP / Mode change
Please note when the IP address or mode is changed, you may lose connectivity to this session.
Please reconnect to the new address and login if you decide to change mode / IP address.

Address Mode	Static
Static IP Address	10.10.0.20
Network Mask	255.255.255.0
Default Gateway	10.10.0.1
Domain Name	CAMNWK
DNS Server 1	10.110.12.110
DNS Server 2	10.110.12.111
Enable Nat	□ When NAT is enabled, IP addresses under this SVI are hidden
Enable DHCP Server	□ Enable DHCP server for this interface

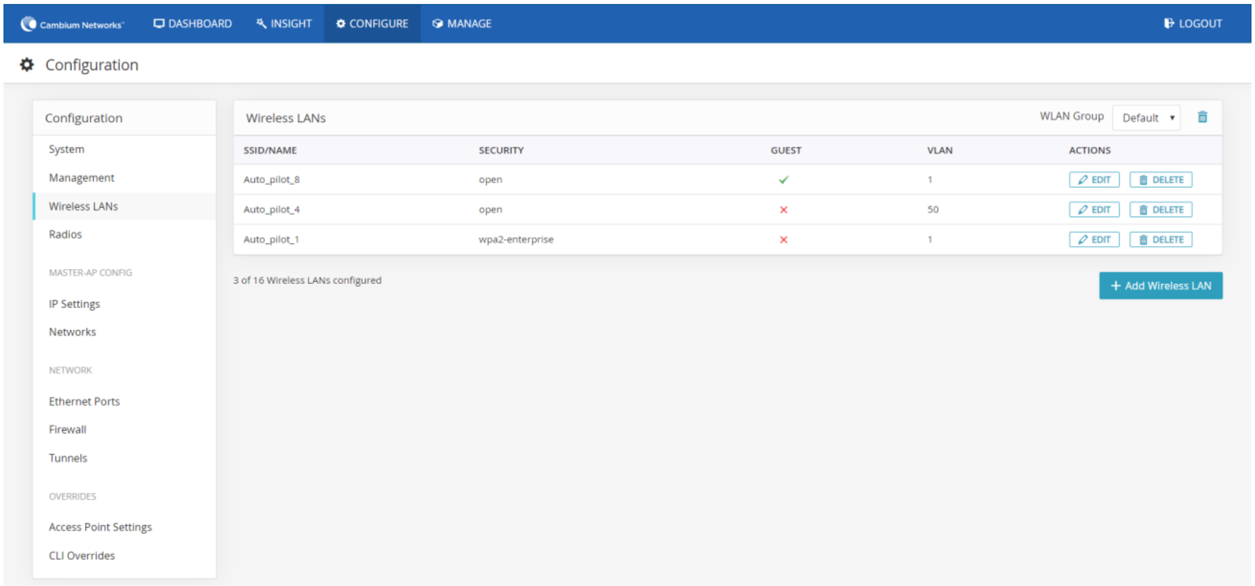
3. Refresh the page after saving with newly configured Ip address. In this example, open URL in browser http://10.10.10.25.

Configuring WLAN in default WLAN Group

To configure WLAN in default WLAN group:

1. Add a Wireless LAN.

Figure 93 Configure > Wireless LANs



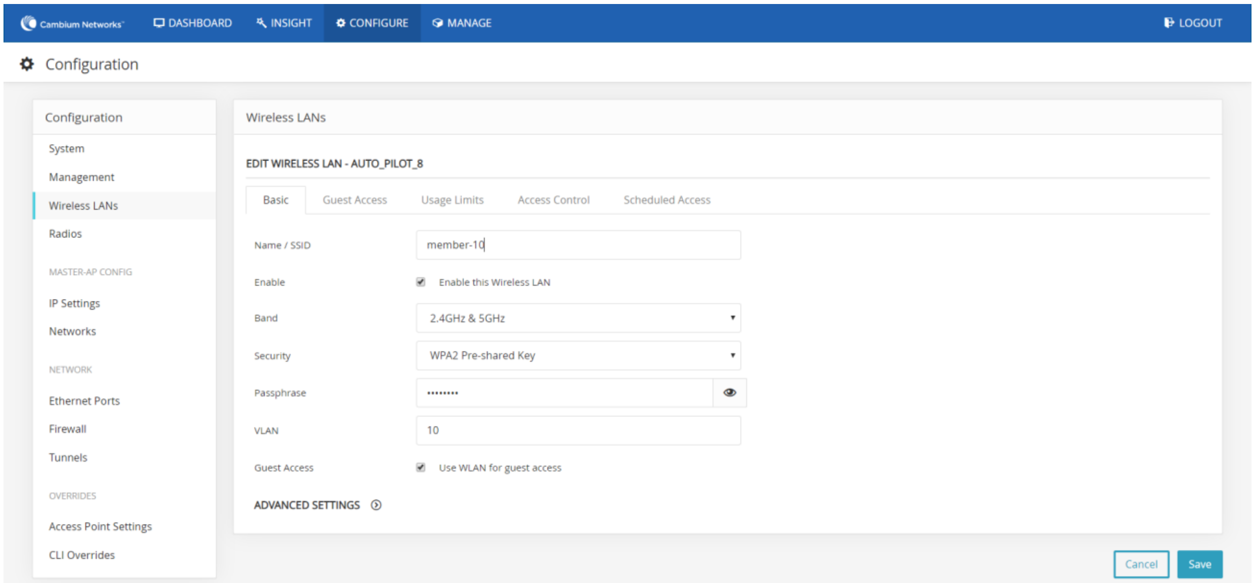
Wireless LANs WLAN Group Default

SSID/NAME	SECURITY	GUEST	VLAN	ACTIONS
Auto_pilot_8	open	✓	1	EDIT DELETE
Auto_pilot_4	open	✗	50	EDIT DELETE
Auto_pilot_1	wpa2-enterprise	✗	1	EDIT DELETE

3 of 16 Wireless LANs configured

2. Enter SSID and password in respective fields.
3. Configure VLAN as 10 and click Save.

Figure 94 Configure > Wireless LANs > VLAN 10



EDIT WIRELESS LAN - AUTO_PILOT_8

Name / SSID: member-10

Enable: ☑ Enable this Wireless LAN

Band: 2.4GHz & 5GHz

Security: WPA2 Pre-shared Key

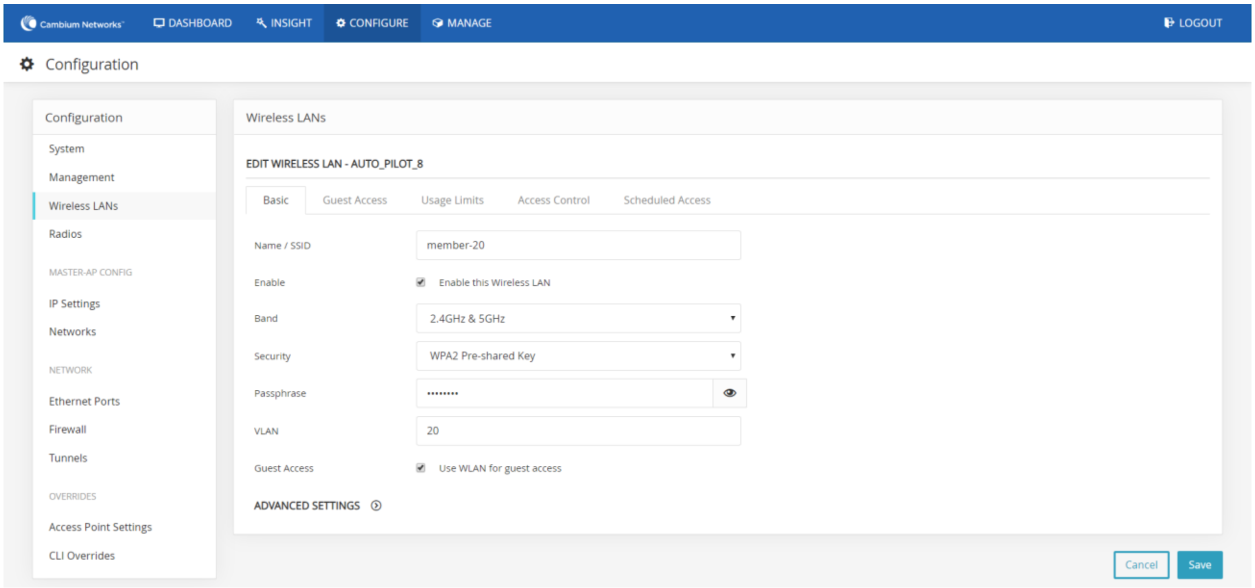
Passphrase: ••••••••

VLAN: 10

Guest Access: ☑ Use WLAN for guest access

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

Figure 95 Configure > Wireless LANs > VLAN 20



EDIT WIRELESS LAN - AUTO_PILOT_8

Name / SSID: member-20

Enable: ☑ Enable this Wireless LAN

Band: 2.4GHz & 5GHz

Security: WPA2 Pre-shared Key

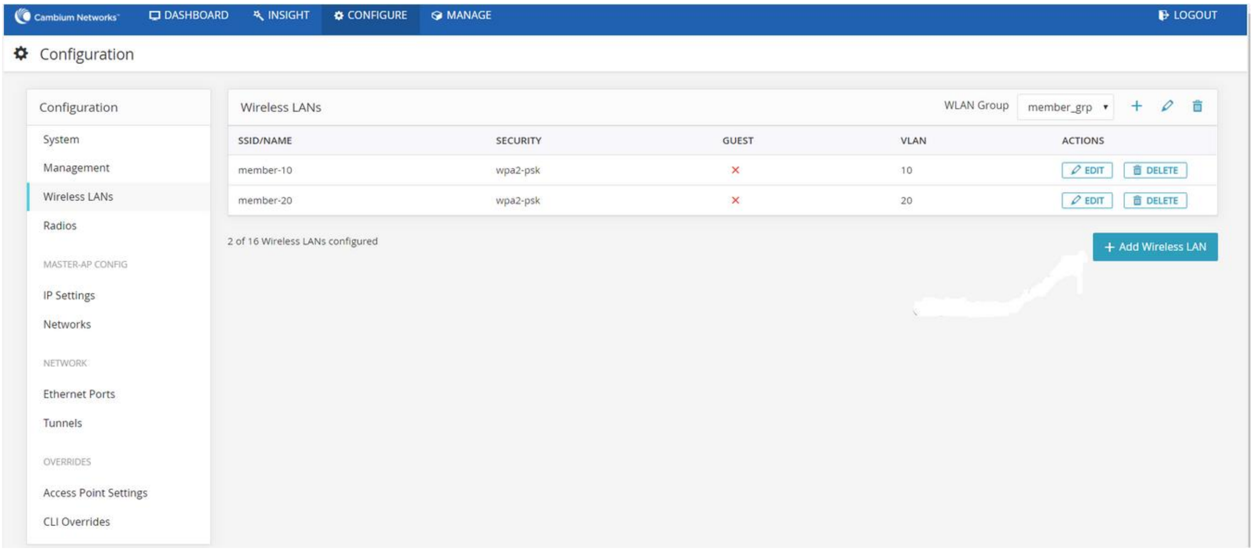
Passphrase: ••••••••

VLAN: 20

Guest Access: ☑ Use WLAN for guest access

6. Check the configured WLANs.

Figure 96 Configure > Wireless LANs > VLAN 10 and 20

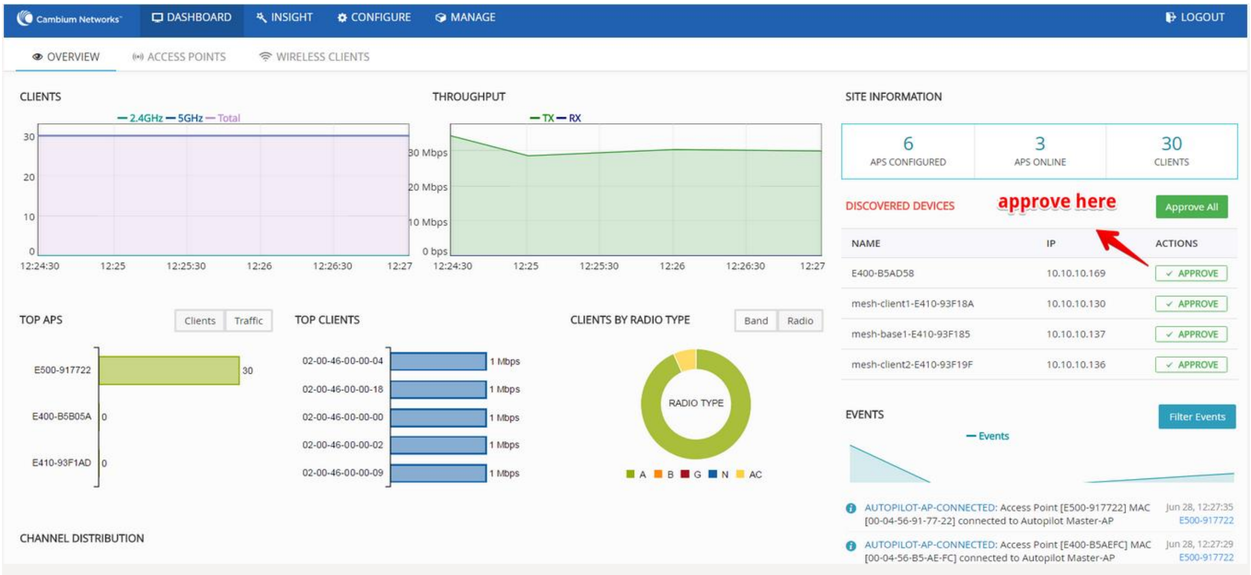


SSID/NAME	SECURITY	GUEST	VLAN	ACTIONS
member-10	wpa2-psk	✗	10	EDIT DELETE
member-20	wpa2-psk	✗	20	EDIT DELETE

2 of 16 Wireless LANs configured

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 97 Dashboard



6	3	30
APS CONFIGURED	APS ONLINE	CLIENTS

DISCOVERED DEVICES

NAME	IP	ACTIONS
E400-B5AD58	10.10.10.169	✓ APPROVE
mesh-client1-E410-93F18A	10.10.10.130	✓ APPROVE
mesh-base1-E410-93F185	10.10.10.137	✓ APPROVE
mesh-client2-E410-93F19F	10.10.10.136	✓ APPROVE

AUTOPILOT-AP-CONNECTED: Access Point [E500-917722] MAC [00-04-56-91-77-22] connected to Autopilot Master-AP — Jun 28, 12:27:35 E500-917722

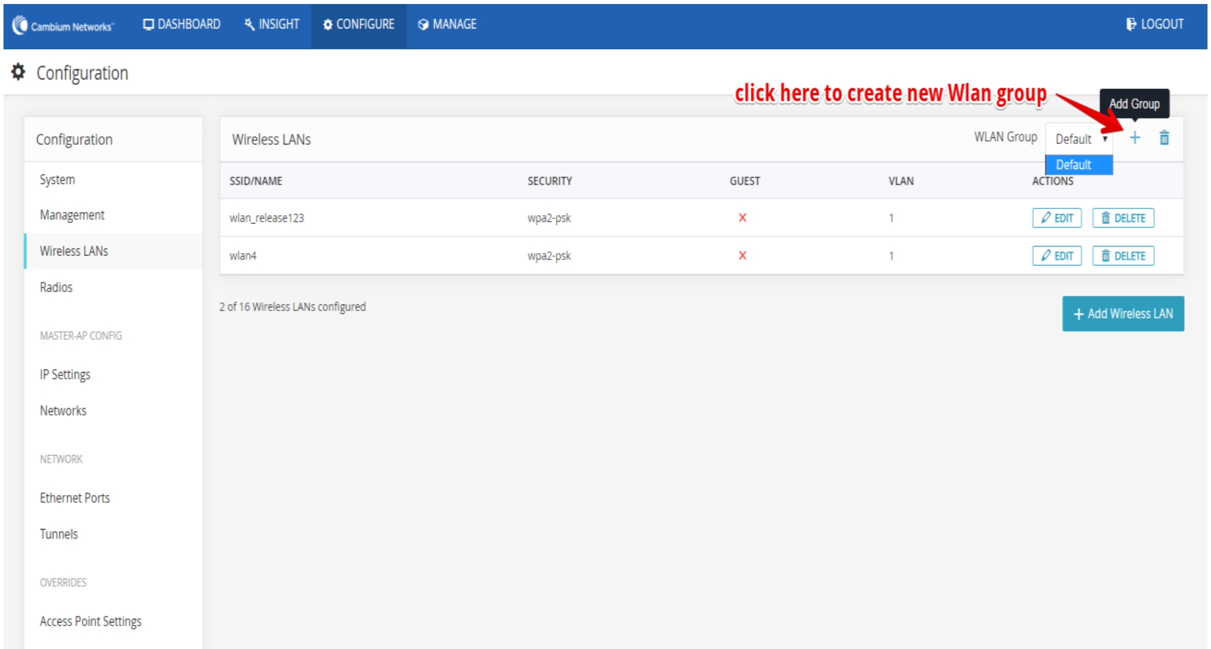
AUTOPILOT-AP-CONNECTED: Access Point [E400-B5AEFC] MAC [00-04-56-B5-AE-FC] connected to Autopilot Master-AP — Jun 28, 12:27:29 E500-917722

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.

Figure 98 Create a WLAN group



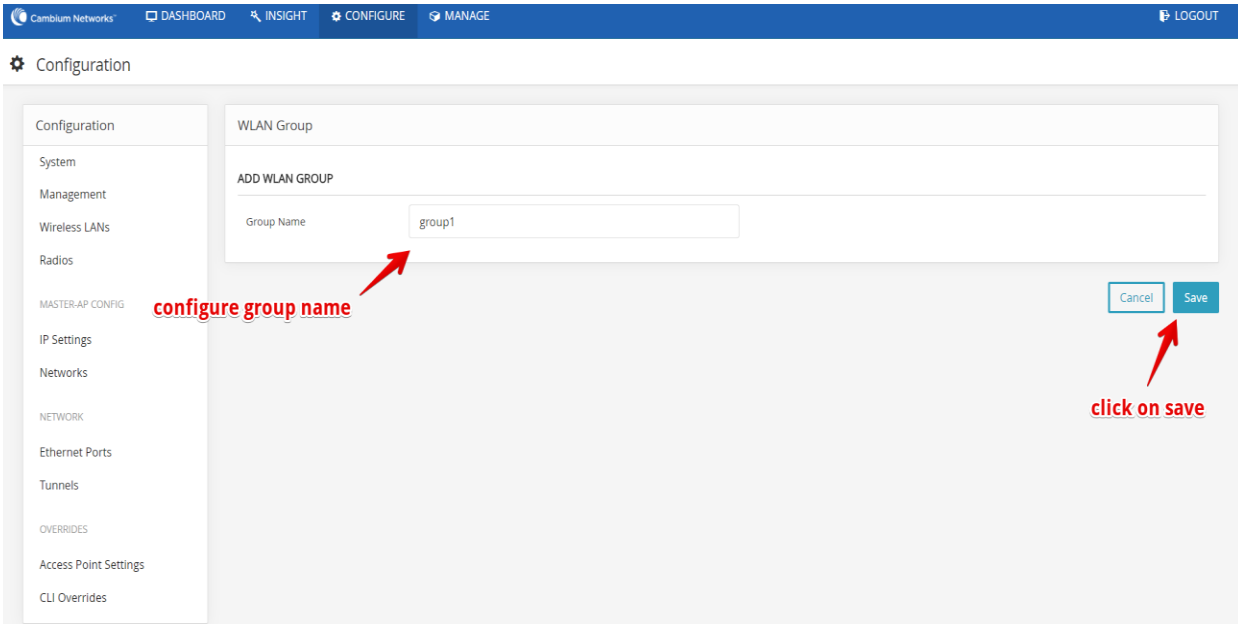
click here to create new Wlan group

SSID/NAME	SECURITY	GUEST	VLAN	ACTIONS
wlan_release123	wpa2-psk	✗	1	EDIT DELETE
wlan4	wpa2-psk	✗	1	EDIT DELETE

2 of 16 Wireless LANs configured

2. Configure a new WLAN Group.

Figure 99 Configure a new WLAN Group



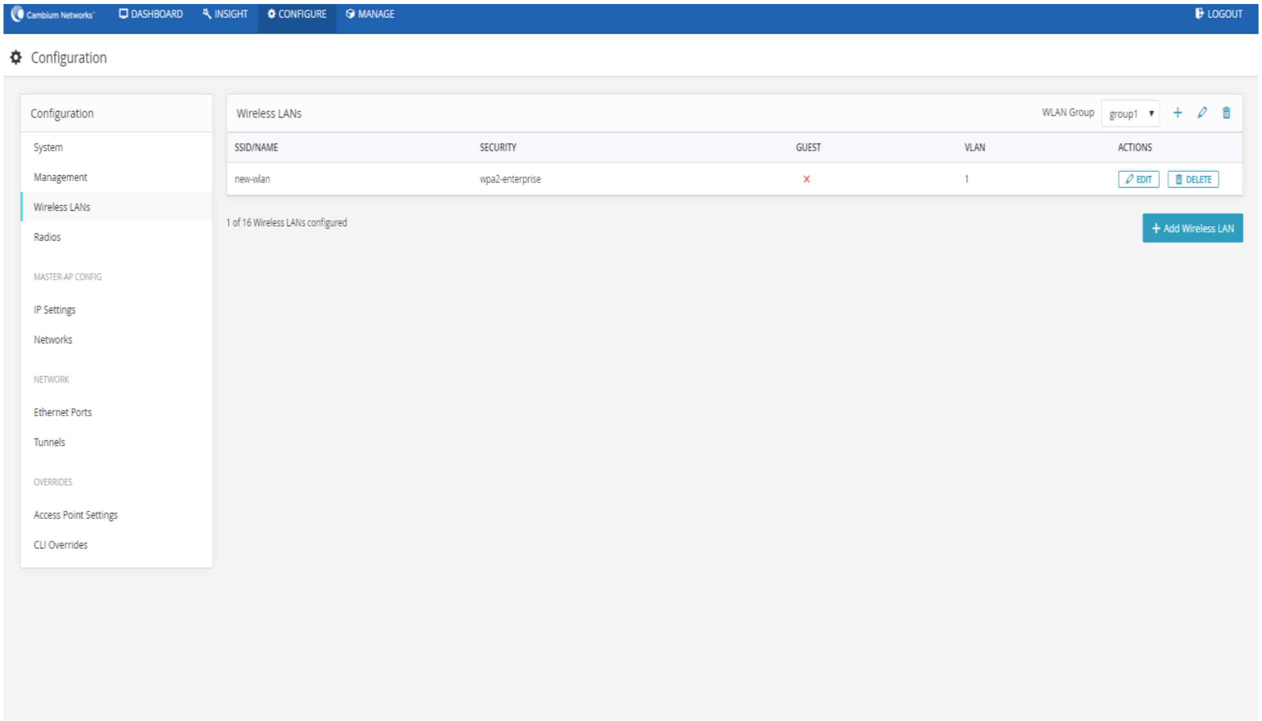
Group Name: group1

configure group name

click on save

3. Configure WLAN under the newly created WLAN Group.

Figure 100 Configure WLAN under the newly created WLAN Group



SSID/NAME	SECURITY	GUEST	VLAN	ACTIONS
new-wlan	wpa2-enterprise	✗	1	EDIT DELETE

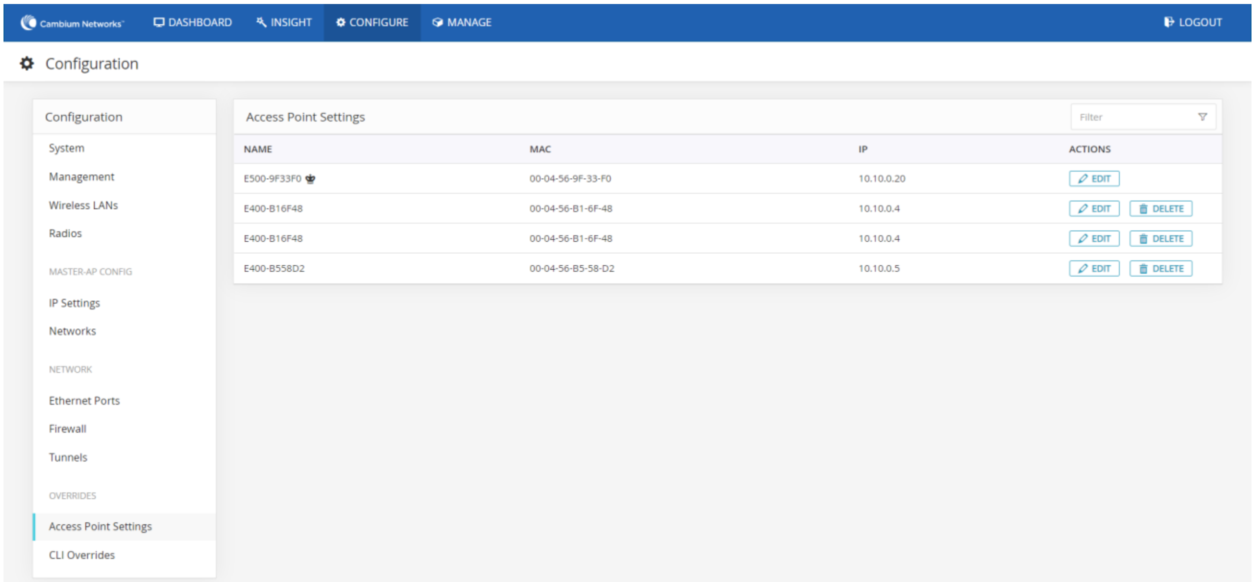
1 of 16 Wireless LANs configured

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.

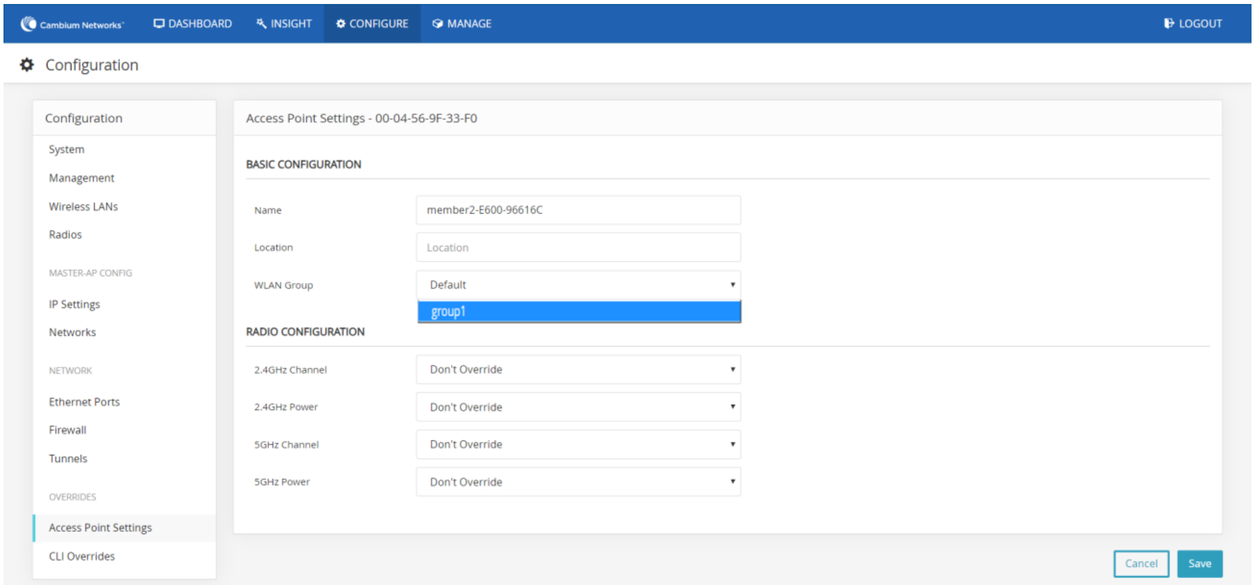
Figure 101 Configure > Access Point settings



NAME	MAC	IP	ACTIONS
E500-9F33F0 ♚	00-04-56-9F-33-F0	10.10.0.20	EDIT
E400-B16F48	00-04-56-B1-6F-48	10.10.0.4	EDIT DELETE
E400-B16F48	00-04-56-B1-6F-48	10.10.0.4	EDIT DELETE
E400-B558D2	00-04-56-B5-58-D2	10.10.0.5	EDIT DELETE

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.

Figure 102 Configure > Access Point settings > WLAN Group



Access Point Settings - 00-04-56-9F-33-F0

BASIC CONFIGURATION

Name	member2-E600-96616C
Location	Location
WLAN Group	Default group1

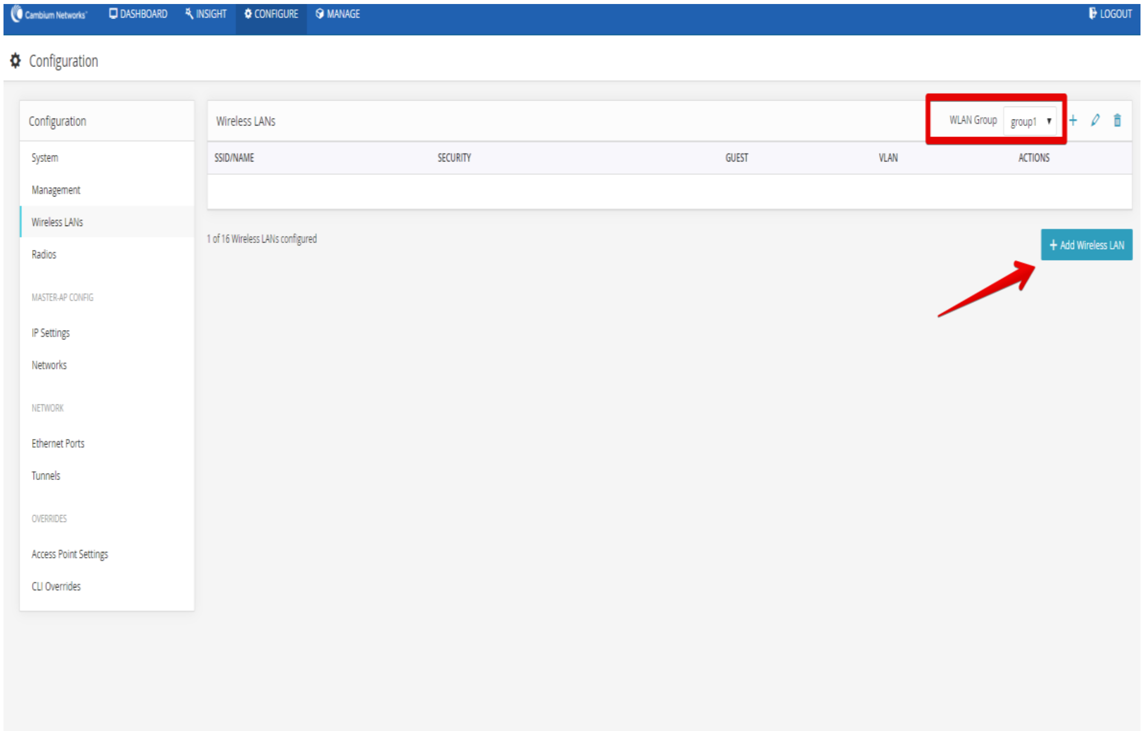
RADIO CONFIGURATION

2.4GHz Channel	Don't Override
2.4GHz Power	Don't Override
5GHz Channel	Don't Override
5GHz Power	Don't Override

Configuring WPA2-Enterprise WLAN

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

Figure 103 Configure > Access Point settings > user created WLAN Group



Wireless LANs — WLAN Group: group1

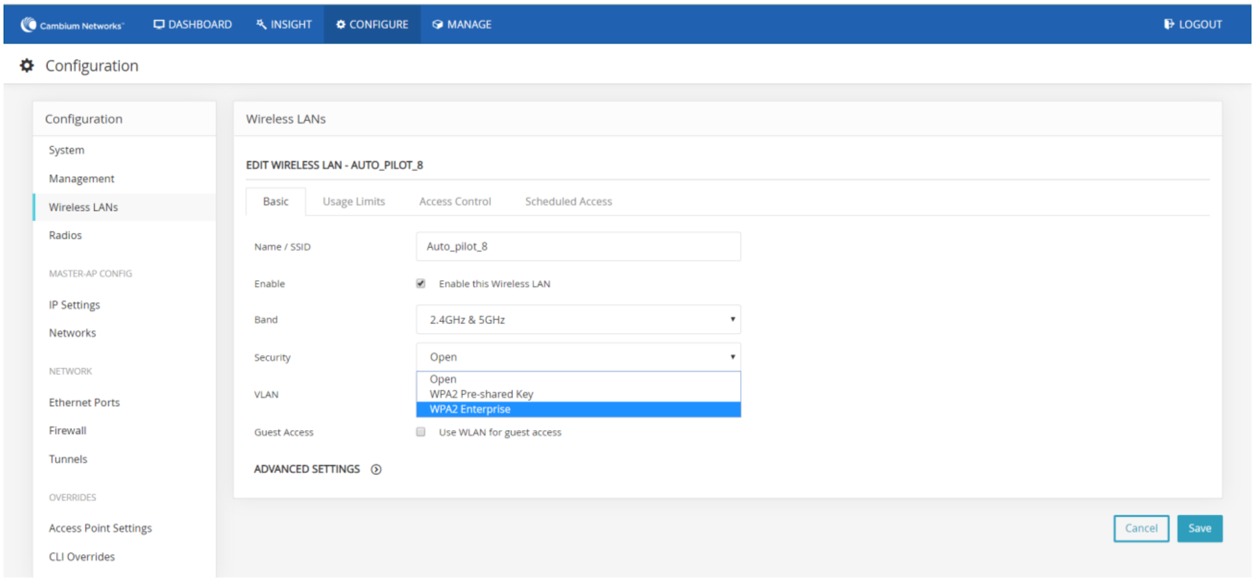
SSID/NAME	SECURITY	GUEST	VLAN	ACTIONS

1 of 16 Wireless LANs configured

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.

Figure 104 Configure > Wireless LANs > Security



EDIT WIRELESS LAN - AUTO_PILOT_8

Name / SSID: Auto_pilot_8

Enable: ☑ Enable this Wireless LAN

Band: 2.4GHz & 5GHz

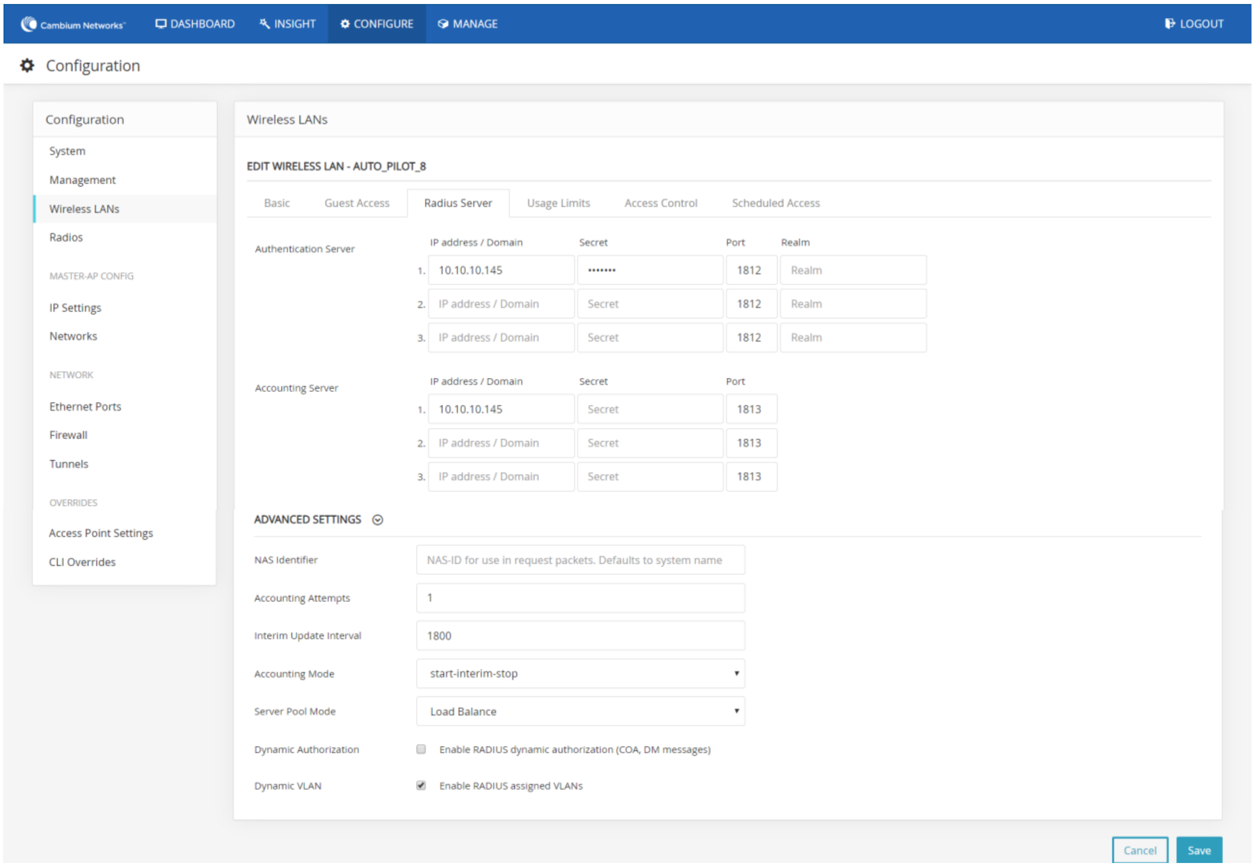
Security: Open
- Open
- WPA2 Pre-shared Key
- WPA2 Enterprise

VLAN

Guest Access: □ Use WLAN for guest access

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

Figure 105 Configure > Wireless LANs > Radius Server



EDIT WIRELESS LAN - AUTO_PILOT_8

		IP address / Domain	Secret	Port	Realm
Authentication Server	1.	10.10.10.145	•••••••	1812	Realm
	2.	IP address / Domain	Secret	1812	Realm
	3.	IP address / Domain	Secret	1812	Realm

		IP address / Domain	Secret	Port
Accounting Server	1.	10.10.10.145	Secret	1813
	2.	IP address / Domain	Secret	1813
	3.	IP address / Domain	Secret	1813

ADVANCED SETTINGS

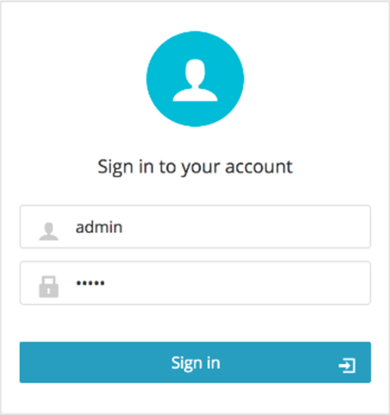
NAS Identifier	NAS-ID for use in request packets. Defaults to system name
Accounting Attempts	1
Interim Update Interval	1800
Accounting Mode	start-interim-stop
Server Pool Mode	Load Balance
Dynamic Authorization	□ Enable RADIUS dynamic authorization (COA, DM messages)
Dynamic VLAN	☑ Enable RADIUS assigned VLANs

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 106 Login page



admin

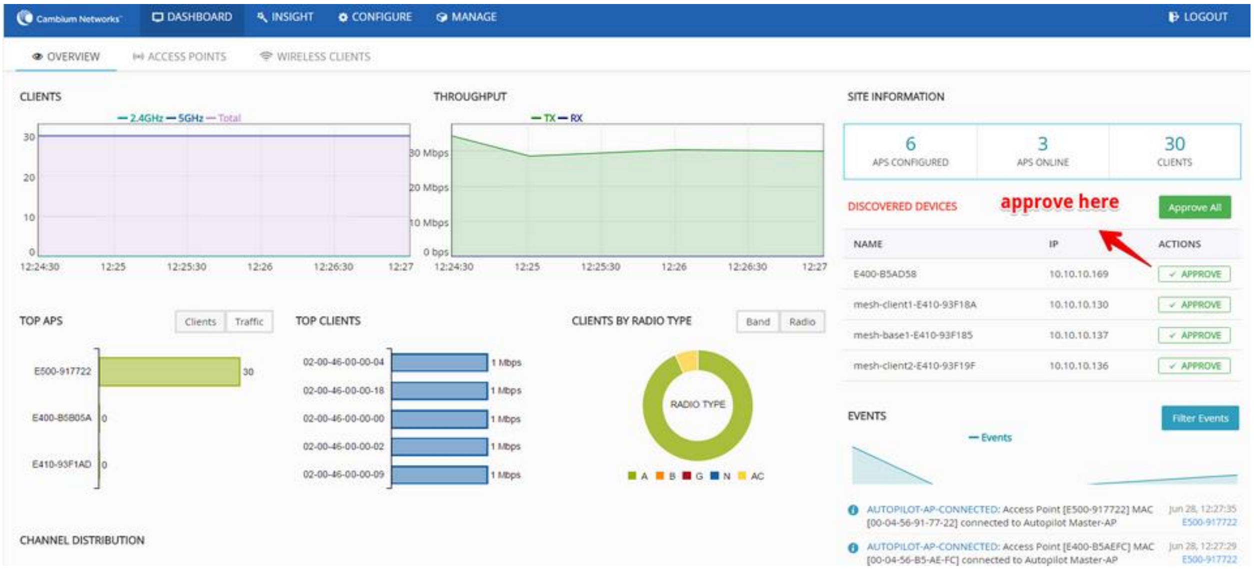
•••••

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

> Note The member AP needs to be upgraded with autopilot firmware.

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

Figure 107 Dashboard > Overview



DISCOVERED DEVICES

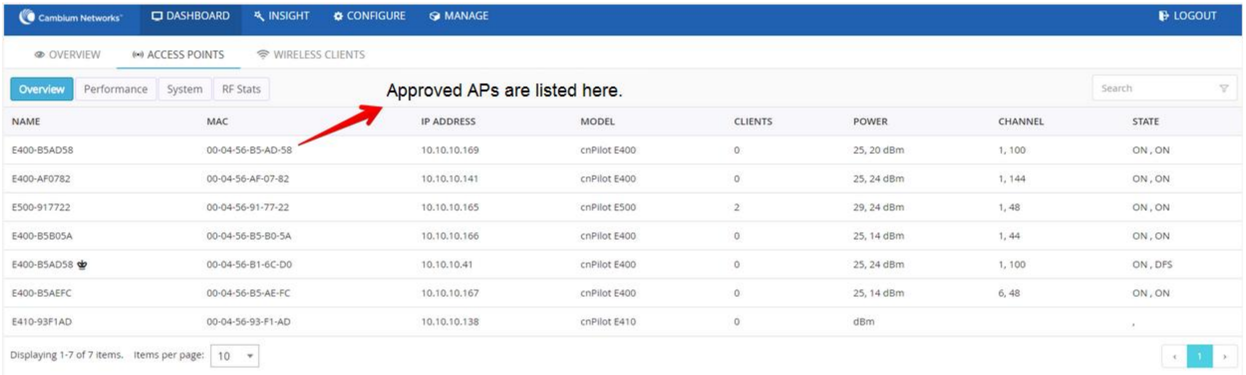
NAME	IP	ACTIONS
E400-B5AD58	10.10.10.169	✓ APPROVE
mesh-client1-E410-93F18A	10.10.10.130	✓ APPROVE
mesh-base1-E410-93F185	10.10.10.137	✓ APPROVE
mesh-client2-E410-93F19F	10.10.10.136	✓ APPROVE

AUTOPILOT-AP-CONNECTED: Access Point [E500-917722] MAC [00-04-56-91-77-22] connected to Autopilot Master-AP — Jun 28, 12:27:35 E500-917722

AUTOPILOT-AP-CONNECTED: Access Point [E400-B5AEFC] MAC [00-04-56-B5-AE-FC] connected to Autopilot Master-AP — Jun 28, 12:27:29 E500-917722

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

Figure 108 Dashboard > Access points



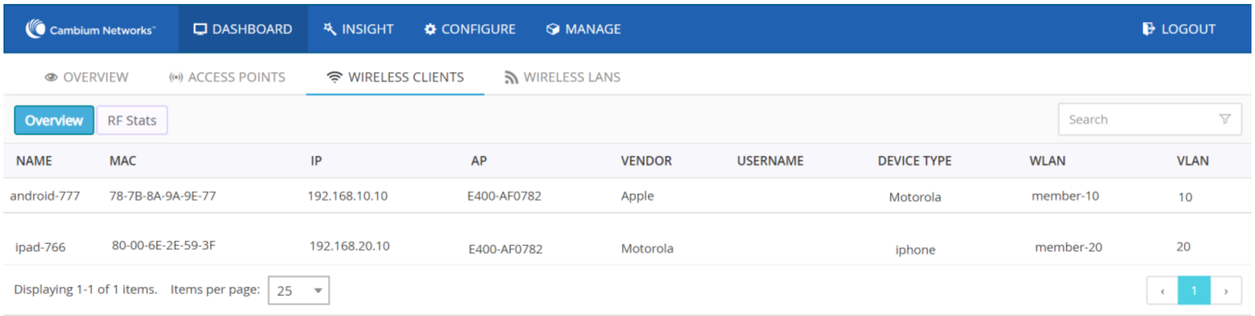
NAME	MAC	IP ADDRESS	MODEL	CLIENTS	POWER	CHANNEL	STATE
E400-B5AD58	00-04-56-B5-AD-58	10.10.10.169	cnPilot E400	0	25, 20 dBm	1, 100	ON , ON
E400-AF0782	00-04-56-AF-07-82	10.10.10.141	cnPilot E400	0	25, 24 dBm	1, 144	ON , ON
E500-917722	00-04-56-91-77-22	10.10.10.165	cnPilot E500	2	29, 24 dBm	1, 48	ON , ON
E400-B5B05A	00-04-56-B5-B0-5A	10.10.10.166	cnPilot E400	0	25, 14 dBm	1, 44	ON , ON
E400-B5AD58 ♚	00-04-56-B1-6C-D0	10.10.10.41	cnPilot E400	0	25, 24 dBm	1, 100	ON , DFS
E400-B5AEFC	00-04-56-B5-AE-FC	10.10.10.167	cnPilot E400	0	25, 14 dBm	6, 48	ON , ON
E410-93F1AD	00-04-56-93-F1-AD	10.10.10.138	cnPilot E410	0	dBm		,

Displaying 1-7 of 7 items. Items per page: 10

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 109 Dashboard > Wireless clients



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

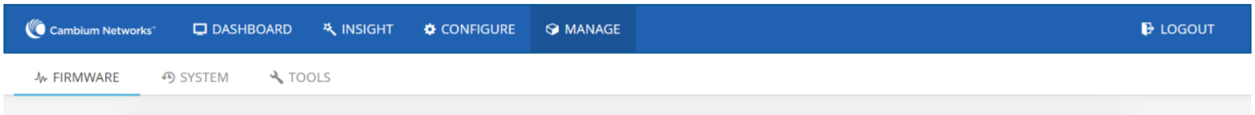
Displaying 1-1 of 1 items. Items per page: 25

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 110 Manage > Firmware



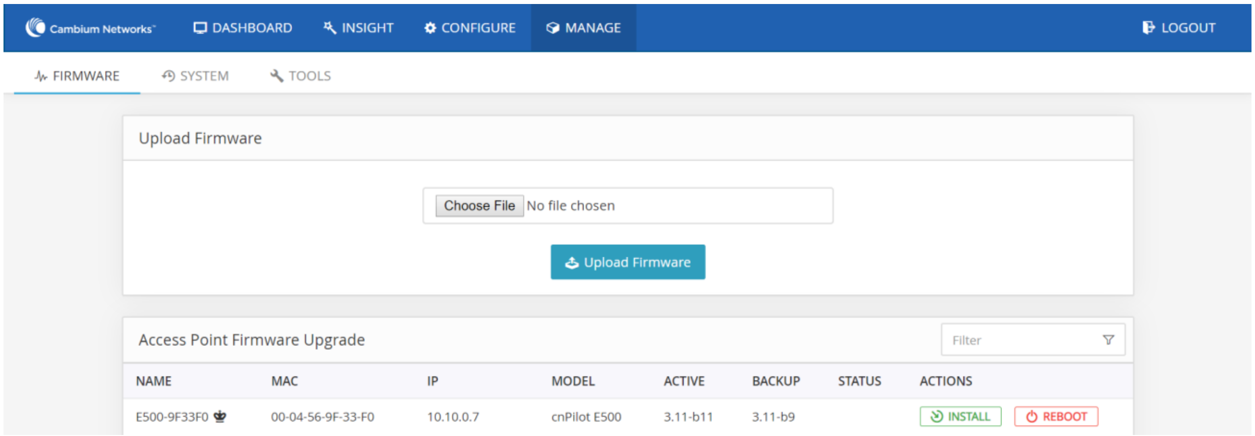
Firmware

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.

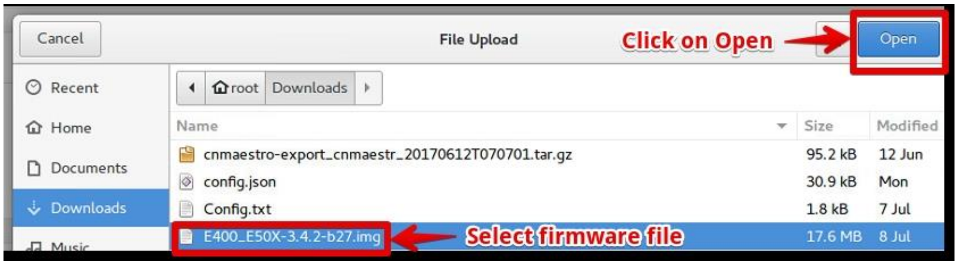
Figure 111 Manage > Upload Firmware



NAME	MAC	IP	MODEL	ACTIVE	BACKUP	STATUS	ACTIONS
E500-9F33F0	00-04-56-9F-33-F0	10.10.0.7	cnPilot E500	3.11-b11	3.11-b9		INSTALL REBOOT

3. Select the required firmware file and click Open. For example, firmware file: E400_E50X-3.4.2-b27.img.

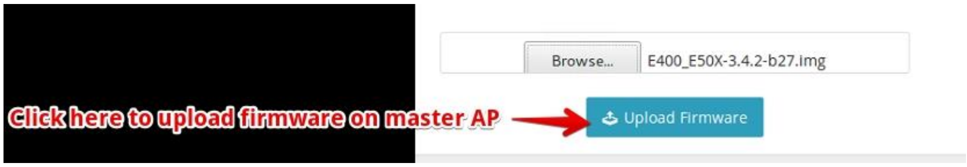
Figure 112 To open required Firmware



Name	Size	Modified
cnmaestro-export_cnmaestr_20170612T070701.tar.gz	95.2 kB	12 Jun
config.json	30.9 kB	Mon
Config.txt	1.8 kB	7 Jul
E400_E50X-3.4.2-b27.img	17.6 MB	8 Jul

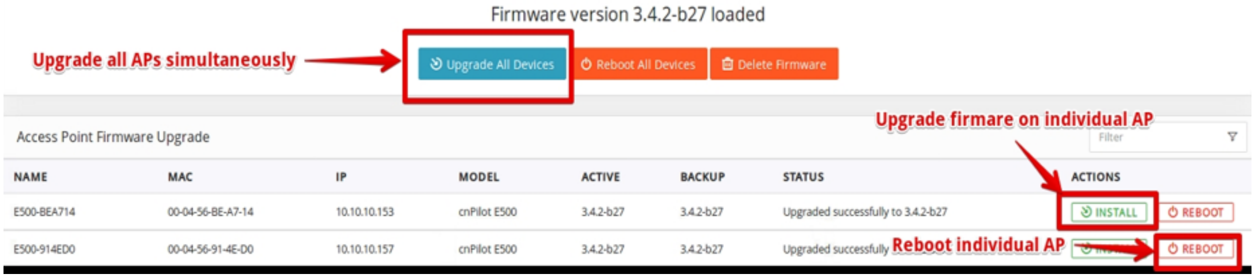
4. Click Upload Firmware button and wait for upload.

Figure 113 Upload firmware on Master AP



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.

Figure 114 To upgrade firmware in all devices

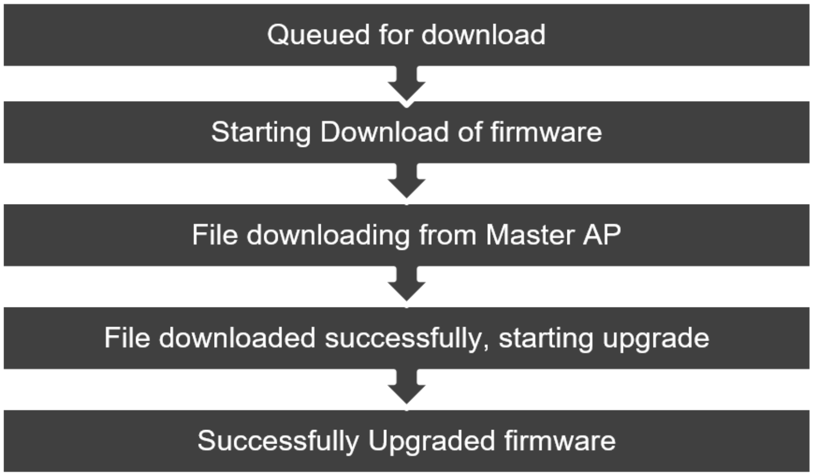

Firmware version 3.4.2-b27 loaded
Upgrade all APs simultaneously
Upgrade All Devices
Reboot All Devices
Delete Firmware
Upgrade firmare on individual AP
Filter
Reboot individual AP

Access Point Firmware Upgrade

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	INSTALL 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

Once step 5 is done, the following statuses during the Firmware upgrade can be seen in Figure 115.

Figure 115 Firmware upgraded sequence



Queued for download

Starting Download of firmware

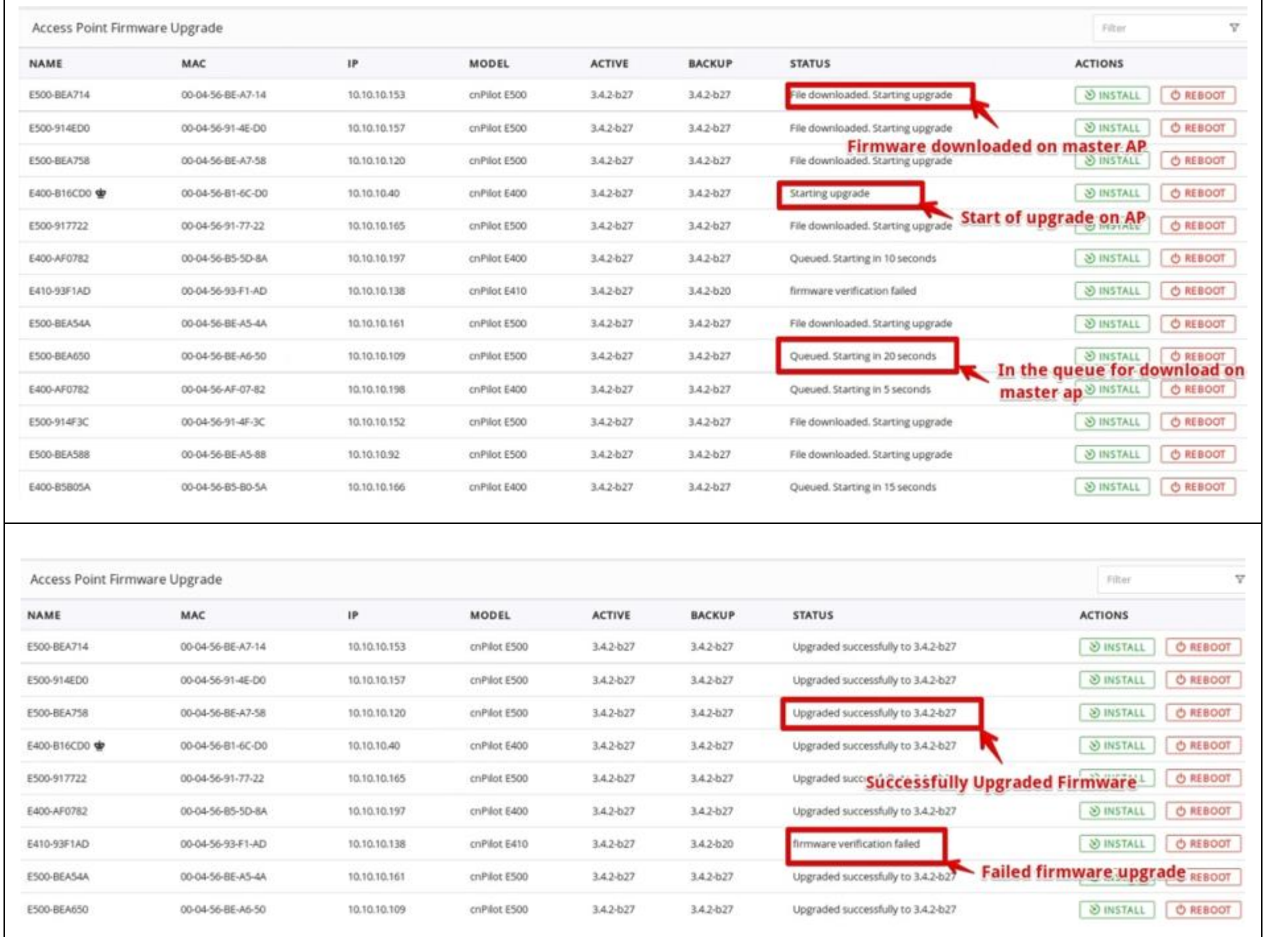
File downloading from Master AP

File downloaded successfully, starting upgrade

Successfully Upgraded firmware

6. Different statuses of the firmware upgrade can be seen in Figure 116.

Figure 116 Firmware upgraded status



Access Point Firmware Upgrade

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	File downloaded. Starting upgrade	INSTALL REBOOT
E500-914ED0	00-04-56-91-4E-D0	10.10.10.157	cnPilot E500	3.4.2-b27	3.4.2-b27	File downloaded. Starting upgrade	INSTALL REBOOT
E500-BEA758	00-04-56-BE-A7-58	10.10.10.120	cnPilot E500	3.4.2-b27	3.4.2-b27	File downloaded. Starting upgrade	INSTALL REBOOT
E400-B16CD0 ♛	00-04-56-B1-6C-D0	10.10.10.40	cnPilot E400	3.4.2-b27	3.4.2-b27	Starting upgrade	INSTALL REBOOT
E500-917722	00-04-56-91-77-22	10.10.10.165	cnPilot E500	3.4.2-b27	3.4.2-b27	File downloaded. Starting upgrade	INSTALL REBOOT
E400-AF0782	00-04-56-B5-5D-8A	10.10.10.197	cnPilot E400	3.4.2-b27	3.4.2-b27	Queued. Starting in 10 seconds	INSTALL REBOOT
E410-93F1AD	00-04-56-93-F1-AD	10.10.10.138	cnPilot E410	3.4.2-b27	3.4.2-b20	firmware verification failed	INSTALL REBOOT
E500-BEA54A	00-04-56-BE-A5-4A	10.10.10.161	cnPilot E500	3.4.2-b27	3.4.2-b27	File downloaded. Starting upgrade	INSTALL REBOOT
E500-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	INSTALL REBOOT
E400-AF0782	00-04-56-AF-07-82	10.10.10.198	cnPilot E400	3.4.2-b27	3.4.2-b27	Queued. Starting in 5 seconds	INSTALL REBOOT
E500-914F3C	00-04-56-91-4F-3C	10.10.10.152	cnPilot E500	3.4.2-b27	3.4.2-b27	File downloaded. Starting upgrade	INSTALL REBOOT
E500-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 REBOOT
E400-B5B05A	00-04-56-B5-B0-5A	10.10.10.166	cnPilot E400	3.4.2-b27	3.4.2-b27	Queued. Starting in 15 seconds	INSTALL REBOOT

Firmware downloaded on master AP

Start of upgrade on AP

In the queue for download on master ap

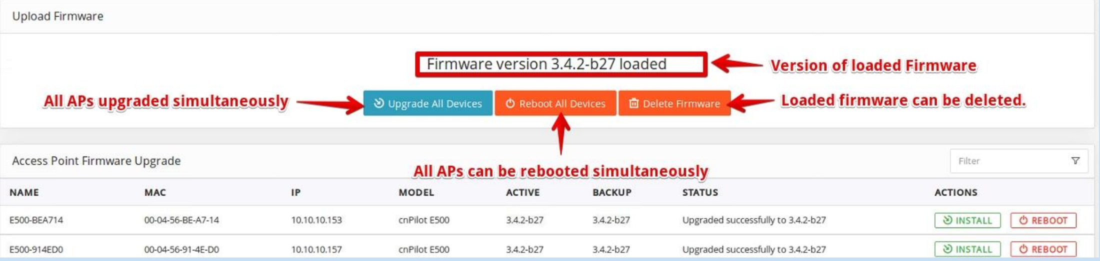
Access Point Firmware Upgrade

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	INSTALL 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 to 3.4.2-b27	INSTALL REBOOT
E500-BEA758	00-04-56-BE-A7-58	10.10.10.120	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	INSTALL REBOOT
E400-B16CD0 ♛	00-04-56-B1-6C-D0	10.10.10.40	cnPilot E400	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	INSTALL REBOOT
E500-917722	00-04-56-91-77-22	10.10.10.165	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded succ	INSTALL REBOOT
E400-AF0782	00-04-56-B5-5D-8A	10.10.10.197	cnPilot E400	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	INSTALL REBOOT
E410-93F1AD	00-04-56-93-F1-AD	10.10.10.138	cnPilot E410	3.4.2-b27	3.4.2-b20	firmware verification failed	INSTALL REBOOT
E500-BEA54A	00-04-56-BE-A5-4A	10.10.10.161	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	REBOOT
E500-BEA650	00-04-56-BE-A6-50	10.10.10.109	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	INSTALL REBOOT

Successfully Upgraded Firmware

Failed firmware upgrade

> 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.



Firmware version 3.4.2-b27 loaded

Version of loaded Firmware

All APs upgraded simultaneously

Loaded firmware can be deleted.

All APs can be rebooted simultaneously

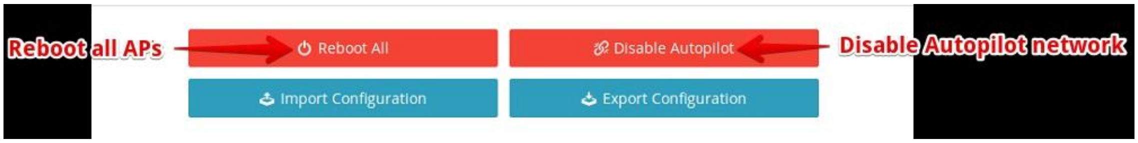
NAME	MAC	IP	MODEL	ACTIVE	BACKUP	STATUS	ACTIONS
E500-BEA714	00-04-56-BE-A7-14	10.10.10.153	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	INSTALL REBOOT
E500-914ED0	00-04-56-91-4E-D0	10.10.10.157	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded successfully to 3.4.2-b27	INSTALL REBOOT

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 117 System

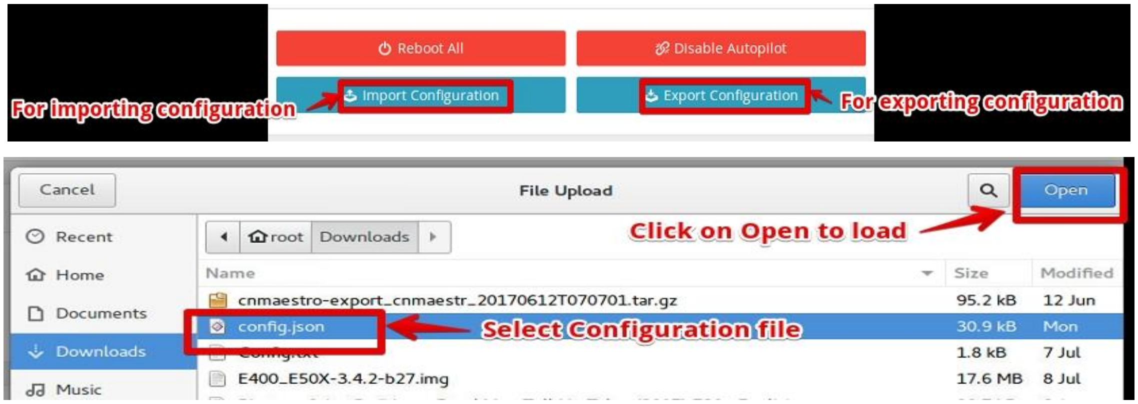


Reboot all APs

Disable Autopilot network

- 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 118 System > Import/Export Configuration



For importing configuration

For exporting configuration

Click on Open to load

Select Configuration file

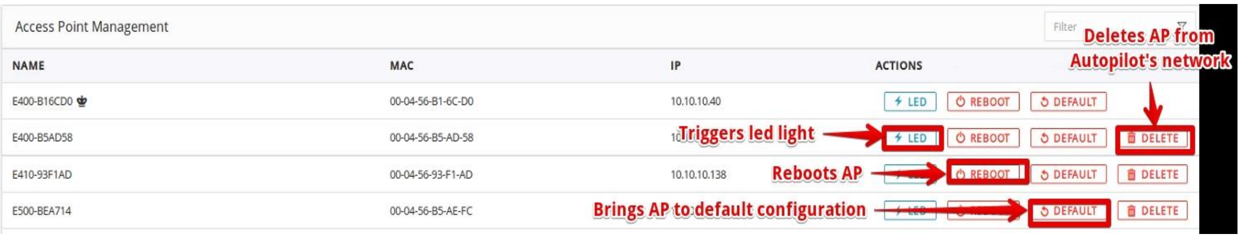
Name	Size	Modified
cnmaestro-export_cnmaestr_20170612T070701.tar.gz	95.2 kB	12 Jun
config.json	30.9 kB	Mon
Config.txt	1.8 kB	7 Jul
E400_E50X-3.4.2-b27.img	17.6 MB	8 Jul

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 119 Access Point management



Access Point Management

Filter

NAME	MAC	IP	ACTIONS
E400-B16CD0 ♛	00-04-56-B1-6C-D0	10.10.10.40	LED · REBOOT · DEFAULT
E400-B5AD58	00-04-56-B5-AD-58	10	LED · REBOOT · DEFAULT · DELETE
E410-93F1AD	00-04-56-93-F1-AD	10.10.10.138	LED · REBOOT · DEFAULT · DELETE
E500-BEA714	00-04-56-B5-AE-FC		LED · REBOOT · DEFAULT · DELETE

Deletes AP from Autopilot's network

Triggers led light

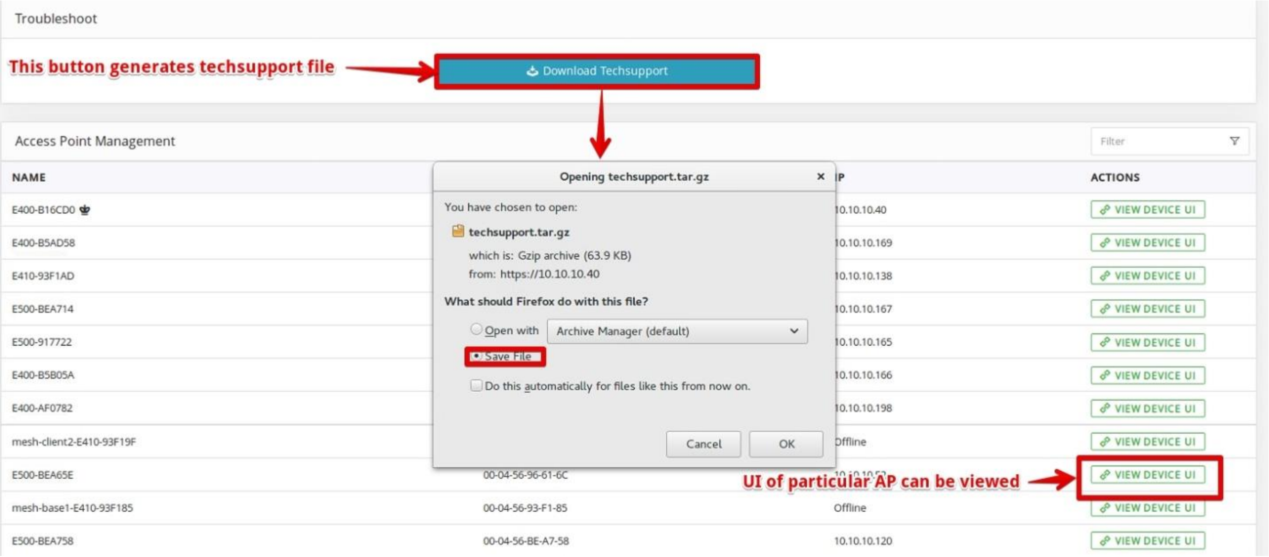
Reboots AP

Brings AP to default configuration

Tools

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

Figure 120 Tools > Troubleshoot



Troubleshoot

This button generates techsupport file

Download Techsupport

Access Point Management

Filter

NAME		IP	ACTIONS
E400-B16CD0 ♛		10.10.10.40	VIEW DEVICE UI
E400-B5AD58		10.10.10.169	VIEW DEVICE UI
E410-93F1AD		10.10.10.138	VIEW DEVICE UI
E500-BEA714		10.10.10.167	VIEW DEVICE UI
E500-917722		10.10.10.165	VIEW DEVICE UI
E400-B5B05A		10.10.10.166	VIEW DEVICE UI
E400-AF0782		10.10.10.198	VIEW DEVICE UI
mesh-client2-E410-93F19F		Offline	VIEW DEVICE UI
E500-BEA65E	00-04-56-96-61-6C	[illegible]	VIEW DEVICE UI
mesh-base1-E410-93F185	00-04-56-93-F1-85	Offline	VIEW DEVICE UI
E500-BEA758	00-04-56-BE-A7-58	10.10.10.120	VIEW DEVICE UI

Opening techsupport.tar.gz ×

You have chosen to open:

techsupport.tar.gz

which is: Gzip archive (63.9 KB)

from: https://10.10.10.40

What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

□ Do this automatically for files like this from now on.

Cancel OK

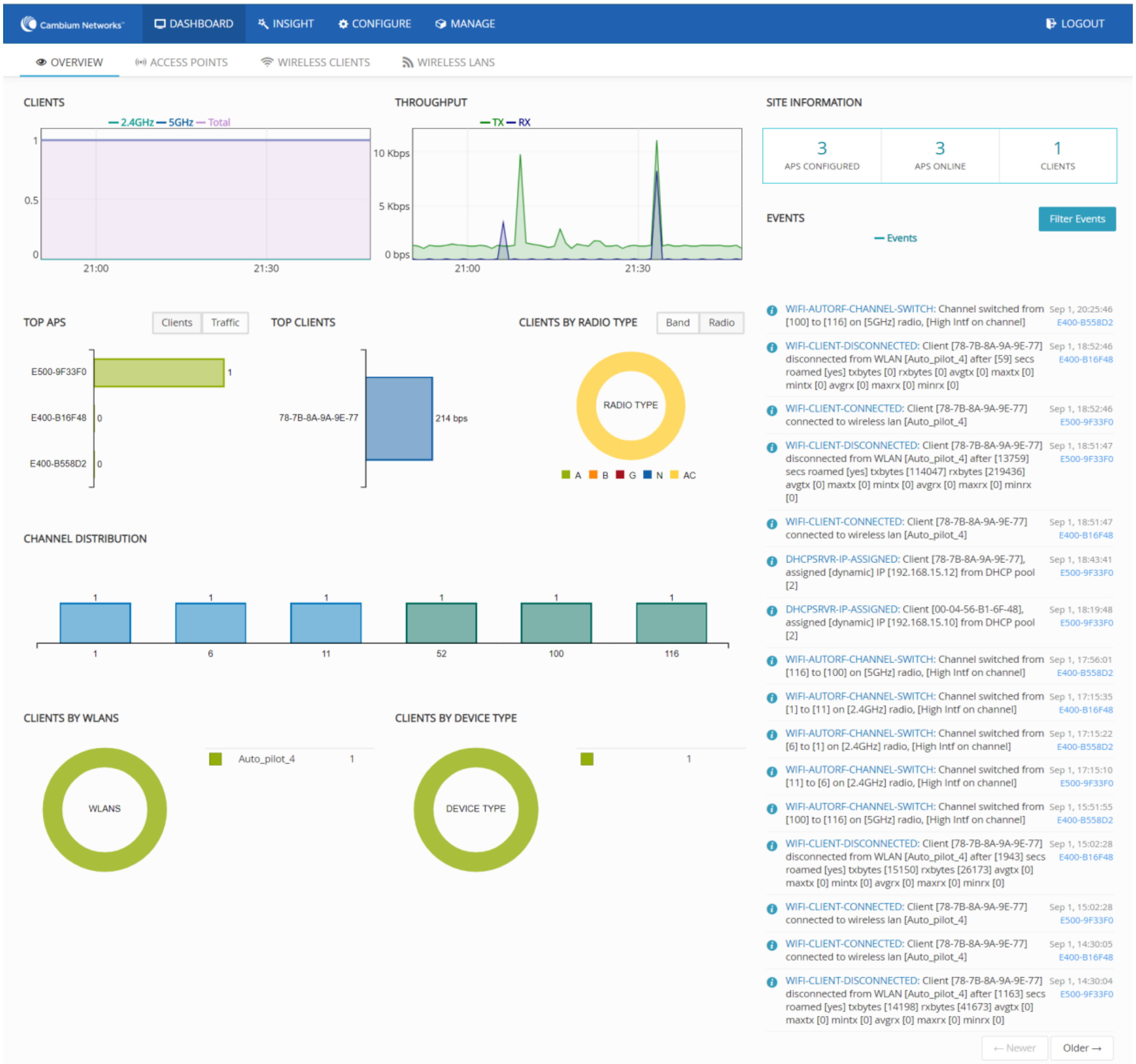
UI of particular AP can be viewed

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 121 Dashboard



```
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from    Sep 1, 20:25:46
[100] to [116] on [5GHz] radio, [High Intf on channel]   E400-B558D2

WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] Sep 1, 18:52:46
disconnected from WLAN [Auto_pilot_4] after [59] secs    E400-B16F48
roamed [yes] txbytes [0] rxbytes [0] avgtx [0] maxtx [0]
mintx [0] avgrx [0] maxrx [0] minrx [0]

WIFI-CLIENT-CONNECTED: Client [78-7B-8A-9A-9E-77]    Sep 1, 18:52:46
connected to wireless lan [Auto_pilot_4]                 E500-9F33F0

WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] Sep 1, 18:51:47
disconnected from WLAN [Auto_pilot_4] after [13759]      E500-9F33F0
secs roamed [yes] txbytes [114047] rxbytes [219436]
avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx
[0]

WIFI-CLIENT-CONNECTED: Client [78-7B-8A-9A-9E-77]    Sep 1, 18:51:47
connected to wireless lan [Auto_pilot_4]                 E400-B16F48

DHCPSRVR-IP-ASSIGNED: Client [78-7B-8A-9A-9E-77],    Sep 1, 18:43:41
assigned [dynamic] IP [192.168.15.12] from DHCP pool     E500-9F33F0
[2]

DHCPSRVR-IP-ASSIGNED: Client [00-04-56-B1-6F-48],    Sep 1, 18:19:48
assigned [dynamic] IP [192.168.15.10] from DHCP pool     E500-9F33F0
[2]

WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from    Sep 1, 17:56:01
[116] to [100] on [5GHz] radio, [High Intf on channel]   E400-B558D2

WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from    Sep 1, 17:15:35
[1] to [11] on [2.4GHz] radio, [High Intf on channel]    E400-B16F48

WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from    Sep 1, 17:15:22
[6] to [1] on [2.4GHz] radio, [High Intf on channel]     E400-B558D2

WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from    Sep 1, 17:15:10
[11] to [6] on [2.4GHz] radio, [High Intf on channel]    E500-9F33F0

WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from    Sep 1, 15:51:55
[100] to [116] on [5GHz] radio, [High Intf on channel]   E400-B558D2

WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] Sep 1, 15:02:28
disconnected from WLAN [Auto_pilot_4] after [1943] secs  E400-B16F48
roamed [yes] txbytes [15150] rxbytes [26173] avgtx [0]
maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]

WIFI-CLIENT-CONNECTED: Client [78-7B-8A-9A-9E-77]    Sep 1, 15:02:28
connected to wireless lan [Auto_pilot_4]                 E500-9F33F0

WIFI-CLIENT-CONNECTED: Client [78-7B-8A-9A-9E-77]    Sep 1, 14:30:05
connected to wireless lan [Auto_pilot_4]                 E400-B16F48

WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] Sep 1, 14:30:04
disconnected from WLAN [Auto_pilot_4] after [1163] secs  E500-9F33F0
roamed [yes] txbytes [14198] rxbytes [41673] avgtx [0]
maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]
```

Overview

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

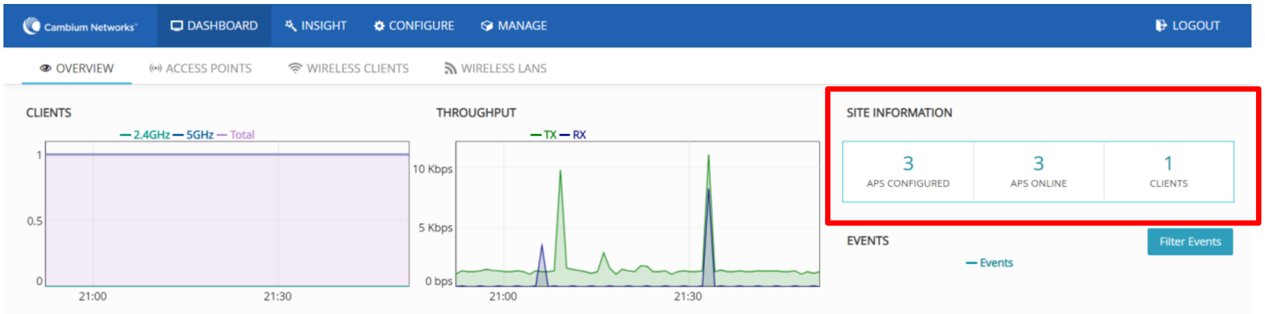
- Site information
- Discovered devices
- Events
- Clients
- Throughput
- Top AP
- Top clients

- 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.

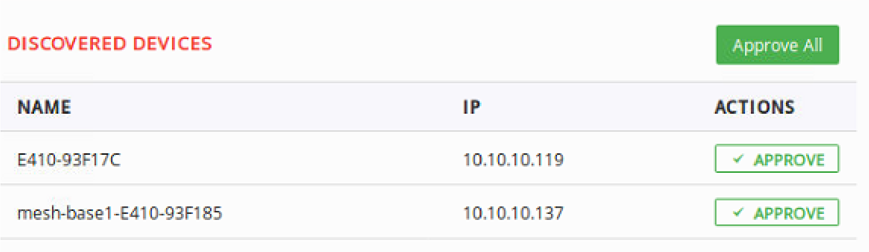
Figure 122 Dashboard > Overview > Site information



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 123 Dashboard > Overview > Discovered devices



DISCOVERED DEVICES

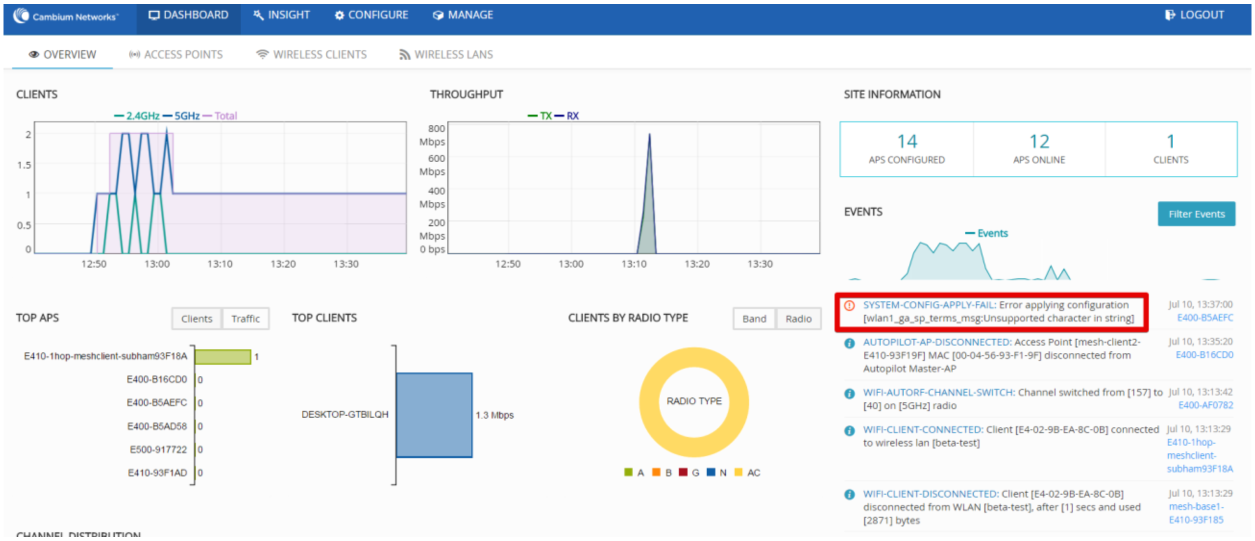
Approve All

NAME	IP	ACTIONS
E410-93F17C	10.10.10.119	✓ APPROVE
mesh-base1-E410-93F185	10.10.10.137	✓ 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 124 Dashboard > Overview > Events



SYSTEM-CONFIG-APPLY-FAIL: Error applying configuration [wlan1_ga_sp_terms_msg:Unsupported character in string] Jul 10, 13:37:00 E400-B5AEFC

AUTOPILOT-AP-DISCONNECTED: Access Point [mesh-client2-E410-93F19F] MAC [00-04-56-93-F1-9F] disconnected from Autopilot Master-AP Jul 10, 13:35:20 E400-B16CD0

WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [157] to [40] on [5GHz] radio Jul 10, 13:13:42 E400-AF0782

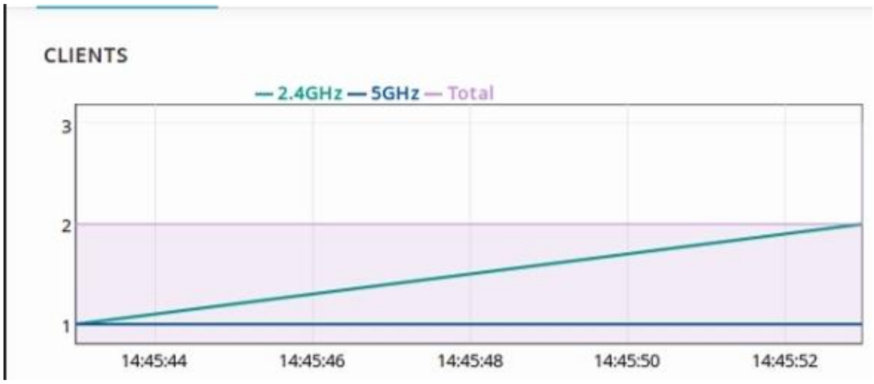
WIFI-CLIENT-CONNECTED: Client [E4-02-9B-EA-8C-0B] connected to wireless lan [beta-test] Jul 10, 13:13:29 E410-1hop-meshclient-subham93F18A

WIFI-CLIENT-DISCONNECTED: Client [E4-02-9B-EA-8C-0B] disconnected from WLAN [beta-test], after [1] secs and used [2871] bytes Jul 10, 13:13:29 mesh-base1-E410-93F185

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.

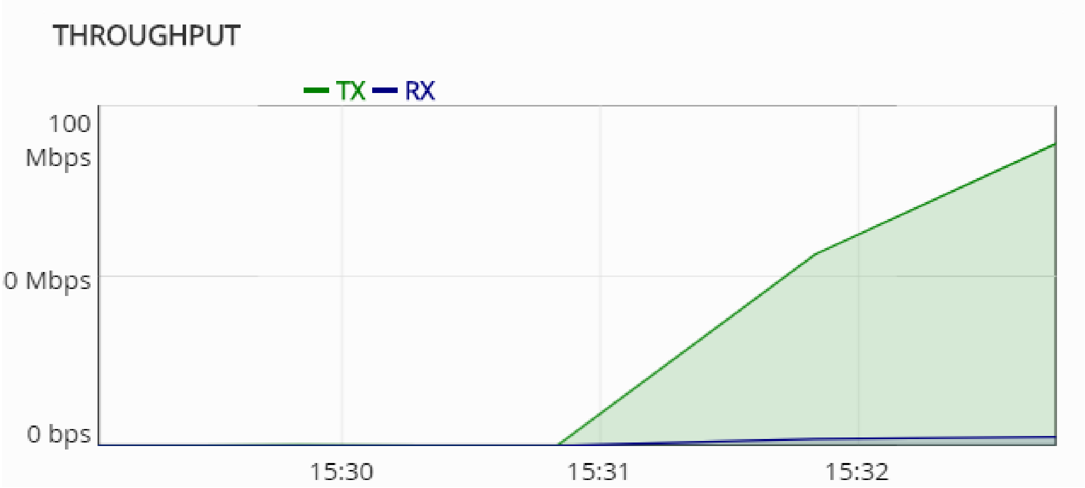
Figure 125 Dashboard > Overview > Clients



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.

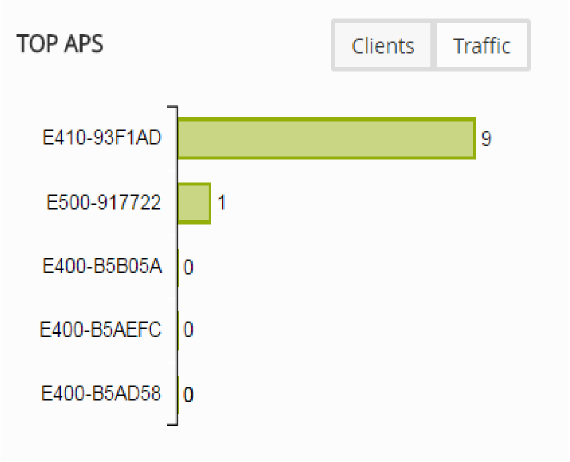
Figure 126 Dashboard > Overview > Throughput

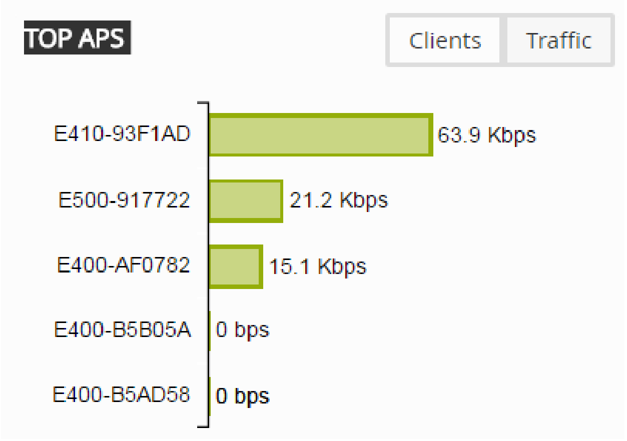


Top APs

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).

Figure 127 Dashboard > Overview > Top Aps

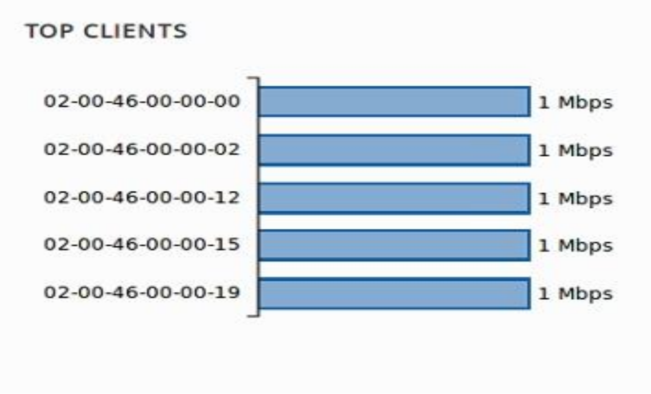




Top clients

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

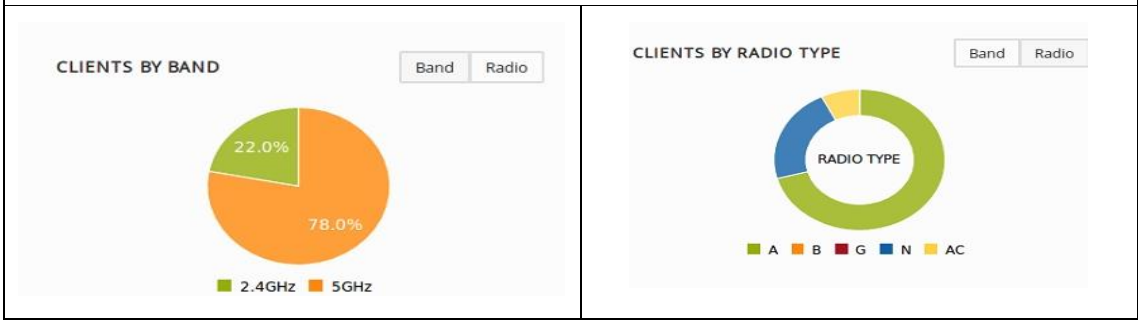
Figure 128 Dashboard > Overview > Top clients



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.

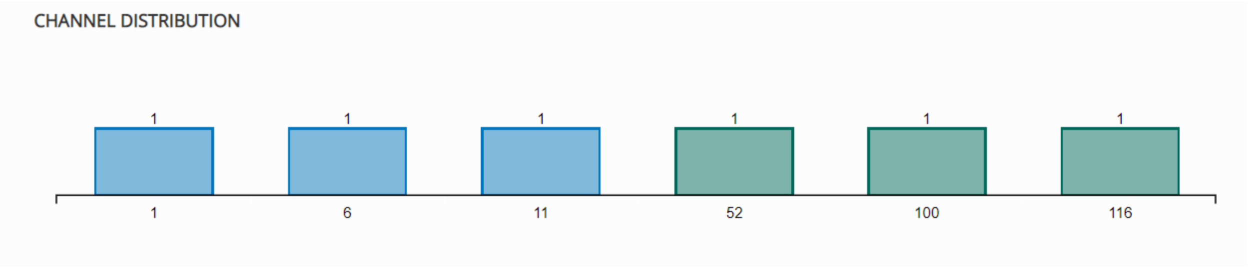
Figure 129 Dashboard > Overview > Clients by Band/Radio



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.

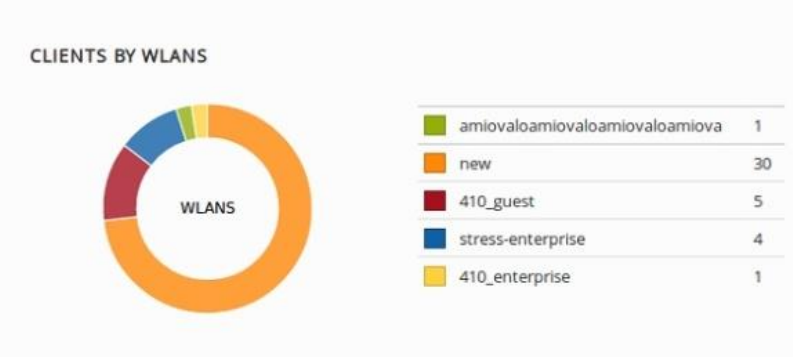
Figure 130 Dashboard > Overview > Channel distribution



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 131 Dashboard > Overview > Clients by WLANs

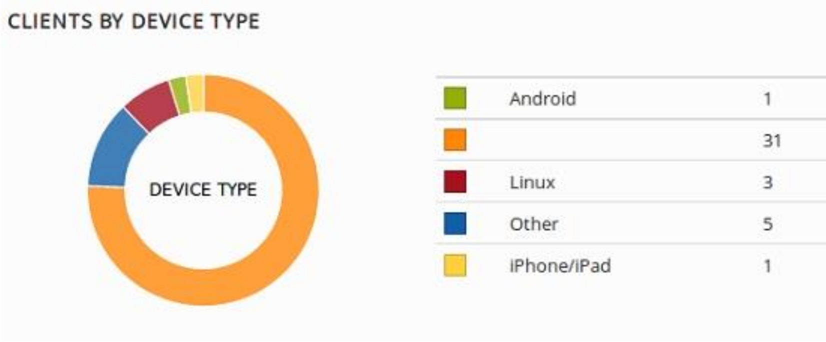


🟩	amiovaloamiovaloamiovaloamiova	1
🟧	new	30
🟥	410_guest	5
🟦	stress-enterprise	4
🟨	410_enterprise	1

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.

Figure 132 Dashboard > Overview > Clients by device type



🟩	Android	1
🟧		31
🟥	Linux	3
🟦	Other	5
🟨	iPhone/iPad	1

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:

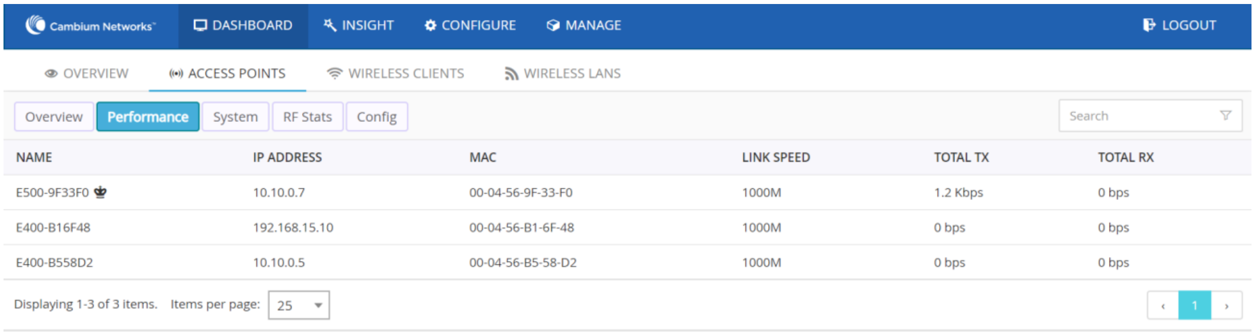
Overview

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.

Figure 133 Dashboard > Access Points > Performance



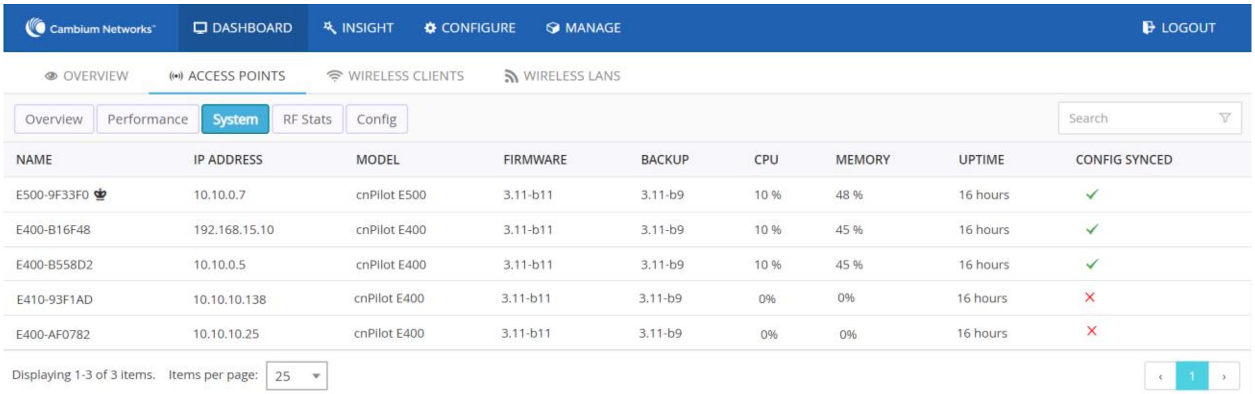
NAME	IP ADDRESS	MAC	LINK SPEED	TOTAL TX	TOTAL RX
E500-9F33F0 ♚	10.10.0.7	00-04-56-9F-33-F0	1000M	1.2 Kbps	0 bps
E400-B16F48	192.168.15.10	00-04-56-B1-6F-48	1000M	0 bps	0 bps
E400-B558D2	10.10.0.5	00-04-56-B5-58-D2	1000M	0 bps	0 bps

Displaying 1-3 of 3 items. Items per page: 25

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 134.

Figure 134 Dashboard > Access Points > System



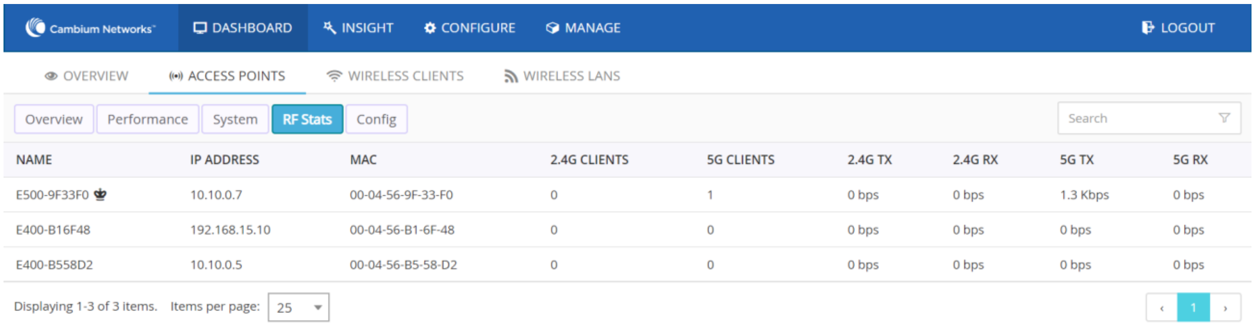
NAME	IP ADDRESS	MODEL	FIRMWARE	BACKUP	CPU	MEMORY	UPTIME	CONFIG SYNCED
E500-9F33F0 ♚	10.10.0.7	cnPilot E500	3.11-b11	3.11-b9	10 %	48 %	16 hours	✓
E400-B16F48	192.168.15.10	cnPilot E400	3.11-b11	3.11-b9	10 %	45 %	16 hours	✓
E400-B558D2	10.10.0.5	cnPilot E400	3.11-b11	3.11-b9	10 %	45 %	16 hours	✓
E410-93F1AD	10.10.10.138	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	✗

Displaying 1-3 of 3 items. Items per page: 25

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.

Figure 135 Dashboard > Access Points > RF Status



NAME	IP ADDRESS	MAC	2.4G CLIENTS	5G CLIENTS	2.4G TX	2.4G RX	5G TX	5G RX
E500-9F33F0 ♛	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. Items per page: 25

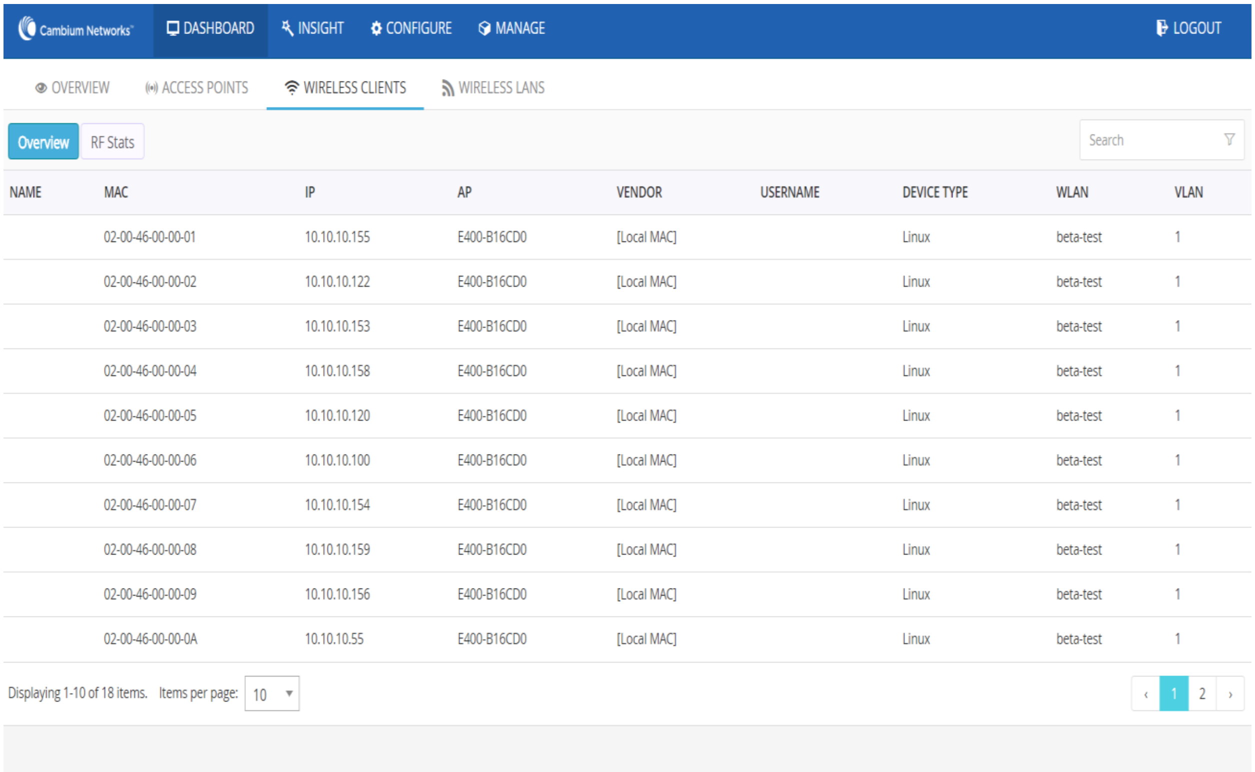
Wireless clients

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.

Figure 136 Dashboard > Wireless clients



NAME	MAC	IP	AP	VENDOR	USERNAME	DEVICE TYPE	WLAN	VLAN
	02-00-46-00-00-01	10.10.10.155	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	10.10.10.153	E400-B16CD0	[Local MAC]		Linux	beta-test	1
	02-00-46-00-00-04	10.10.10.158	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	10.10.10.154	E400-B16CD0	[Local MAC]		Linux	beta-test	1
	02-00-46-00-00-08	10.10.10.159	E400-B16CD0	[Local MAC]		Linux	beta-test	1
	02-00-46-00-00-09	10.10.10.156	E400-B16CD0	[Local MAC]		Linux	beta-test	1
	02-00-46-00-00-0A	10.10.10.55	E400-B16CD0	[Local MAC]		Linux	beta-test	1

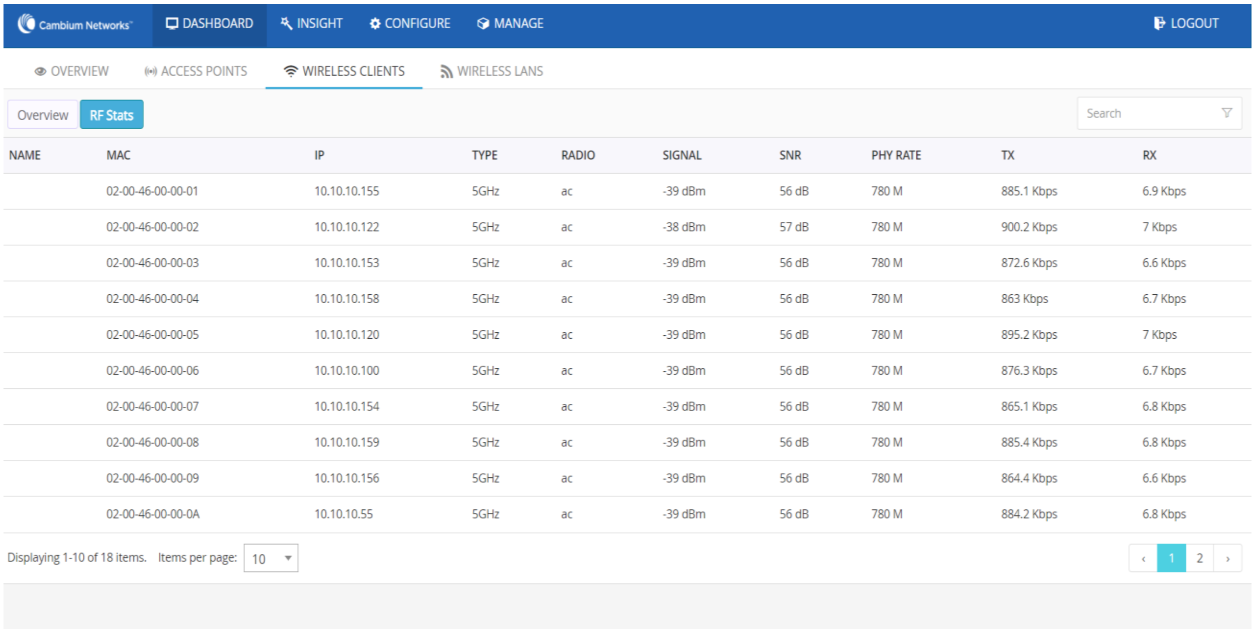
Displaying 1-10 of 18 items. Items per page: 10

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 137 Dashboard > Wireless clients > RF status



NAME	MAC	IP	TYPE	RADIO	SIGNAL	SNR	PHY RATE	TX	RX
	02-00-46-00-00-01	10.10.10.155	5GHz	ac	-39 dBm	56 dB	780 M	885.1 Kbps	6.9 Kbps
	02-00-46-00-00-02	10.10.10.122	5GHz	ac	-38 dBm	57 dB	780 M	900.2 Kbps	7 Kbps
	02-00-46-00-00-03	10.10.10.153	5GHz	ac	-39 dBm	56 dB	780 M	872.6 Kbps	6.6 Kbps
	02-00-46-00-00-04	10.10.10.158	5GHz	ac	-39 dBm	56 dB	780 M	863 Kbps	6.7 Kbps
	02-00-46-00-00-05	10.10.10.120	5GHz	ac	-39 dBm	56 dB	780 M	895.2 Kbps	7 Kbps
	02-00-46-00-00-06	10.10.10.100	5GHz	ac	-39 dBm	56 dB	780 M	876.3 Kbps	6.7 Kbps
	02-00-46-00-00-07	10.10.10.154	5GHz	ac	-39 dBm	56 dB	780 M	865.1 Kbps	6.8 Kbps
	02-00-46-00-00-08	10.10.10.159	5GHz	ac	-39 dBm	56 dB	780 M	885.4 Kbps	6.8 Kbps
	02-00-46-00-00-09	10.10.10.156	5GHz	ac	-39 dBm	56 dB	780 M	864.4 Kbps	6.6 Kbps
	02-00-46-00-00-0A	10.10.10.55	5GHz	ac	-39 dBm	56 dB	780 M	884.2 Kbps	6.8 Kbps

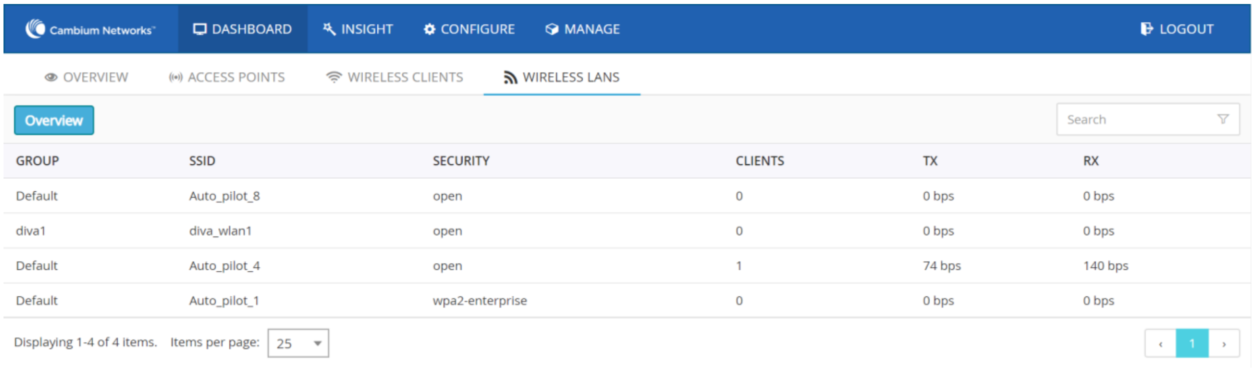
Displaying 1-10 of 18 items. Items per page: 10

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 138 Dashboard > Wireless LANs



GROUP	SSID	SECURITY	CLIENTS	TX	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-enterprise	0	0 bps	0 bps

Displaying 1-4 of 4 items. Items per page: 25

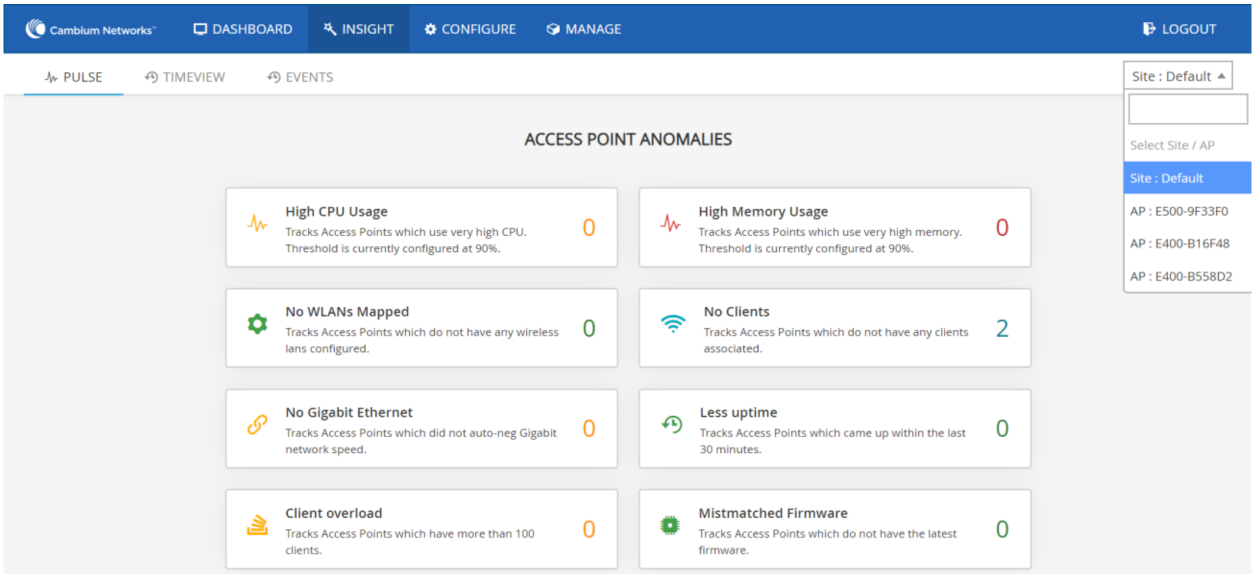
Insight

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.

Figure 139 Insight > Pulse



ACCESS POINT ANOMALIES

High CPU Usage
Tracks Access Points which use very high CPU. Threshold is currently configured at 90%. 0

High Memory Usage
Tracks Access Points which use very high memory. Threshold is currently configured at 90%. 0

No WLANs Mapped
Tracks Access Points which do not have any wireless lans configured. 0

No Clients
Tracks Access Points which do not have any clients associated. 2

No Gigabit Ethernet
Tracks Access Points which did not auto-neg Gigabit network speed. 0

Less uptime
Tracks Access Points which came up within the last 30 minutes. 0

Client overload
Tracks Access Points which have more than 100 clients. 0

Mismatched Firmware
Tracks Access Points which do not have the latest firmware. 0

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.

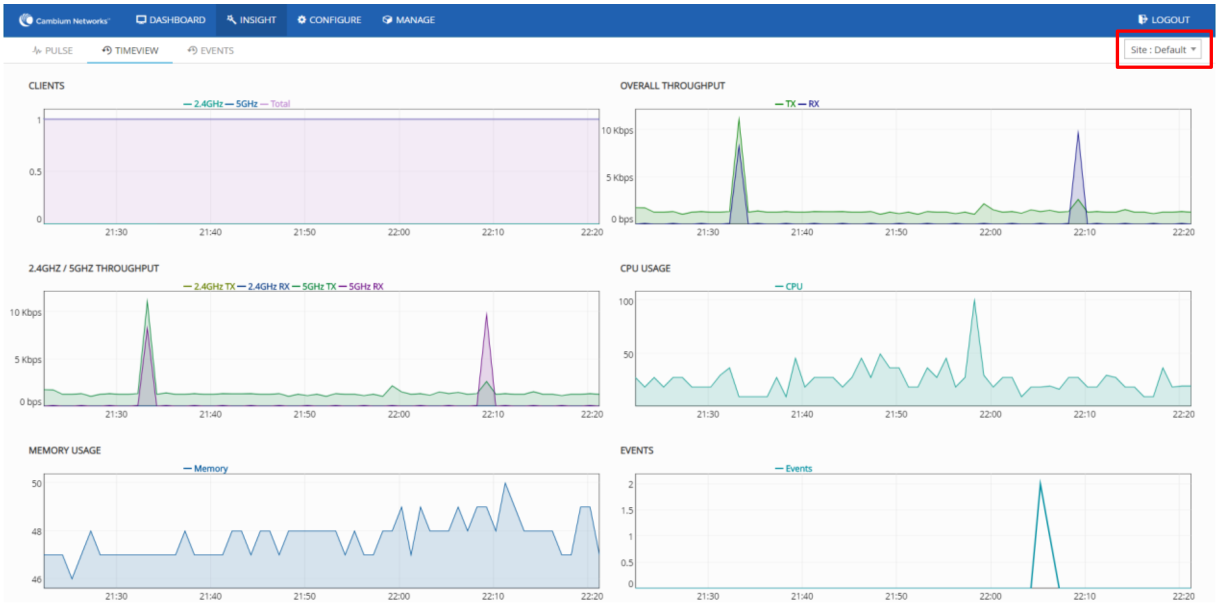
- No WLANs mapped: This option leads to APs page of Dashboard tab and tracks number of APs without wireless LANs configured.
- No Gigabit ethernet: This option leads to APs page of Dashboard tab and tracks APs which do not auto negotiate Gigabit network speed.
- Client overload: This option leads to 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.

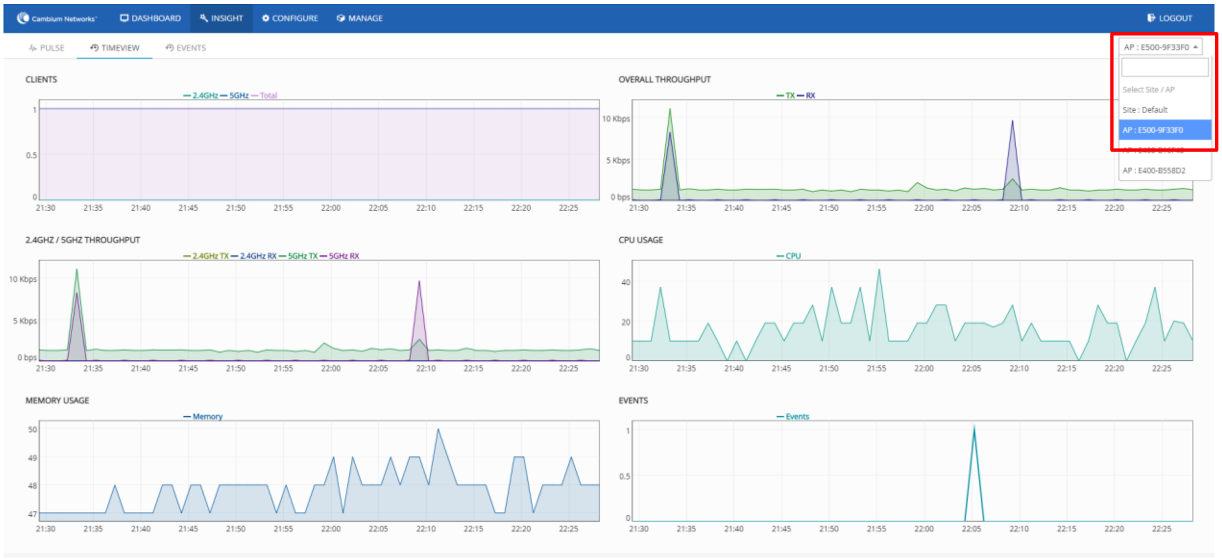
> Note In current version not all of these options are supported.

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.

Figure 140 Insight > Timeview

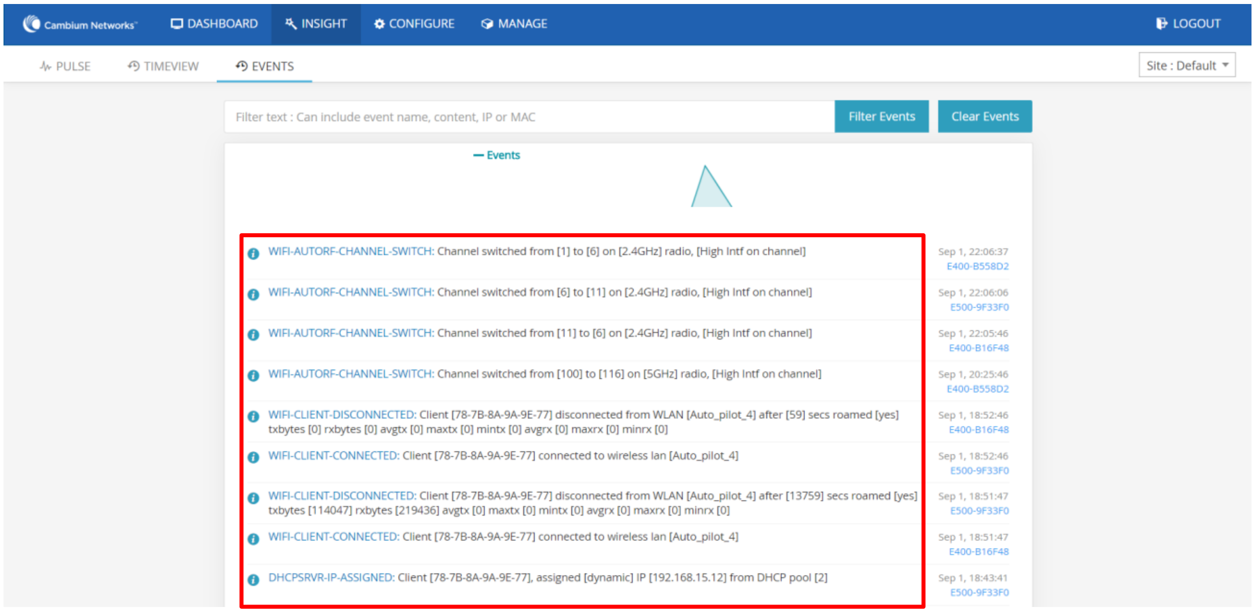




Events

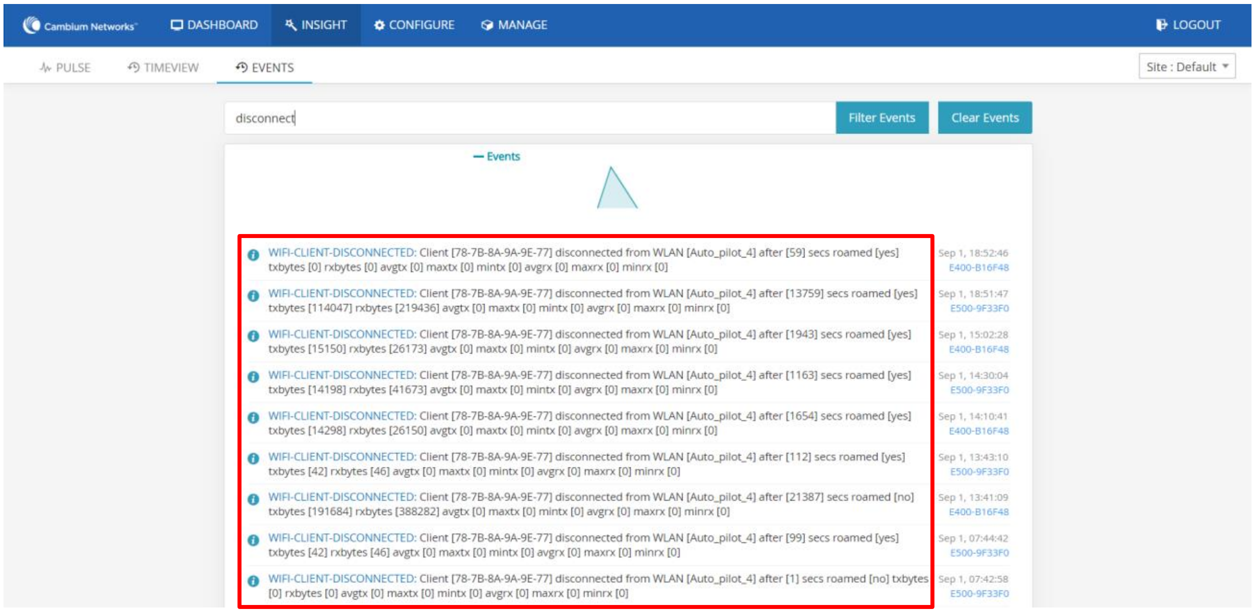
This tab provides the list of all the latest events of master and member APs. Events can be filtered for specific APs based on their event name, content, Mac or IP address. All the old events can be cleared to start afresh.

Figure 141 Insight > Unfiltered Events



```
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [1] to [6] on [2.4GHz] radio, [High Intf on channel]     Sep 1, 22:06:37
                                                                                                            E400-B558D2
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [6] to [11] on [2.4GHz] radio, [High Intf on channel]    Sep 1, 22:06:06
                                                                                                            E500-9F33F0
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [11] to [6] on [2.4GHz] radio, [High Intf on channel]    Sep 1, 22:05:46
                                                                                                            E400-B16F48
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [100] to [116] on [5GHz] radio, [High Intf on channel]   Sep 1, 20:25:46
                                                                                                            E400-B558D2
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [59] secs roamed [yes]    Sep 1, 18:52:46
txbytes [0] rxbytes [0] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                                         E400-B16F48
WIFI-CLIENT-CONNECTED: Client [78-7B-8A-9A-9E-77] connected to wireless lan [Auto_pilot_4]                 Sep 1, 18:52:46
                                                                                                            E500-9F33F0
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [13759] secs roamed [yes] Sep 1, 18:51:47
txbytes [114047] rxbytes [219436] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]               E500-9F33F0
WIFI-CLIENT-CONNECTED: Client [78-7B-8A-9A-9E-77] connected to wireless lan [Auto_pilot_4]                 Sep 1, 18:51:47
                                                                                                            E400-B16F48
DHCPSRVR-IP-ASSIGNED: Client [78-7B-8A-9A-9E-77], assigned [dynamic] IP [192.168.15.12] from DHCP pool [2]  Sep 1, 18:43:41
                                                                                                            E500-9F33F0
```

Figure 142 Insight > Filtered Events



disconnect

```
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [59] secs roamed [yes]    Sep 1, 18:52:46
txbytes [0] rxbytes [0] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                                         E400-B16F48
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [13759] secs roamed [yes] Sep 1, 18:51:47
txbytes [114047] rxbytes [219436] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]               E500-9F33F0
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [1943] secs roamed [yes]  Sep 1, 15:02:28
txbytes [15150] rxbytes [26173] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                 E400-B16F48
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [1163] secs roamed [yes]  Sep 1, 14:30:04
txbytes [14198] rxbytes [41673] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                 E500-9F33F0
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-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] avgrx [0] maxrx [0] minrx [0]                 E400-B16F48
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [112] secs roamed [yes]   Sep 1, 13:43:10
txbytes [42] rxbytes [46] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                       E500-9F33F0
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [21387] secs roamed [no]  Sep 1, 13:41:09
txbytes [191684] rxbytes [388282] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]               E400-B16F48
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [99] secs roamed [yes]    Sep 1, 07:44:42
txbytes [42] rxbytes [46] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                       E500-9F33F0
WIFI-CLIENT-DISCONNECTED: Client [78-7B-8A-9A-9E-77] disconnected from WLAN [Auto_pilot_4] after [1] secs roamed [no] txbytes Sep 1, 07:42:58
[0] rxbytes [0] avgtx [0] maxtx [0] mintx [0] avgrx [0] maxrx [0] minrx [0]                                 E500-9F33F0
```

Glossary

Term	Definition
AP	Access Point Module. One module that distributes network or Internet services to subscriber modules.
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host.
BHM	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.
DFS	See Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
FCC	Federal Communications Commission of the U.S.A.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
UI	User interface.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure
HT	High Throughput

Term	Definition
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 assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Cambium implementation, this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MIR	See Maximum Information Rate.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not 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. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.
VHT	Very High Throughput