cnPilot™ Enterprise AP User Guide

e410/e600/e430W/e502S/e700/e430H
E400/E500/E501S

System Release 3.9

Cambium Networks

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.

Safety and Regulatory Information

This section describes important safety and regulatory guidelines that must be observed by personnel installing or operating cnPilot Enterprise AP equipment.

Important Safety Information

⚠Warning

To prevent loss of life or physical injury, observe the safety guidelines in this section.

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

Grounding and protective earth

cnPilot Enterprise AP devices must be properly grounded to protect against lightning. It is the user’s responsibility to install the equipment in accordance with national regulations. In the USA, follow Section 810 of the *National Electric Code, ANSI/NFPA No.70-1984* (USA). In Canada, follow Section 54 of the *Canadian Electrical Code*. These codes describe correct installation procedures for grounding the outdoor unit, mast, lead-in wire and discharge unit, size of grounding conductors and connection requirements for grounding electrodes. Other regulations may apply in different countries and therefore it is recommended that installation be contracted to a professional installer.

Powering down before servicing

Always power down and unplug the equipment before servicing.

Primary disconnect device

The cnPilot Enterprise AP power supply is the primary disconnect device.

RF exposure near the antenna

Strong radio frequency (RF) fields will be present close to the antenna when the transmitter is on. Always turn off the power to the cnPilot Enterprise AP device before undertaking maintenance activities in front of the antenna.

Important Regulatory Information

The cnPilot Enterprise AP product is certified as an unlicensed device in frequency bands where it is not allowed to cause interference to licensed services (called primary users of the bands).

Radar avoidance

In countries where radar systems are the primary band users, the regulators have mandated special requirements to protect these systems from interference caused by unlicensed devices. Unlicensed devices must detect and avoid co-channel operation with radar systems.

The cnPilot Enterprise AP detects and avoids functionality for countries and frequency bands requiring protection for radar systems. The cnPilot Enterprise AP is qualified for ETSI/FCC DFS certification for radar detection and avoidance as per the law.

Installers and users must meet all local regulatory requirements for radar detection. To meet these requirements, users must set the correct country code during commissioning of the cnPilot Enterprise AP equipment. If this is not done, installers and users may be liable to civil and criminal penalties.

Contact the Cambium helpdesk if more guidance is required.

USA and Canada Specific Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

⚠Caution

Any changes or modifications not expressly approved by the party
responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures.

This device is restricted for indoor use.

Note

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance **20 cm** between the radiator & your body.

IC Statement

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. *L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

This device and it's antennas(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with IC multi-transmitter product procedures.
Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems.
les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.
Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

CE Statement:

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

Specific expertise and training required for professional installers

To ensure that the cnPilot Enterprise AP is installed and configured in compliance with the requirements of Industry Canada and the FCC, installers must have the radio engineering skills and training described in this section. This is particularly important when installing and configuring an cnPilot Enterprise AP system for operation in the 5 GHz band (5150 – 5250 MHz – FCC only, 5250 – 5350 MHz, 5470 – 5725 MHz and 5725 – 5850 MHz).

Avoidance of weather radars

The installer must be familiar with the requirements in FCC KDB 443999. Essentially, the installer must be able to:

- Access the FCC database of weather radar location and channel frequencies.
- Use this information to correctly configure the product (using the GUI) to avoid operation on channels that must be avoided according to the guidelines that are contained in the KDB and explained in detail in this user guide.

In ETSI regions, the band 5600 MHz to 5650 MHz is reserved for the use of weather radars.

External antennas

When using a connectorized version of the product (as compared to the version with an integrated antenna), the conducted transmit power must be reduced to ensure the regulatory limit on transmitter EIRP is not exceeded. The installer must have an understanding of how to compute the effective antenna gain from the actual antenna gain and the antenna cable losses.

The product GUI automatically applies the correct conducted power limit to ensure that it is not possible for the installation to exceed the EIRP limit, when the appropriate values for antenna gain are entered into the GUI.

Ethernet networking skills

The installer must have the ability to configure IP addressing on a PC and to set up and control products using a web browser interface.

Lightning protection

To protect outdoor radio installations from the impact of lightning strikes, the installer must be familiar with the normal procedures for site selection, bonding and grounding.

Training

The installer needs to have basic competence in radio and IP network installation. The specific requirements applicable to the cnPilot Enterprise AP must be gained by reading this user guide and by performing sample setups at base workshop before live installments.

Contents

About this User Guide

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

Intended Audience

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

Contacting Cambium Networks

Support website:	http://www.cambiumnetworks.com/support
Main website:	http://www.cambiumnetworks.com
Community:	http://community.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	support@cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/support/contact-support/
Address:	Cambium Networks Limited, 3800 Golf Road, Suite 360 Rolling Meadows, IL 60008

Purpose

Cambium Networks cnPilot Enterprise AP documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium cnPilot Enterprise AP 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.

Cross References

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

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents.

For feedback, e-mail to support@cambiumnetworks.com.

Warnings, Cautions, and Notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warning

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

Warning

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

Caution

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

Caution

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

Note

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

Note

Note text.

Problems and Warranty

Reporting Problems

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

1. Search this document and the software release notes of supported releases.
2. Visit the support website:
   http://www.cambiumnetworks.com/support
3. Ask for assistance from the Cambium product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support:
   http://www.cambiumnetworks.com/support/contact-support

Repair and Service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Warranty

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

To register PMP products or activate warranties, visit the support website.

For warranty assistance, contact the reseller or distributor.

⚠Caution

Do not open the radio housing for repair or diagnostics; there are no serviceable parts within the housing.

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

Security Advice

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

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

Cambium Networks cnPilot Enterprise AP equipment is shipped with default web management interface login credentials. It is highly recommended that the following default username and password should to be modified prior to system installments.

Username: admin

Password: admin

Human exposure to radio frequency energy

Relevant standards (USA and EC) applicable when working with RF equipment are:

- ANSI IEEE C95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.
- Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC) and respective national regulations.
- Directive 2004/40/EC of the European Parliament and of the Council of 29 April 2004 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- US FCC limits for the general population. See the FCC web site at https://www.fcc.gov/, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites-eng.php and Safety Code 6.
- EN 50383:2002 to 2010 Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz - 40 GHz).
- BS EN 50385:2002 Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz – 40 GHz) – general public.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

Power density exposure limit

Install the radios for the 450 Platform Family of wireless solutions so as to provide and maintain the minimum separation distances from all persons.

The applicable FCC power density exposure limit for RF energy in the 2.4 and 5 GHz frequency bands is 1 mW/cm2.

The applicable ISEDC power density exposure limit for RF energy in unlicensed bands is 0.02619 * (f^(0.6834)), where f is the lowest frequency of the supported band. For licensed bands, the power density exposure limit is 0.6455 * (f^(0.5)), where f is the lowest frequency of the supported band.

Calculation of power density and distance

The following calculation is based on the ANSI IEEE C95.1-1991 method, as that provides a worst case analysis. Details of the assessment to EN50383:2002 can be provided, if required.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P.G}{4\pi d^2}$$

Where:	Is:
S	power density in W/m^2
P	maximum average transmit power capability of the radio, in W
G	total Tx gain as a factor, converted from dB
d	distance from point source, in m

Product	Antenna	G (For 2.4 GHz in dBi)	G (For 5 GHz in dBi)
E400	Omnidirectional	4.55	4.25
e410	Omnidirectional	4.55	4.25
e600	Omnidirectional	4.55	4.25
e430W	Omnidirectional	3	4
E500	Omnidirectional	5	
E501S	Sector	10.5	13
e502S	Sector	12.5	15.9
e700	Omnidirectional	7.5	8

Calculated distances and power compliance margins

The following tables show calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination for the USA and Canada. These are conservative distances that include compliance margins. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

cnPilot Enterprise AP adheres to all applicable EIRP limits for transmit power when operating in MIMO mode. Separation distances and compliance margins include compensation for both transmitters.

$$d = \sqrt{\frac{P.G}{4\pi.S}}$$

Explanation of terms used in the following tables:

P – maximum average transmit power of the radio (Watt)

G – total transmit gain as a factor, converted from dB

S – power density (Watt/m2)

d – minimum safe separation distance from point source (meters)

Product	Regulatory Domain	Power density S (mW/cm²)	distance
E400	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	20cm
	IC	0.54/0.975 (2.4GHz/5GHz)	20cm
	CE	0.196/1.555 (2.4GHz/5GHz)	20cm
e410	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	20cm
	IC	0.54/0.975 (2.4GHz/5GHz)	20cm
	CE	0.1947/5.737 (2.4GHz/5GHz)	20cm
e600	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	23cm
	IC	0.49	20cm
	CE	0.1375/6.257 (2.4G/5G)	24cm
e430W	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	20cm
	IC	0.27	20cm
	CE	0.1935/1.481 (2.4G/5G)	20cm
E430H	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	20cm
	IC	0.27	20cm
	CE	0.1935/1.481 (2.4G/5G)	20cm

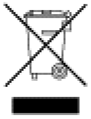
E500	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	20cm
	IC		
	CE	0.193/6.296 (2.4G/5G)	20cm
E501S	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	25cm
	IC		
	CE	0.193/7.494 (2.4G/5G)	20cm
e502S	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	26cm
	IC	0.486	20cm
	CE	0.193/7.865 (2.4G/5G)	20cm
e700	FCC	5 or 1 (Controlled exposure/uncontrolled exposure	24cm
	IC	0.45/0.975 (2.4G/5G)	28cm
	CE		

Caring for the Environment

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

In EU Countries

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



Disposal of Cambium Equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, see http://www.cambiumnetworks.com/support

Disposal of Surplus Packaging

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

In non-EU Countries

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

Product Description

This chapter provides a high level description of the cnPilot Enterprise AP product. It describes the function of the product and the main hardware components.

The major topics described in this document are:

- Overview of cnPilot Enterprise AP
- System configuration
- Radio configuration
- WLAN Configuration
- Network Configuration
- Guest Access
- Firewall and ACL
- Firmware Management
- Troubleshooting

Overview of cnPilot Enterprise AP

This section introduces the key features, typical use cases, product variants and components of the cnPilot Enterprise AP.

PURPOSE

cnPilot Enterprise AP is an 802.11ac dual band radio Wi-Fi Access point. It can be used both as indoor and outdoor AP. It has one Gigabit Ethernet port that also provides Power over Ethernet.

KEY FEATURES

This section describes the key features of cnPilot Enterprise AP:

- Maximum client capacity of cnPilot:

Platform	2.4GHz	5GHz
E400/E500/E50XS	256	128
e410/e430X	256	256
e600/e700	512	512

- Maximum Wireless SSIDs supported by cnPilot is 16 WLANs.
- Can be managed via Cambium Networks cnMaestro cloud-based network manager.
- Supports device configuration by using CLI or UI.
- Can be monitored via SNMP versions v2 and v3.
- A Client traffic can be controlled through rate-limiting policies, configured per-WLAN or per-client.

- Supports Captive Portal redirection (Guest Access) with WISPr functionality
- Supports L3 services such as NAT, port forwarding, DHCP server, and DNS proxy
- Access to the network can be controlled based on traffic type and MAC address using features such as WLAN and Port Access Control (ACL), DNS based whitelist and blacklist, and DoS attack prevention

Supported Features	
Controller modes	• Autonomous Controller-less operations (E.g: roaming) • Cloud Managed • On-premise virtualized controller
Secure WLAN	• WPA-TKIP, WPA2 AES, 802.1x • 802.11w (Protected Management Frames)
Hotspot 2.0/Passpoint	
Captive Portal/ Guest Access	• cnMaestro controller • Stand-alone AP based • Redirection to external radius server • Active Directory Integration
Authentication	Secure Web page, RADIUS based 802.1x including EAP-SIM/AKA, EAP-PEAP, EAP-TTLS, and EAP-TLS MAC authentication (local database or External RADIUS server)
Accounting	Supports RADIUS based accounting to multiple AAAs
Scheduled SSID	Turn SSID ON/OFF on a daily/weekly/time of day basis
VLAN	• Dynamic VLAN assignment from RADIUS server. • VLAN per SSID per user, VLAN load balancing
Data Limiting	Dynamic rate limiting of client traffic per SSID & per client
Subscriber QoS	WMM
Client Isolation	
Controller-Less Fast Roaming	• Yes. 802.11r, Opportunistic Key Caching supports Enhanced roaming • Disconnect for sticky clients
ACS: Automatic Channel Selection	Set at start or run periodically
NAT	
DHCP Server	
Firewall	NAT logging
ACL, DNS-ACL	L2, L3 or DNS based access control

Supported Features	
Band Steering Band Balancing	
Airtime Fairness	
Tunneling	• L2TP • L2oGRE • PPPoE
Tools	• Packet Capture • Wireless Sniffer • IP Connectivity • Wi-Fi Analyser • Tech Support (Logs)
Services	
APIs	Presence Locating API
Certifications	FCC, ETSI, CE EN 60601-1-2 (Medical EMC) UL2043 Plenum rated

DEFAULT SETTINGS

The cnPilot Access Point is setup to obtain its IP address from a DHCP server. A default IP address of 192.168.0.1 will be used if an IP address is not obtained from DHCP. The default username and password for CLI as well as GUI (http/https) access are admin / admin.

LED STATUS

The **`e410/e430X/e600/e700`** Access Point has two dual color LEDs. The power LED will glow Orange as the AP boots up, and turn Green once it has booted up successfully. The network/status LED will glow Orange if the connection to cnMaestro controller/manager is down, and Green once the AP is connected successfully to cnMaestro.

Table 1: e410/e430X/e600/e700 LED Status

LED Color	Description
Amber	Access Point is powering up and initializing.
Green	Access Point is in service.
Blue	Access Point is managed through cnMaestro.

Table 2: E400/E500/E50XS LED Status

LED Color	Description
Amber	Access Point is powering up and initializing.
Green	Access Point is in service.
Green	Access Point is managed through cnMaestro.

Installation

This chapter provides details on the following sections:

- Lightning Protection Guidelines
- Mounting the Device
- Powering Up the Device
- Configure Management PC
- Accessing the Device UI
- Accessing the Device CLI

Lightning Protection Guidelines

⚠ Warning

Electro-Magnetic Discharge (EMD) lightning damage is not covered under warranty. The recommendations in this section, when followed correctly, provides the user the best protection from the harmful effects of EMD. However, 100% protection is neither implied nor possible.

Purpose

To protect structures, equipment and people against power surges (typically caused by lightning) by conducting the surge current to ground via a separate preferential solid path. The actual degree of protection required depends on local conditions and applicable local regulations. Cambium recommends cnPilot installation is contracted to a professional installer.

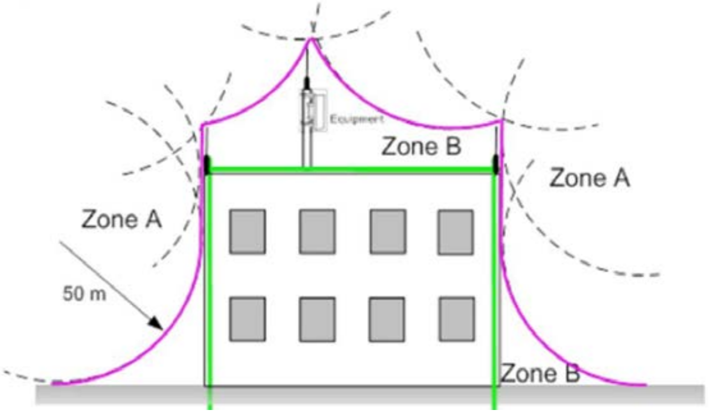
Standards

Refer international standards IEC 62305-1 and IEC 62304-4, the U.S. National Electric Code ANSI/NFPA No. 70-2017 or section 54 of the Canadian Electric Code for details of lightning protection methods and requirements.

Lightning Protection Installation Zones

The “rolling sphere method” (Figure 1) is used to determine the safe zone to install the lightning protection equipment. An imaginary sphere, typically 50 meters in radius is rolled over the structure. Where the sphere rests against the ground and a strike termination device (such as a finial or ground bar), all the space under the sphere is in the zone of protection (Zone B) as shown in the below figure. Similarly, where the sphere rests on two finals, the space under the sphere is considered as in the zone of protection.

Figure 1: Rolling sphere method to determine the lightning protection zones



Assess locations on poles, towers and buildings to determine, whether the location is in Zone A or Zone B:

- **Zone A:** In this zone a direct lightning strike is possible. Do not mount equipment in this zone.
- **Zone B:** In this zone, direct lightning effects are still possible, but mounting in this zone significantly reduces the possibility of a direct strike. Mount the equipment in this zone.

⚠ Warning

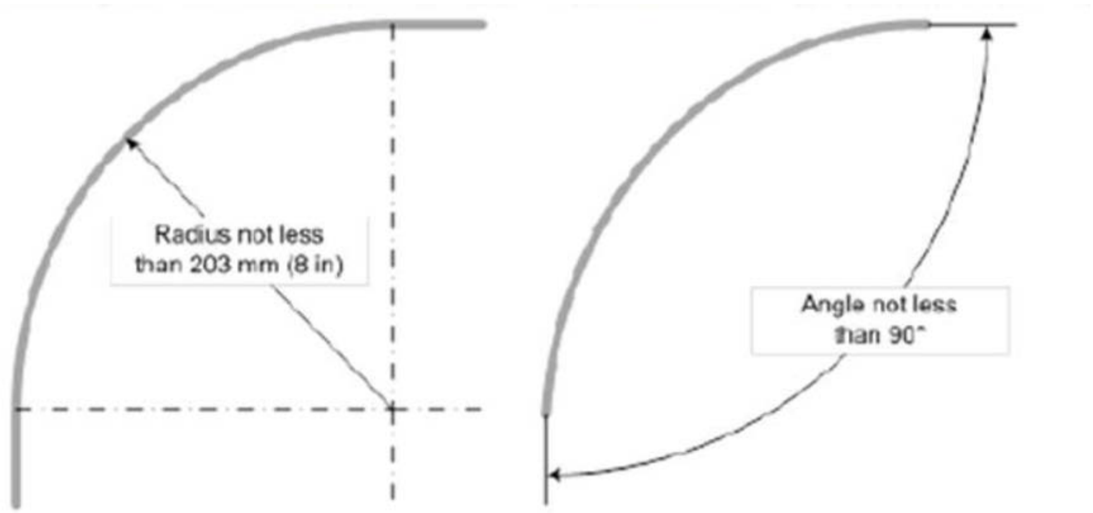
Never mount equipment in Zone A. Mounting in Zone A may put equipment, structures and life at risk.

Grounding Guidelines

Implement the following requirements, when routing, fastening and connecting grounding cables:

- Make sure the grounding conductors run as short, straight, and smoothly as possible, with the minimum bends and curves.
- Do not install the grounding cables with drip loops.
- All bends must have a minimum radius of 203 mm and a minimum angle of 90° as shown in the below figure. A diagonal run is preferable to a bend, even though it does not follow the contour or run parallel to the supporting structure.
- Route all bends, curves and connections towards the grounding electrode system, ground rod, or ground bar.
- Securely fasten the grounding conductors.
- Use the braided grounding conductors.
- Use the approved bonding techniques for the connection of dissimilar metals.

Figure 2: Grounding cable minimum bend radius and angle



General Protection Requirements

To adequately protect AP installation for both ground bonding and transient voltage, surge suppression is required.

Basic Requirements

Implement the following basic protection requirements:

- Install the equipment in ‘Zone B’
- Ground the AP to the supporting structure.
- If additional surge protection is required, then install one more Surge Suppressor near the AP.
- Install the 56V-Gigabit Surge Suppressor (1000SS) within 600 mm of the point at which the power cable enters the building or equipment room.
- Ground the drop cable at the entry point of the building.
- Make sure the drop cable is not laid alongside a lightning air terminal.
- All grounding cables must be a minimum size of 10 mm2 csa (8AWG), preferably 16 mm2 csa (6AWG), or 25 mm2 csa (4AWG).

Pole or Tower Mount Guidelines

If you need to install AP to a metal tower or pole, then in addition to the general protection requirements, follow the below requirements:

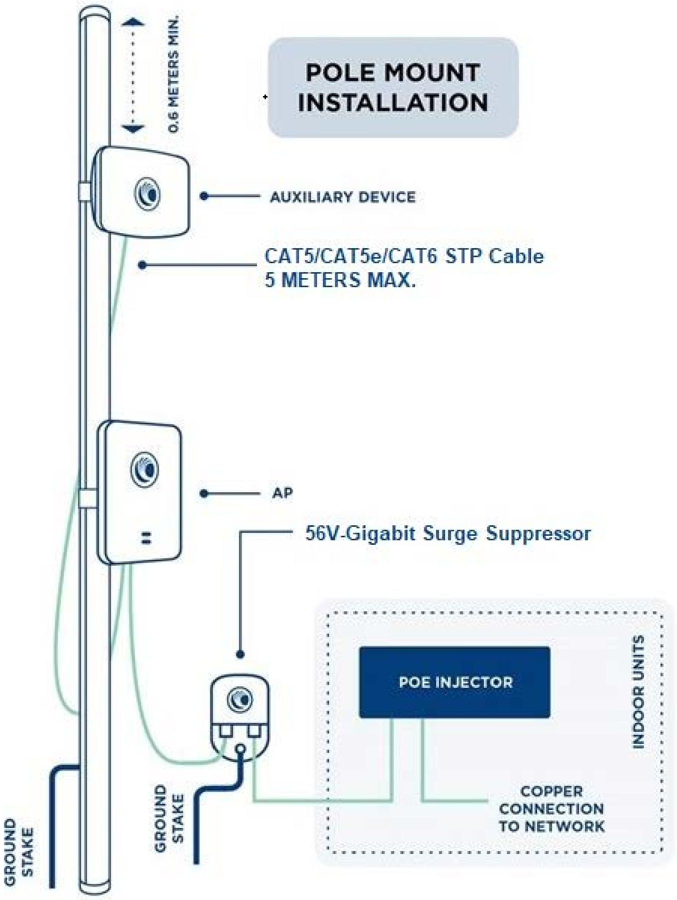
- Ensure that the position of the equipment is lower than the top of the tower or its lightning air terminal.
- Ensure that the metal tower or pole is correctly grounded.
- Install a grounding kit at the first point of contact (top), between the drop cable and the tower.
- Install a grounding kit at the bottom of the tower, near the vertical to horizontal transition point.

Note

If grounding kit is installed, make sure the grounding kit is bonded to the tower or Tower Ground Bus bar (TGB).

Connection examples of pole or tower installations are shown in the below figure.

Figure 3: Grounding and lightning protection on pole or tower



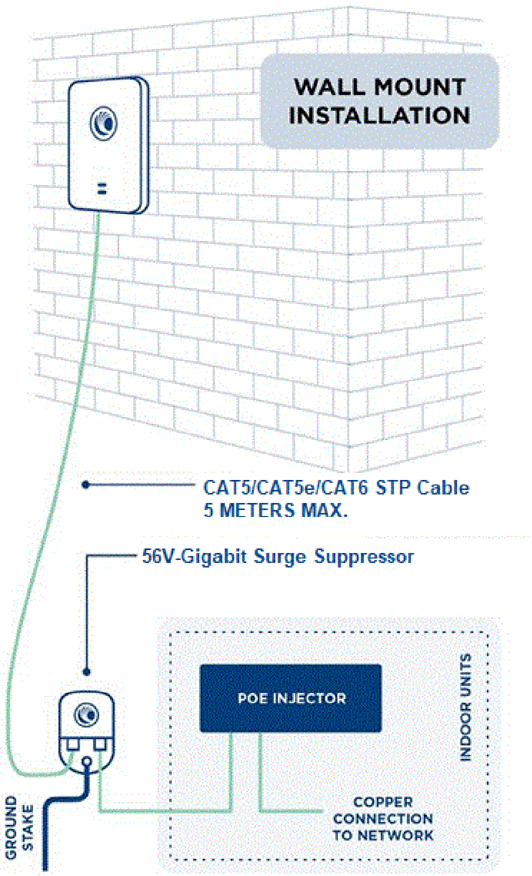
Wall Mount Guidelines

If you need to install AP on the wall of a building, then in addition to the general protection requirements, follow the below requirements also:

- Ensure that the position of the equipment is lower than the top of the building or its lightning air terminal.
- Ensure that the building is correctly grounded.

Connection examples of wall installations are shown in the below figure.

Figure 4: Grounding and lightning protection on wall


WALL MOUNT INSTALLATION
CAT5/CAT5e/CAT6 STP Cable
5 METERS MAX.
56V-Gigabit Surge Suppressor
POE INJECTOR
INDOOR UNITS
COPPER CONNECTION TO NETWORK
GROUND STAKE

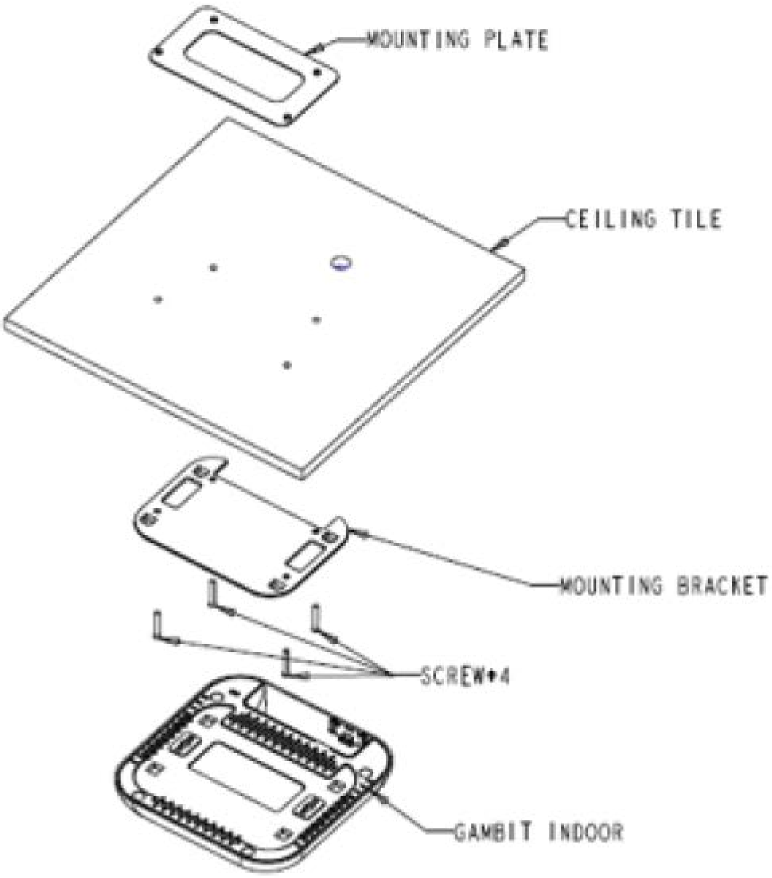
Mounting the Device

Note

For detailed information on Mounting and Installing the device, please refer to the cnPilot Quick Start Guide of respective cnPilot Enterprise AP.

Mounting E400/e410/e600

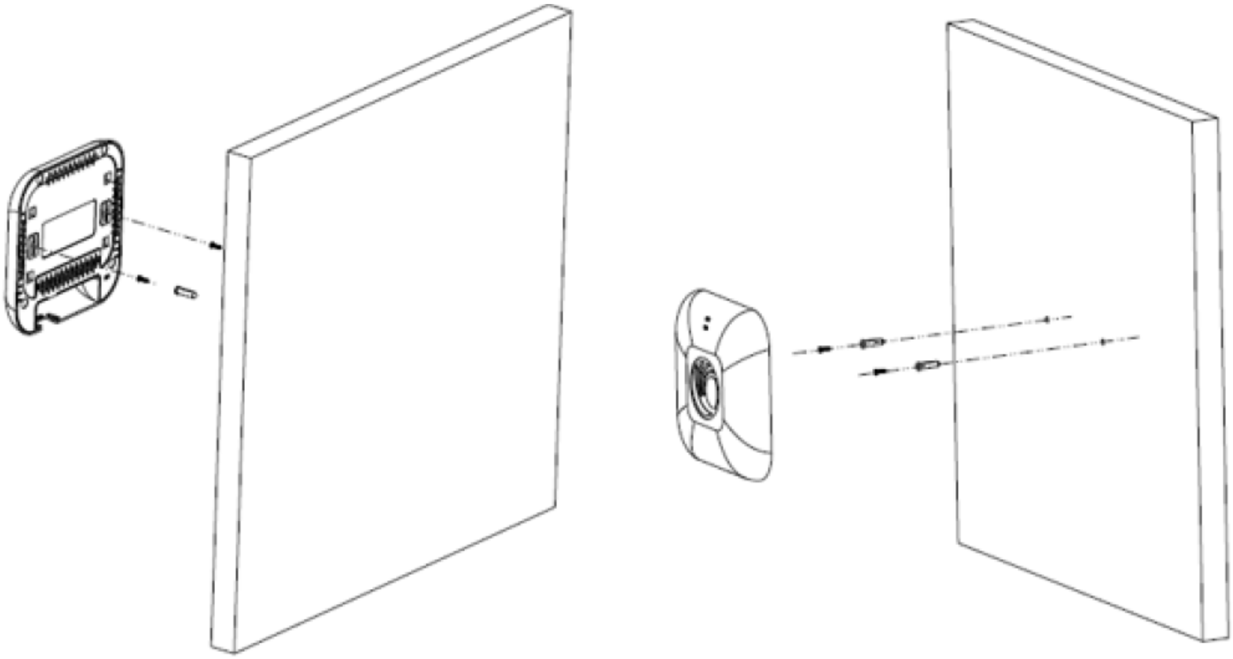
Ceiling Installation



Instructions:

1. Determine where E400 needs to be mounted and remove the ceiling tile.
2. Using the hole template, mark the hole locations.
3. Drill the holes for the 4 mounting screws using a 5mm (3/6”) diameter drill bit.
4. Drill the RJ45 cable hole using a 15 mm (5/8”) diameter bit.
5. Hold the mounting plate on the top side of the ceiling tile and screw it on the mounting bracket.
6. Run the RJ45 cable through the 15mm hole and remount the ceiling tile
7. Attach the RJ45 cable to E400
8. Slide E400 onto the mounting bracket

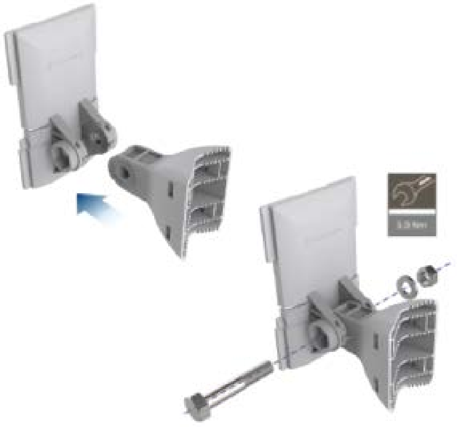
Wall Installation



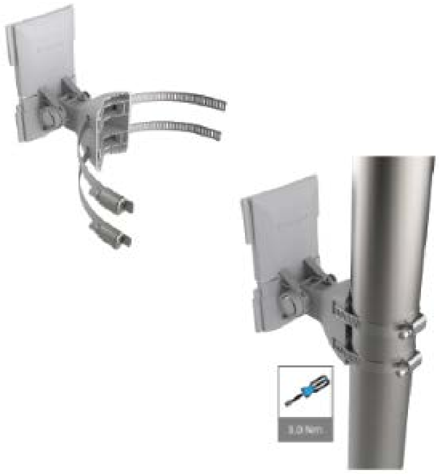
Mounting E500/E50XS

Pole Mount

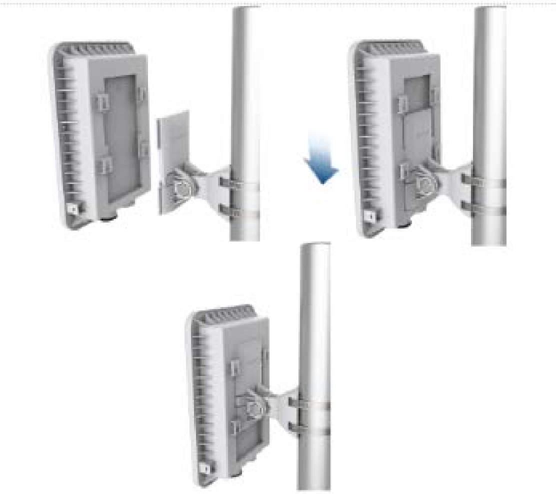
Assemble the radio holder to the pole mounting bracket and secure it with M8 nuts by applying 3.0 Nm torque.



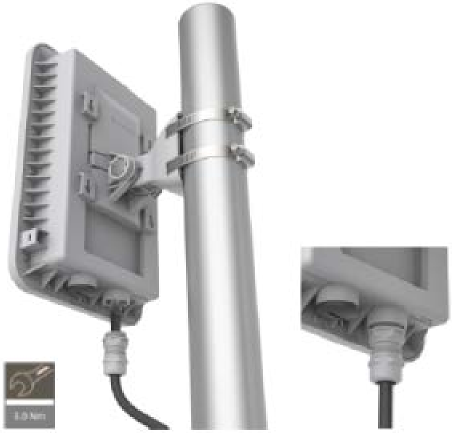
Insert hose clamps through pole mounting bracket and clamp to pole by applying 3.0 Nm torque.



Align the radio chassis with the guide rails of radio holder and slide it downwards until it clicks into place.

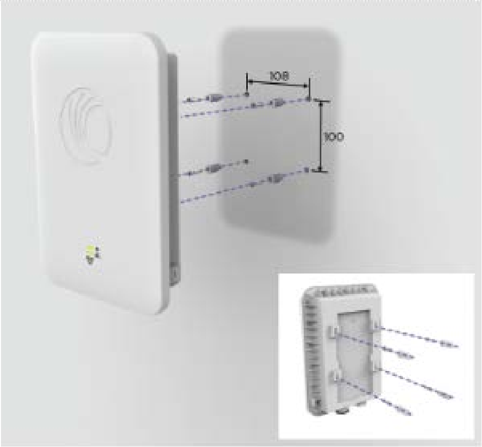


Insert RJ45 to radio housing and the lock cable gland to radio housing with 1.5Nm to 2Nm torque.



Wall Mount

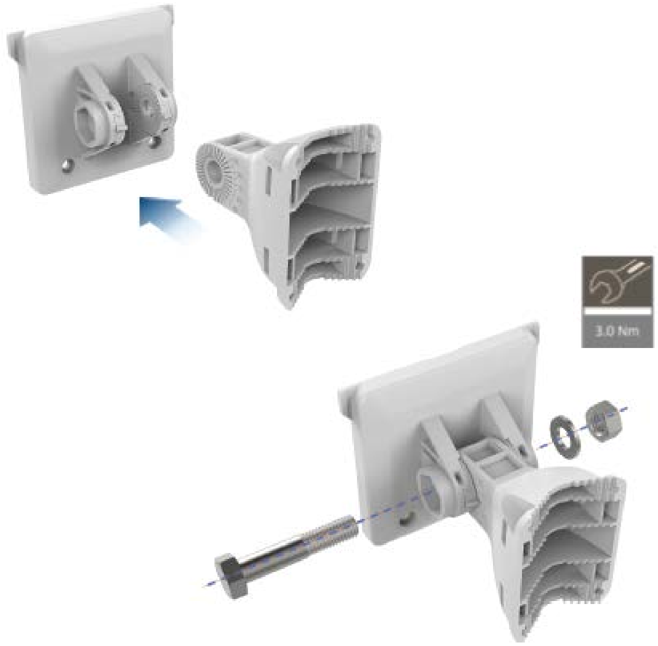
Drill 4 holes of Ø6mm (Ø0.25”Inch) on wall. Press fit plastic anchor and assembly fastener. Leave 5mm to 6mm gap between wall and fastener head. Use the four mounting slots given on the back of the radio to mount to the wall.



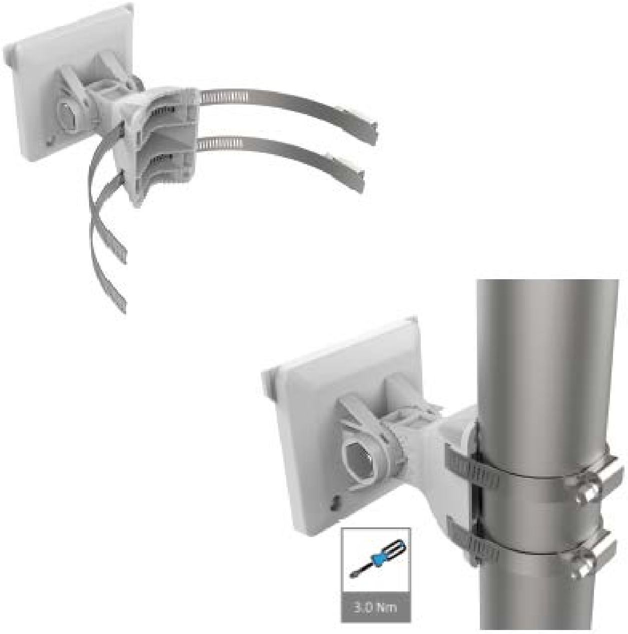
Mounting e700

Pole Mount

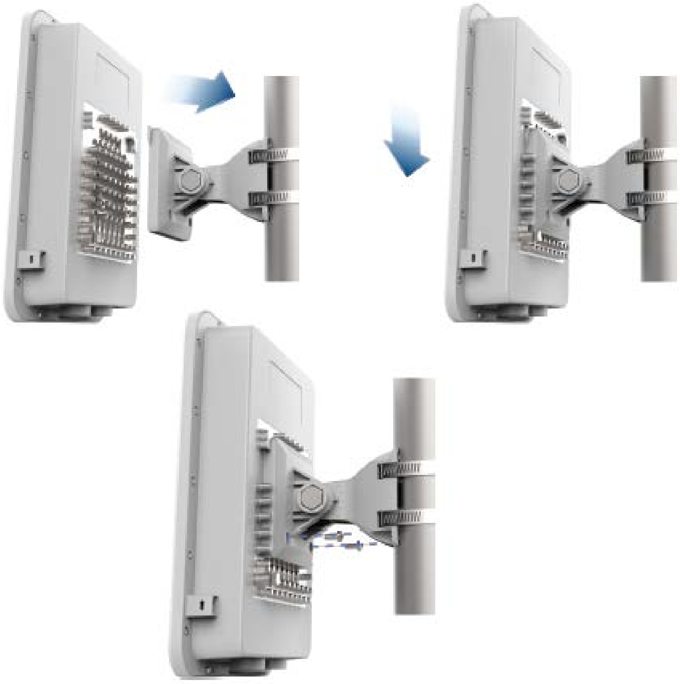
1. Assemble the radio holder to the pole mounting bracket and secure it with M8 nuts by applying 3.0 Nm torque.



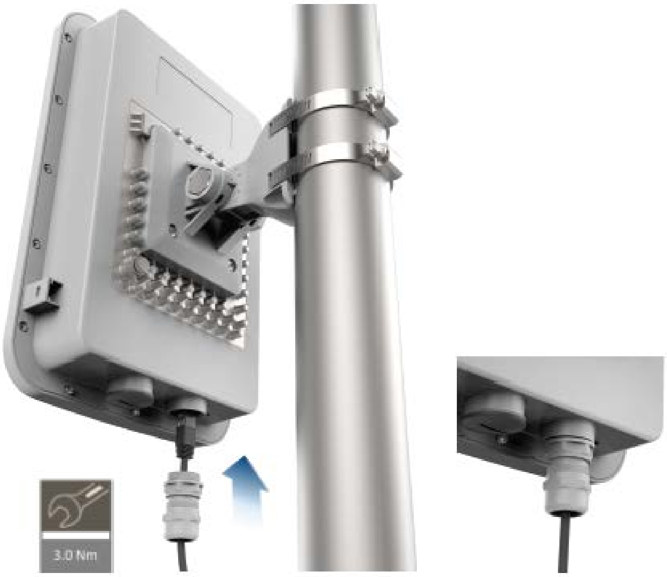
2. Insert hose clamps through pole mounting bracket and clamp to pole by applying 3.0 Nm torque.



3. Align the radio chassis with the guide rails of radio holder and slide it downwards until it clicks into place.



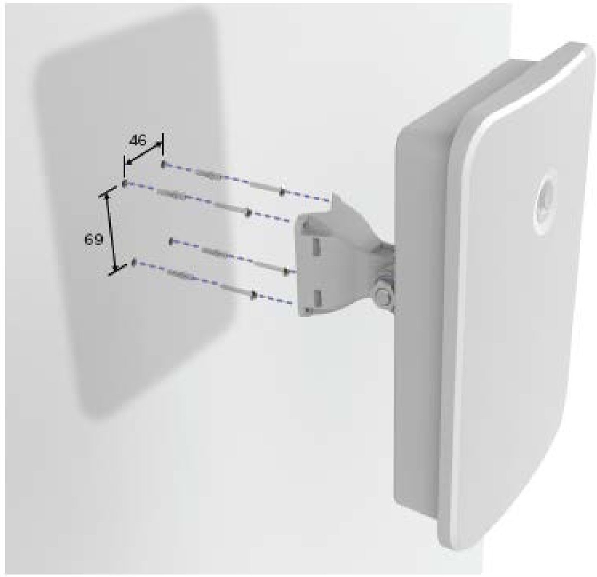
4. Insert RJ45 to radio housing and the lock cable gland to radio housing with 1.5Nm to 2Nm torque.



5. Align Radio to required angle by tilting up and down. The maximum radio tilting angle is ± 40°, with an incremental of 10°

Wall Mounting

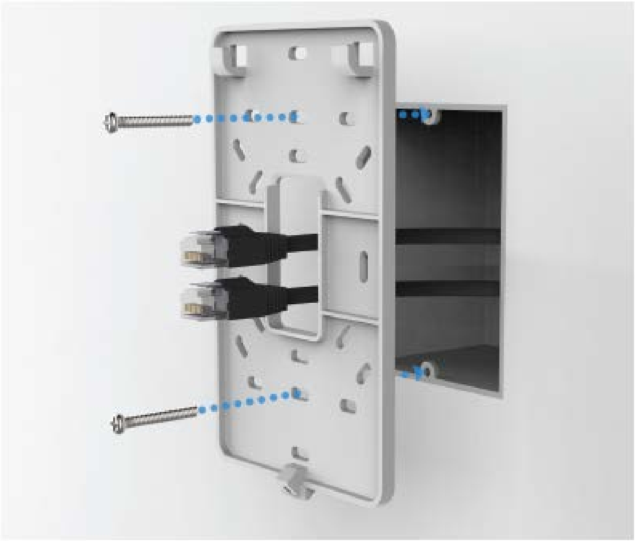
Drill 4 holes of Ø6mm (Ø0.25”Inch) on wall. Press fit plastic anchor and assembly fastener. Leave 5mm to 6mm gap between wall and fastener head. Use the four mounting slots given on the back of the radio to mount to the wall.



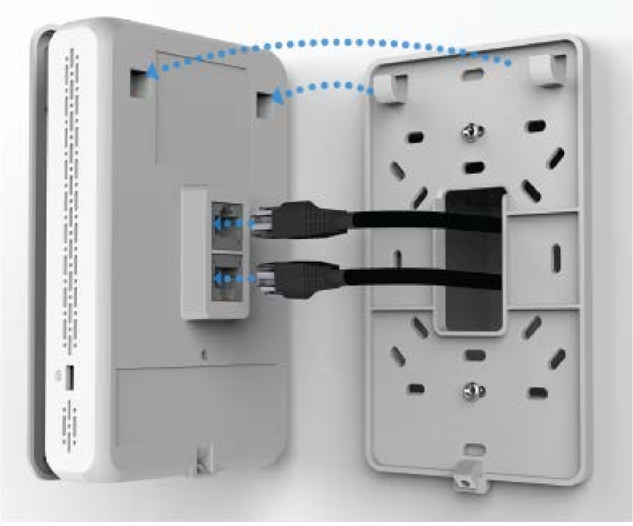
Mounting e430W/e430H

Single Gang Mounding

1. Remove single-gang box cover.
2. Place Cambium single-gang wall bracket on the gang box and secure with atleast 2 screws.



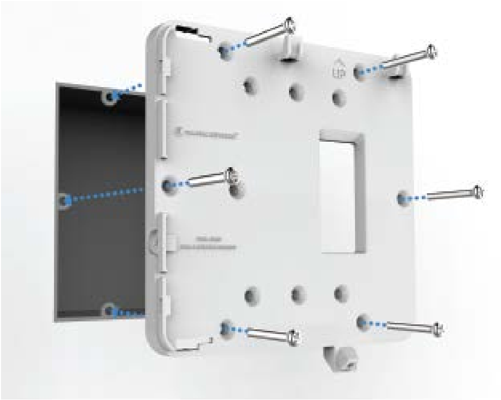
3. Connect Ethernet cable to the upper RJ-45 port labeled Eth1/PoE at the rear side of e430W to provide connectivity. Use the other RJ-45 port labeled PASS-Through for any additional cable that might need to pass through e430W.
4. Align the two slots at rear side of the e430W with two hooks on the bracket.



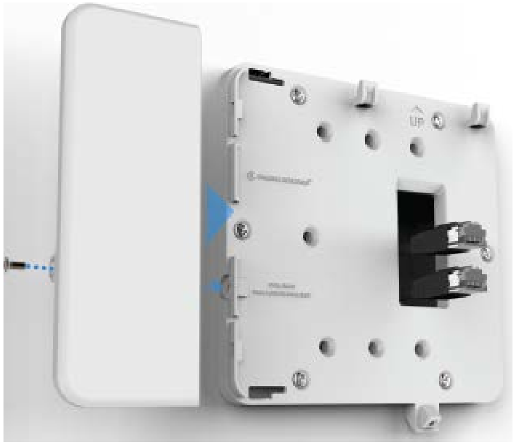
5. Secure e430W to the bracket with a screw at the bottom edge of e430W using standard Torx security screw or standard Philips head screw.

Dual Gang Mounding

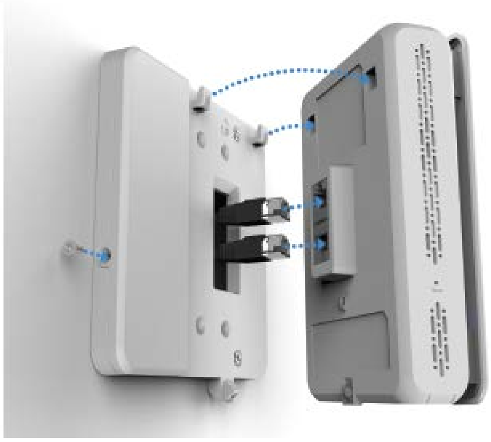
1. Remove dual-gang box cover.



2. Place Cambium dual-gang wall bracket on the gang box and secure with at least two screws.



3. Slide the plastic cover over the exposed portion next to the mounted e430W.
4. Connect Ethernet cable to the upper RJ-45 port labeled Eth1/PoE at the rear side of e430W to provide connectivity. Use the other RJ-45 port labeled Pass-thru for any additional cable that might need to pass through e430W.

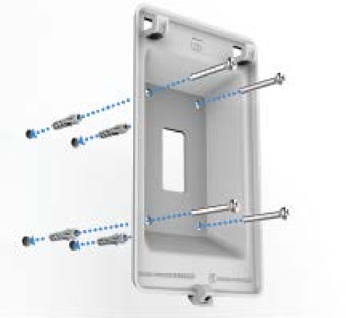


5. Align the two slots at rear side of e430W with two hooks on the bracket.

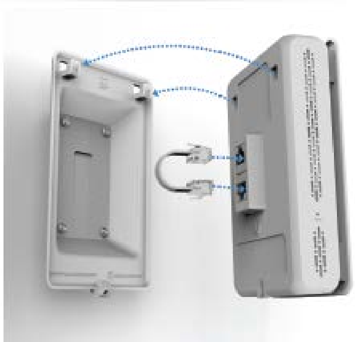
6. Secure e430W to the bracket with a screw at the bottom edge of e430W using standard Philips head or Torx security screwdriver.

Wall Mounting

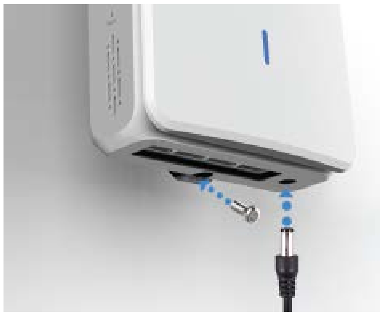
1. Choose location on the wall to mount the bracket using the four mounting screws and anchors (if needed).



2. Connect the short Ethernet jumper cable between the two RJ-45 connections on the rear side of e430W.
3. Mount e430W into the Generic Wall bracket by aligning the hooks.



4. Secure e430W to the bracket using Torx (or standard) screw on the lower edge of e430W.
5. Power e430W either with a 48Vdc/1A power adapter or using the PASS-THRU port at the bottom edge of the device using Ethernet power.



Powering Up the Device

Follow the below procedure to power up:

1. Connect the Ethernet cable from Eth1/PoE-IN of E501S 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

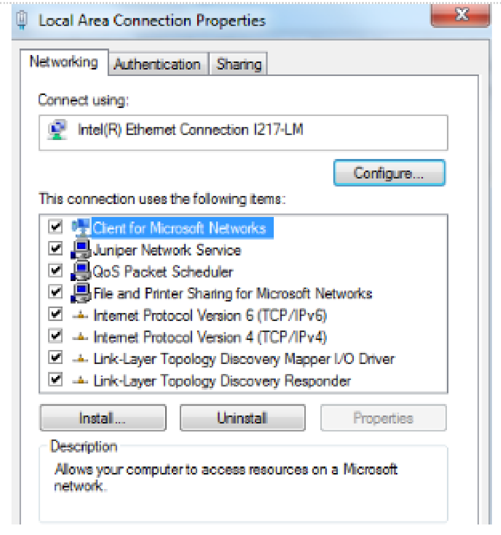
Note

1. If Aux Port is used to power a secondary device, the maximum cable length between Access Point 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 as shown in the figure 3.
3. If Aux 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. Once powered ON -- Power LED should illuminate continuously on the PoE Adapter.

Configure Management PC

1. Select Properties for the Ethernet port. In Windows it is found in Control Panel > Network and Internet > Network Connections > Local Area Connection.



Connect using:

Intel(R) Ethernet Connection I217-LM

This connection uses the following items:

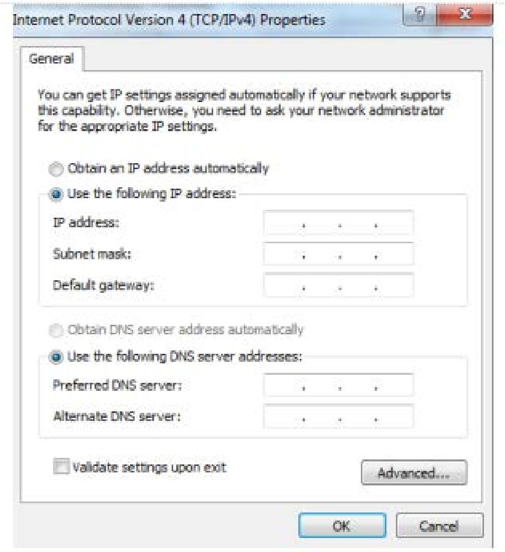
- ☑ Client for Microsoft Networks
- ☑ Juniper Network Service
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology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

Description

Allows your computer to access resources on a Microsoft network.

2. IP Address Configuration

cnPilot Access Point obtains its IP address from a DHCP server. A default IP address of 192.168.0.1 will be used if an IP address is not obtained from DHCP.



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: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

3. Default Login information

Username: admin
Password: admin
Management Protocols enabled by default –http or https (webpage management interface access), SSH (CLI management interface access).

Accessing the Device UI

Follow the below procedure to access the device UI:

1. Using a web browser, navigate to 169.254.X.Y and login with username: admin and password: admin
2. Configuration - IP Address, a Subnet Mask, and a Gateway IP Address OR DHCP state to Enabled to have the IP address, subnet mask, and gateway IP address automatically configured by a DHCP server.
3. Click **Go To Next** Page.
4. Click Save Changes.

Accessing the Device CLI

cnPilot Enterprise AP supports a powerful and structured Command Line Interface (CLI) that can be used for managing the device over SSH or Telnet.
The CLI can be used to configure any system parameter, to view the system status and statistics, and for actions such as reloading the device, or importing and exporting configuration from it. Several troubleshooting tools such as packet-capture and ping are also supported in the CLI.
The CLI is hierarchical, in addition to a global mode for system-wide commands, there are separate modes for Wireless LAN, Radio, Etherent, VLAN, and DHCP server configuration. These specific modes are entered by specifying the instance of the mode.

Use the following CLI to configure wireless LAN 1 parameters:

```
cnWest-5ghz(config)# wireless wlan 1
cnWest-5ghz (config-wlan-1)#
```

Use the following CLI to exit from a mode back to the global context type exit command:

```
cnWest-5ghz(config-wlan-1)# exit
cnWest-5ghz(config)#
```

The default login and password for the CLI are admin. The password can be changed using the management user admin password command.

- Entering ? displays the command menu and any context specific help.
- Pressing &lt;TAB&gt; completes a partially typed CLI command wherever possible.
- Commands to view system status and statistics begin with show.
- Commands to default or negate a configuration begin with no.

Example

Some of the commonly used CLI commands are:
Show config — Displays system configuration.
Save — Used to apply and save any configuration changes.
Show version — Displays the basic device information and firmware version.

Command Line Interface (CLI)

Overview

The cnPilot Enterprise AP supports a powerful and structured Command Line Interface (CLI) that can be used for managing the device over SSH or Telnet.
The CLI can be used to configure any system parameter, to view the system status and statistics, and for actions such as reloading the device, or importing and exporting configuration from it. Several troubleshooting tools such as packet-capture and ping are also supported in the CLI.

The CLI is hierarchical, in addition to a global mode for system-wide commands, there are separate modes for Wireless LAN, Radio, Etherent, VLAN, and DHCP server configuration. These specific modes are entered by specifying the instance of the mode.

Use the following CLI to configure wireless LAN 1 parameters:

```
•       cnWest-5ghz(config)#
•       cnWest-5ghz(config)# wireless wlan 1
•       cnWest-5ghz(config-wlan-1)#
```

Use the following CLI to exit from a mode back to the global context type ***exit*** command:

```
•       cnWest-5ghz(config-wlan-1)# exit
•       cnWest-5ghz(config)#
```

The default login and password for the CLI are **admin**. The password can be changed using the ***management user admin password*** command.

- Entering **?** displays the command menu and any context specific help.
- Pressing **<TAB>** completes a partially typed CLI command wherever possible.
- Commands to view system status and statistics begin with ***show***.
- Commands to default or negate a configuration begin with ***no***.

Example

Some of the commonly used CLI commands are:

Show config — Displays system configuration
Save — Used to apply and save any configuration changes
Show version — Displays the basic device information and firmware version

System Configuration

This section describes the System, Management, Time Settings, and Event Logging functionalities of cnPilot Enterprise AP.

System

The following table lists the fields that are displayed in the **Configuration > System** page:

Table 2: Configuration: **System** parameters

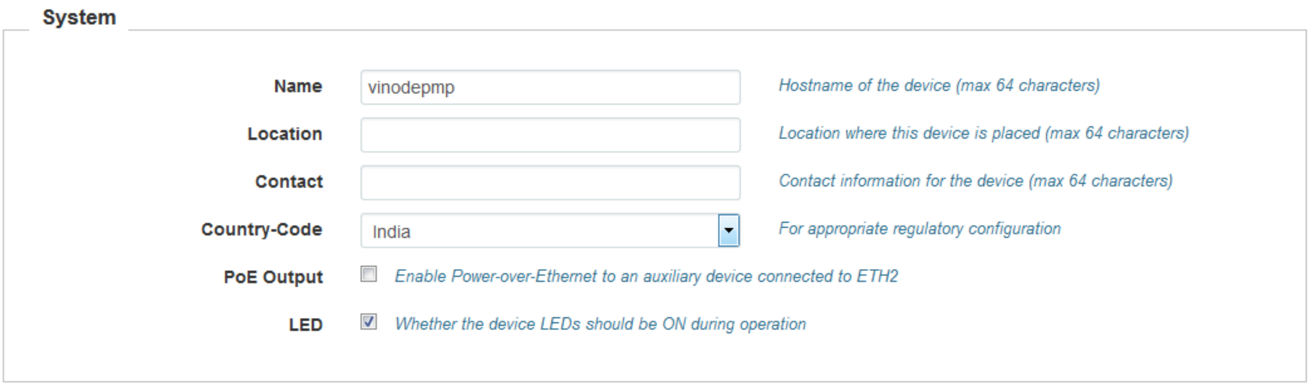
Parameter	Description	Default Value
Name	Hostname of the device. The maximum length of name is 64 characters.	–
Location	The location where the device is placed. The maximum length of location is 64 characters. By adding the RADIUS attribute, **WISPr-Location-Name** this information is sent to the RADIUS server when RADIUS auth method is used.	–
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).	–
LED	Select the LED checkbox for the device LEDs to be **ON** during operation.	–

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > System** tab. The following fields are displayed in **System**:
   a. Enter the hostname of the device in the **Name** text box.
   b. Enter the location where this device is placed in the **Location** text box.
   c. Enter the contact details of the device is placed in the **Contact** text box.
   d. Select the appropriate country code for the regulatory configuration from the **Country-Code** text box.
   e. Select the LED checkbox for the device LEDs to be **ON** during operation.
2. Click **Save**.

Figure 1: Configuration: **System** page



System

Name: vinodepmp — *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*

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

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

In the CLI

To change the hostname:

```
(cnPilot Enterprise AP) (configure)# hostname <name>
```

To change the location:

```
(cnPilot Enterprise AP) (configure)# location
```

To change the country-code:

```
(cnPilot Enterprise AP) (configure)# country-code
```

To view the list of all country-codes:

```
(cnPilot Enterprise AP) # show country-code
```

Management

The following table lists the fields that are displayed in the **Configuration > System > Management** page:

Table 3: Configuration: **System > Management** parameters

Parameter	Description	Default Value
Admin Password	Password for authentication of UI and CLI sessions.	admin
Telnet	Enable Telnet access to the device CLI.	Disabled
SSH	Enable SSH access to the device CLI.	Enabled
HTTP	Enable HTTP access to the device UI.	Enabled
HTTPS	Enable HTTPS access to the device UI.	Enabled
Cambium Remote Mgmt	Enable support for Cambium Remote Management of this device.	Disabled
Cambium ID	Cambium-ID used for provisioning cnMaestro (Cambium Remote Management) of this device.	–

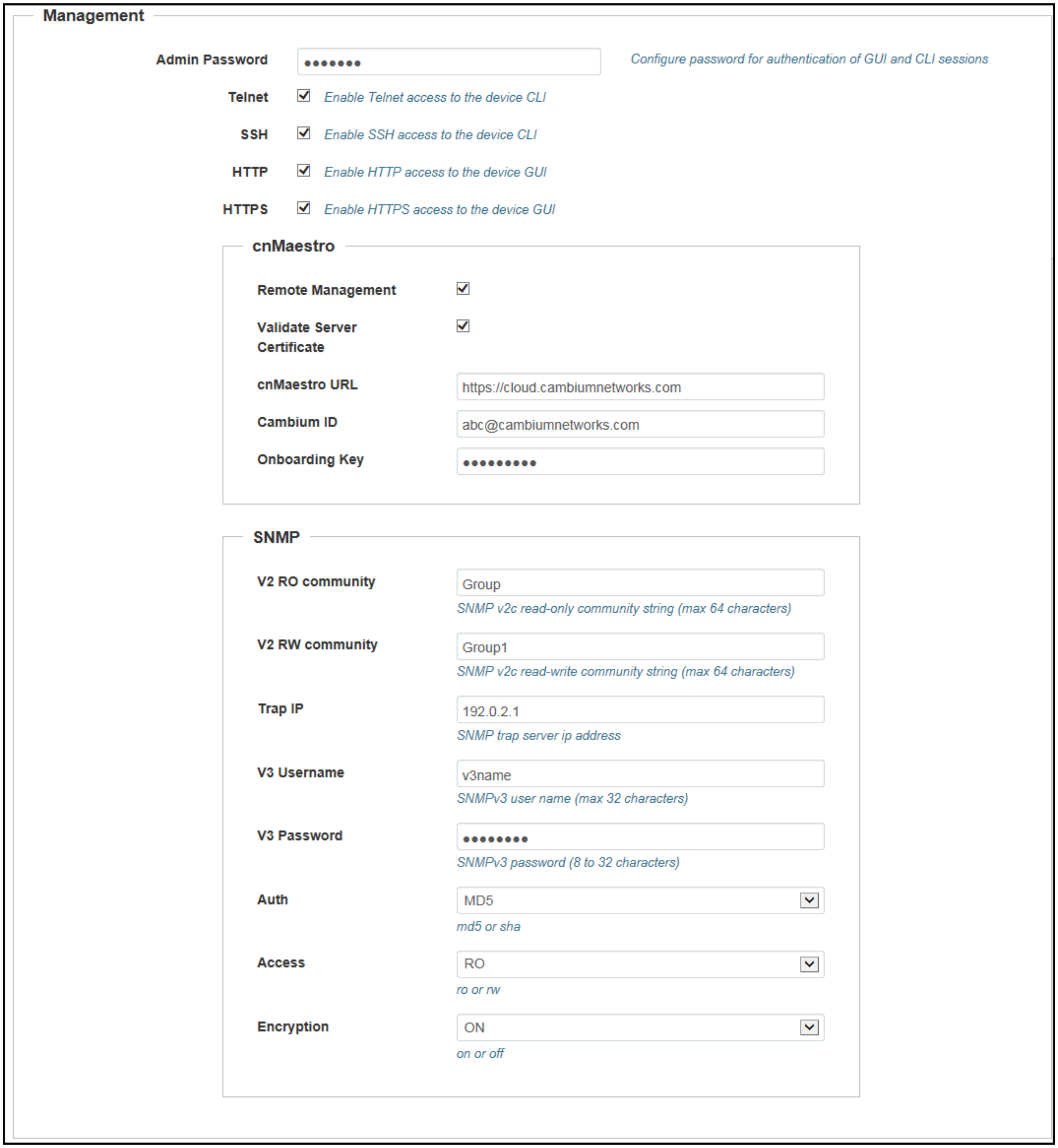
Cambium Password	Password used for onboarding the device to cnMaestro.	–
SNMP		
V2 RO Community	SNMP v2c read-only community string	–
V2 RW Community	SNMP v2c read-write community string	–
V3 Username	SNMP v3 username	–
V3 Password	SNMP v3 password	–
Auth	Choose MD5 or sha	MD5
Access	Choose RO or RW	RO
Encryption	Choose ON or OFF	ON

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > System** tab. The following fields are displayed in **Management**:
    a. Enter the admin password of the device in the **Admin Password** text box.
    b. Select **Master** or **Disabled** to enable/disable the **Autopilot** management of APs.
    c. Enable the **Telnet** checkbox to enable telnet access to the device CLI.
    d. Enable the **SSH** checkbox to enable ssh access to the device CLI.
    e. Enable the **HTTP** checkbox to enable HTTP access to the device UI.
    f. Enable the **HTTPS** checkbox to enable HTTPS access to the device UI.
    g. Under cnMaestro, enable **Remote Management** to support for Cambium Remote Management of this device.
    h. Enter the URL for cnMaestro in the **cnMaestro URL** text box.
    i. Enter the Cambium ID of the user in the **Cambium ID** text box.
    j. Enter the Onboarding Key in the **Onboarding Key** text box.
    k. Enter the SNMP v2c read-only community string in the **V2 RO community** text box.
    l. Enter the SNMP v2c read-write community string in the **V2 RW community** text box.
    m. Enter the SNMP V3 username in the V3 Username text box.
    n. Enter the SNMP V3 password in the V3 Password text box.
    o. Choose **MD5** or **SHA** from the **Auth** drop-down list.
    p. Choose **RO** or **RW** from the **Access** drop-down list.
    q. Choose **ON** or **OFF** from the **Encryption** drop-down list.
2. Click **Save**.

Figure 2: Configuration: **Management** page



Management

Admin Password	•••••••	Configure password for authentication of GUI and CLI sessions
Telnet	☑ Enable Telnet access to the device CLI	
SSH	☑ Enable SSH access to the device CLI	
HTTP	☑ Enable HTTP access to the device GUI	
HTTPS	☑ Enable HTTPS access to the device GUI	

cnMaestro

Remote Management	☑
Validate Server Certificate	☑
cnMaestro URL	https://cloud.cambiumnetworks.com
Cambium ID	abc@cambiumnetworks.com
Onboarding Key	•••••••••

SNMP

V2 RO community	Group SNMP v2c read-only community string (max 64 characters)
V2 RW community	Group1 SNMP v2c read-write community string (max 64 characters)
Trap IP	192.0.2.1 SNMP trap server ip address
V3 Username	v3name SNMPv3 user name (max 32 characters)
V3 Password	•••••••• SNMPv3 password (8 to 32 characters)
Auth	MD5 md5 or sha
Access	RO ro or rw
Encryption	ON on or off

In the CLI

To configure management:

```
(cnPilot Enterprise AP) (configure)# management {telnet, ssh, http. https}
```

To configure Cambium-ID:

```
(cnPilot Enterprise AP) (configure)# cambium-id CAMBIUM-ID PASSWORD
```

Time Settings

The user can configure upto 2 NTP servers. These are used by the AP to set its internal clock to UTC/GMT time. Note that the AP does not have a battery backup, and on power-cycle its clock will reset to default and needs to sync time again. The servers can be specified as IP addresses or as hostname (Eg: pool.ntp.org).

The following table lists the fields that are displayed in the Configuration > System > Time Settings page:

Table 4: Configuration: **System > Time Settings** parameters

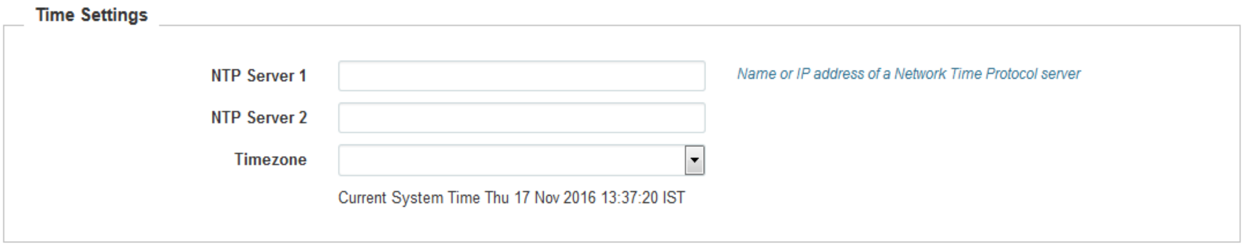
Parameter	Description	Default Value
NTP Server 1	Name or IP address of a Network Time Protocol server 1.	–
NTP Server 2	Name or IP address of a Network Time Protocol server 2.	–
Timezone	Timezone can be set according to the location where the AP is installed. By selecting the appropriate timezone from 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	–

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > System** tab. The following fields are displayed in **Time Settings**:
   a. Enter the name or IP address of the NTP server 1 in the **NTP Server 1** text box.
   b. Enter the name or IP address of the NTP server 2 in the **NTP Server 2** text box.
   c. Select the time zone settings for the AP from the **Timezone** drop-down list.
2. Click **Save**.

Figure 3: Configuration: **Time settings** page



Time Settings

NTP Server 1 — Name or IP address of a Network Time Protocol server

NTP Server 2

Timezone

Current System Time Thu 17 Nov 2016 13:37:20 IST

In the CLI

To configure NTP server:

```
(cnPilot Enterprise AP) (configure)# ntp <server>
```

To configure Timezone:

```
(cnPilot Enterprise APv) (configure)# timezone
```

To view the current system time:

```
(cnPilot Enterprise AP) # show clock
```

Onboarding to cnMaestro

Overview

cnMaestro is Cambium's next generation network management platform based on Cloud technologies. It will eventually replace the entire lineup of Network Management Tools. The initial release will include support for ePMP and cnPilot family of devices. Subsequent releases will add the remaining devices in the Cambium portfolio. The legacy and 3rd party devices will be supported by a proxy application.
In addition to the Cloud installments, the solution can also be installed as a standalone, redundant server solution for installments where access to the Internet is restricted or forbidden.

Onboarding Steps

You can onboard cnPilot Enterprise AP to cnMaestro by using the following steps:

1. To enable Cambium Remote Management:

```
(cnPIlot Enterprise AP) # management cambium-remote
```

2. If the device does not have a unique Serial Number (MSN), then set the cambium-id/password obtained from Cambium Support:

3. If the device is claimed and is able to reach the cnMaestro, it will get on-boarded. The cnMaestro connection status can be seen under “Cambium Remote Management Status”.

To view the connection status:

```
(cnPIlot Enterprise AP) # cambium-id <cambium-id> <password>
(cnPIlot Enterprise AP # management cambium-remote
url https://cloud.cambiumnetworks.com

(cnPIlot Enterprise AP) # apply
(cnPIlot Enterprise AP) # save
(cnPIlot Enterprise AP) # show management
```

Remote Management

Config : Enabled
URL : https://cloud.cambiumnetworks.com
Status: Not Connected

Zero Touch Provisioning

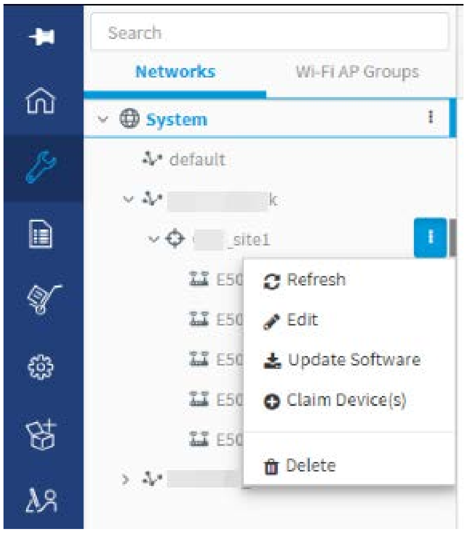
cnPilot Enterprise AP supports zero touch configuration, which makes the deployment of APs plug-n-play.

Steps for Zero-Touch Configuration of AP:

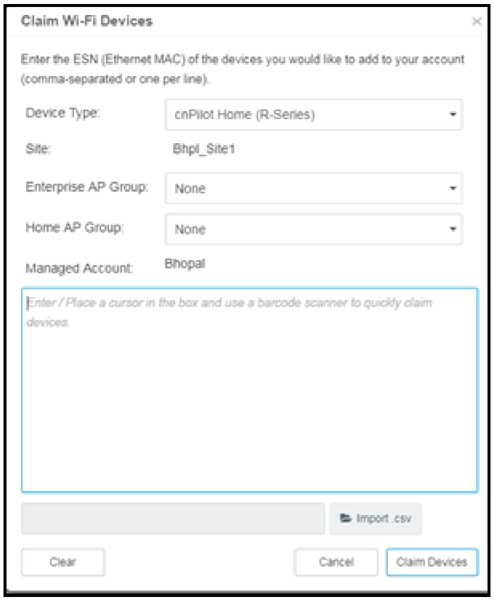
1. Create a Network Topology which has sites configured/enabled in it.
2. Claim your devices on respective Sites as follows:

a. Login to GUI of cnMaestro.

b. Navigate to site and click claim devices



c. Configure AP Group profile for the same.



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 Home (R-Series)

Site: Bhpl_Site1

Enterprise AP Group: None

Home AP Group: None

Managed Account: Bhopal

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

Import .csv

Clear   Cancel   Claim Devices

Wireless Configuration

The wireless settings are divided into the following:

- Radio configuration
- WLAN configuration

Radio Configuration

cnPilot Enterprise AP is a dual band radio solution which operates on 5GHz and 2.4GHz bands concurrently. The dashboard menu in the UI displays the channel and band from the CLI, **show wireless radios** displays the details of the radio.

The following table lists the fields that are displayed in the **Configure > Radio** page and select **Radio 1(2.4GHz)** or **Radio 2(5GHz)** from the drop-down list.

Table 6: Configure: **Radio** parameters

Parameter	Description	Default Value
Enable	Enables operation of this radio.	–
Channel	Primary operating channel.	Auto
Channel Width	Operating width of the channel.	20MHz for 2.4GHz and 80MHz for 5GHz
Transmit Power	Radio transmit power in dBm (1 to 30)	30dBm
Antenna Gain	Gain of connected antenna, in dBm (1 to 30)	–
Beacon interval	Beacon interval in ms (100 to 3400)	100
Multicast Data Rate	Multicast in highest-basic, lowest-basic and highest-supported.	Highest Basic for 2.4GHz and Lowest Basic for 5GHz
Airtime Fairness	Airtime Fairness is a solution on access points (AP) 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	Select available channel.	–
IGMPv3 **(CLI Only)**	Multicast packets are converted to unicast before it is being sent to the interested clients. This feature is mostly used for multicast video streaming.	

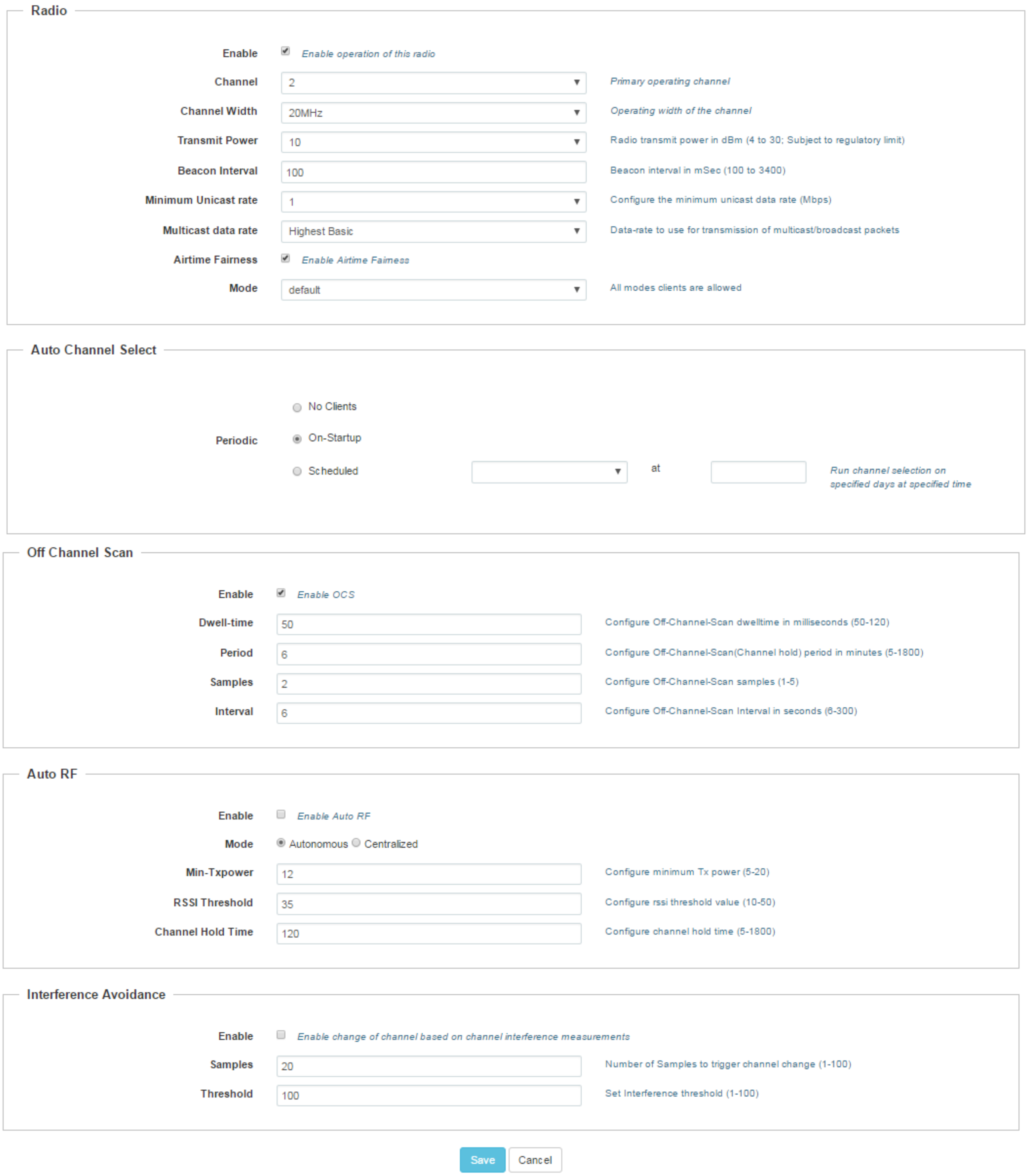
The default channel configuration is set to auto, with this the AP sets the radio to best available channel based on the interference and Noise Floor.
The country-code set in **System** page effects channel selection. Only the channels that are allowed in the country code should be selected.

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configure > Radio** tab and select **Radio 1(2.4GHz)** or **Radio 2(5GHz)** from the drop-down list. The following fields are displayed in **Radio**:
   a. Select the **Enable** checkbox to enable the operations of this radio.
   b. Select the primary operating channel from the **Channel** drop-down list.
   c. 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. We do not support 40 MHz and 80 MHz in 2.4 GHz.
   d. Enter the radio transmit power in the **Transmit Power** text box.
   e. Enter the antenna gain of connected antenna in the **Antenna Gain** text box.
2. Enter the beacon interval in the **Beacon Interval** text box.
3. Select **Highest Basic** or **Lowest Basic** or **Highest Supported** from the **Multicast data rate** drop-down list.
4. To enable Airtime Fairness, select the **Enable Airtime Fairness** checkbox.
5. Select the preferred **Candidate Channels** from the drop-down list.
6. Click **Save**.

Figure 5: Configure: **Radio** page



Radio

Enable	☑ *Enable operation of this radio*	
Channel	2 ▼	*Primary operating channel*
Channel Width	20MHz ▼	*Operating width of the channel*
Transmit Power	10 ▼	Radio transmit power in dBm (4 to 30; Subject to regulatory limit)
Beacon Interval	100	Beacon interval in mSec (100 to 3400)
Minimum Unicast rate	1 ▼	Configure the minimum unicast data rate (Mbps)
Multicast data rate	Highest Basic ▼	Data-rate to use for transmission of multicast/broadcast packets
Airtime Fairness	☑ *Enable Airtime Fairness*	
Mode	default ▼	All modes clients are allowed

Auto Channel Select

	○ No Clients				
Periodic	● On-Startup				
	○ Scheduled	▼	at		*Run channel selection on specified days at specified time*

Off Channel Scan

Enable	☑ *Enable OCS*	
Dwell-time	50	Configure Off-Channel-Scan dwelltime in milliseconds (50-120)
Period	6	Configure Off-Channel-Scan(Channel hold) period in minutes (5-1800)
Samples	2	Configure Off-Channel-Scan samples (1-5)
Interval	6	Configure Off-Channel-Scan Interval in seconds (6-300)

Auto RF

Enable	□ *Enable Auto RF*	
Mode	● Autonomous ○ Centralized	
Min-Txpower	12	Configure minimum Tx power (5-20)
RSSI Threshold	35	Configure rssi threshold value (10-50)
Channel Hold Time	120	Configure channel hold time (5-1800)

Interference Avoidance

Enable	□ *Enable change of channel based on channel interference measurements*	
Samples	20	Number of Samples to trigger channel change (1-100)
Threshold	100	Set Interference threshold (1-100)

Advanced Radio Settings

You can configure the following advanced radio settings on cnPilot Enterprise AP:

- **Scheduled ACS (Auto Channel Select**) - When Scheduled ACS is configured, the radio scans all the channels available in the frequency band and selects the best available channel. Scheduled ACS can be configured to scan on-startup or periodic. (Run channel selection on specified days at specified time).

Table 7: Configure: **Radio > Auto Channel Select** parameters

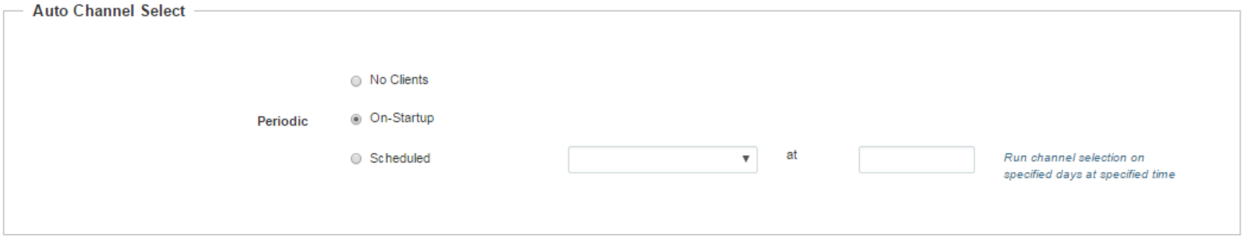
Parameter	Description	Default Value
Periodic	Run channel selection on specified days at specified time. • No Clients • On-Startups • Scheduled	–

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configure > Radio** tab. The following fields are displayed:
   a. Select the **Channel** as **Auto**.
   b. Select **No Clients** radio button if clients are not connected.
2. Click **Save**.

Figure 6: Configure: **Auto Channel Select** page



Auto Channel Select

Periodic ○ No Clients
● On-Startup
○ Scheduled ▾ at

Run channel selection on specified days at specified time

In the CLI

To configure IGMPv3 Support:

To enable Multicast to Unicast Conversion:

```
        (Cambium AP) (configure)# mc2uc
```

To disable Multicast to Unicast Conversion:

```
        (Cambium AP) (configure)# no mc2uc
```

```
(cnPilot Enterprise AP) (configure)# wireless radio 1
(cnPilot Enterprise AP) (config-radio-1)# channel-list

(cnPilot Enterprise AP) (configure)# wireless radio 1

(cnPilot Enterprise AP) (config-radio-1)# channel-list
```

To configure Auto Channel Select:

```
(cnPilot Enterprise AP) (configure)# wireless radio 1
(cnPilot Enterprise AP) (config-radio-1)# channel-list
(cnPilot Enterprise AP) (config-radio-1)# auto-channel-select
```

- **Auto RF –** Interference is an unavoidable threat while installing access points due to large number of APs skyrocketing. The Auto-RF feature monitors the spectrum and collectively handles decision making on groups of access points and not on individual AP basis. In addition to interference, Auto-RF also monitors client channel availability by providing the best in class automatic channel.

Table 7: Configure: **Radio > Auto RF** parameters

Parameter	Description	Default Value
Channel hold Time	Configures channel hold time in minutes.	120
Channel Utilization Threshold	Configures channel change limit. The AP switches whenever the total weight value (difference of best & current channel) > (channel-change-limit). **Note:** For system release 3.9, this parameter is valid only for E400/E500/E50XS.	25
Packet Error Rate Threshold	Configures packet retransmission rate. **Note:** For system release 3.9, this parameter is valid only for E400/E500/E50XS.	30
Off Channel Scan		
Dwell Time	Off Channel scan dwell time in milliseconds (50-120).	50

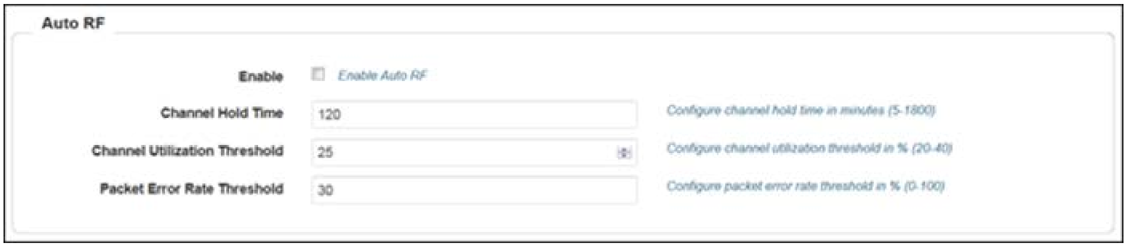
Auto-RF Packet Error Rate Changes

Auto-RF is a feature that continuously attempts to find the optimal channel of operation for the radios on the AP. The existing method of Auto-RF called AP-Interference (API) based method achieves this by detecting nearby APs (both Cambium and non-Cambium) and moving the cambium APs to other channels where the interference from the heard APs is the least. By minimizing the interfering neighbors in this way, the API method tries to optimize the overall congestion levels to enhance throughput.

The new PER (packet error rate) based method adds a new facility to the API method that provides switching out of the current channel if SoS conditions are detected. It takes into the account the actual congestion levels and not just the interference from nearby APs. Note that there may be many wireless services (or APs) operating nearby but they may not be sending much data traffic at all. The API method would still try to move away from the channels on which those services are operating. Whereas the PER method measures the performance on those channels and determines if there is not much harm around and might simply decide to continue operating there. The gist of the PER method is below.

PER engine continuously monitors the TX per (packet error rate) value on the current operating channel. If the value goes above a configured threshold for a period of observation that lasts a few minutes, it switches out of the current channel to the next best channel determined by the API method. Thus, both the API and the PER engines will run at the same time. While the API method makes channel switching decisions over the longer term, the PER method helps to come out of SoS conditions in the shorter term. Both the methods in together provides formidable performance for the network.

Figure 6: Configure: **Auto RF** page



Auto RF

Enable □ *Enable Auto RF*

Channel Hold Time 120 *Configure channel hold time in minutes (5-1800)*

Channel Utilization Threshold 25 *Configure channel utilization threshold in % (20-40)*

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

In the CLI

To configure Auto-RF:

```
(cnPilot Enterprise AP) (configure)#auto-rf
(cnPilot Enterprise AP) (configure)#auto-rf chan-hold-time 120
(cnPilot Enterprise AP) (configure)#auto-rf packet-error-rate-threshold 30
(cnPilot Enterprise AP) (configure)#auto-rf channel-utilization-threshold 25
```

To view the configuration:

```
(cnPilot Enterprise AP) #show auto-rf
   RADIO      AUTO-RF      CHAN    POWER
   2.4Ghz     enabled      auto    static
   5Ghz       enabled      auto    static

(cnPilot Enterprise AP) #show wireless radios rf-statistics
Radio1
Noise Floor                : -96
Interference               : 49
Throughput                 : (null)
Airtime (total/tx/rx/busy) : 48/5/43/0
Radio2
Noise Floor                : -111
Interference               : 30
Throughput                 : (null)
Airtime (total/tx/rx/busy) : 30/1/29/0

(cnPilot Enterprise AP) #show auto-rf per-channel-effective-interference
RADIO      CHANNEL         Effective-Interefence(dbm)  Utilization(%) Score-value
PER(%)
```

```
0             1                     -28                       58          42        -1
0             6                     -32                       58          42        -1
0             11                    -26                       60          40        -1
1             42                    -39                       38          61        -1
1             58                    -60                       14          85        -1
1             155                   -53                       10          90        -1

(cnPilot Enterprise AP) #show auto-rf stats
Radio  Time-Window(hours)  Intf-based-switches   CU-based-switches PER-based-switches
0             1                  1                       0                   0
0             4                  1                       0                   0
0             8                  1                       0                   0
0             24                 1                       0                   0
1             1                  1                       0                   0
1             4                  1                       0                   0
1             8                  1                       0                   0
1             24                 1                       0                   0

(cnPilot Enterprise AP) #show auto-rf history
2018-11-16 09:12:00 - Channel change : 5GHz from channel 149 width 80 interference (-
64) to channel 36 width 80 interference (-67) reason (High Intf on channel)
2018-11-16 09:07:10 - Channel change : 2.4GHz from channel 1 width 20 interference (-
23) to channel 11 width 20 interference (-28) reason (High Intf on channel)
```

To analyse the logs related to Auto-RF set the logging level to debug and save the setting then download the techsupport dump or through show command.

```
(cnPilot Enterprise AP) #service debug auto-rf logging-level debug
(cnPilot Enterprise AP) #Save
(cnPilot Enterprise AP) #service show debug-logs wifid
```

- **Enhanced Roaming** - When enhanced roaming is enabled, the clients are forced to roam when the SNR is below the configured value. This is useful when clients are connected to the AP that is far away and stick to that AP. With enhanced roaming, the AP disconnects the client is the SNR is less than the configured which makes client to find the better AP and roam to it. This is useful in a dense environment and multi-AP setup. It is disabled by default and user should understand his installments topology and then only enable this, user should enable only if he is sure what they want and the threshold should to be set accordingly.

The following table lists the fields that are displayed in the **Configure > Radio > Enhanced Roaming** page:

Table 8: Configure: **Radio > Enhanced Roaming** parameters

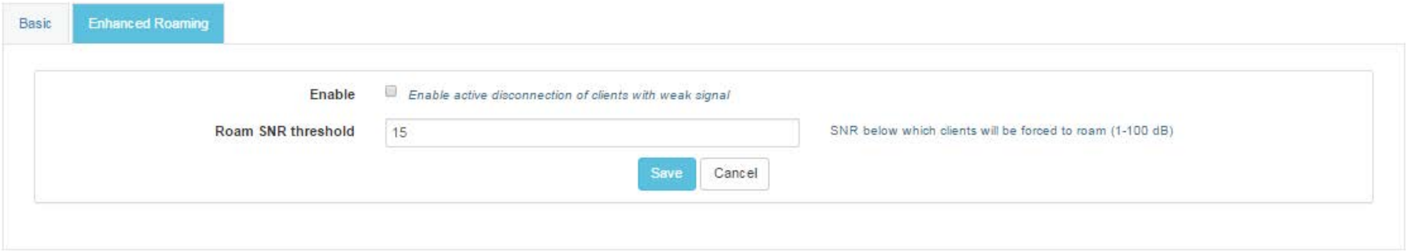
Parameter	Description	Default Value
Enable	Enable active disconnection of clients with weak signal.	Disabled
Roam SNR Threshold	SNR below which clients will be forced to roam (1-100 dB).	–

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configure > Enhanced Roaming** tab. The following fields are displayed:
   a. Select the **Enable** checkbox to enable active disconnection of clients with weak signal.
   b. Enter **Roam SNR Threshold** value between 1-100.
2. Click **Save**.

Figure 7: Configure: **Radio > Enhanced Roaming** tab



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)

In the CLI

To configure Enhanced Roaming:

```
(cnPilot Enterprise AP) (configure)# wireless radio 1
(cnPilot Enterprise AP) (config-radio-1)# enhanced-roaming
(cnPilot Enterprise AP) (config-radio-1)# enhanced-roaming threshold
```

WLAN Configuration

WLAN profile consists of two different parameters:

- Basic
- Advanced

Table 9: Configure: **WLAN Configuration** parameters

Parameter	Description	Default Value
Basic		
Enable	To enable a particular WLAN.	Disable
Mesh	Mesh Base/Client/Recovery mode.	Off
SSID	The SSID of this WLAN (Upto 32 characters).	–
VLAN	Default VLAN assigned to clients on this WLAN. (1-4094).	1
Security	Displays the security type • Open • WPA2 Pre-shared Keys • WPA2 Enterprise	Open

Passphrase	WPA2 Pre-shared Security passphrase or key.	–
Radios	Defines radio types (2.4GHz, 5GHz) on which this WLAN should be supported.	Both 2.4GHz and 5GHz are enabled
VLAN Pooling	To enable or disable VLAN-Pooling feature.	Disable
Max Clients	Max Client assigned to this WLAN. (1-255)	127
Client Isolation	Prevents wireless clients from communicating with each other. The client devices does not connect with each other. When the client isolation mode is enabled, the clients can only reach entries that are present in whitelist and the MAC address of the gateway as the whitelist learnt by the AP internally from the DHCP response packets and the clients can access the internet. To access any other shared resources like printers that are present within the client's subnet, MAC address of that printer should be added in client isolation whitelist.	Disable
Hide SSID	Prevents broadcasting SSID in beacons.	Disable
Session Timeout	Configure Session time in seconds (60 to 604800).	28800
Inactivity Timeout	Inactivity time in seconds (60 to 28800).	1800
Drop Multicast Traffic	To enable or disable the multicast traffic.	Disable
Advanced		
UAPSD	To enable or disable U-APSD	Disable
QBSS	To enable or disable QBSS	Disable
DTIM interval	Configure DTIM interval	1
Monitored Host	IP Address or Hostname that should be reachable for this WLAN to be active.	Disable
DNS Logging Host	With DNS logging enabled, the Access Point can generate syslogs of all DNS requests from the wireless clients, for analytics and reporting purposes.	Disable
Connection Logging Host	It sends the wireless client connectivity events to configured syslog server.	Disable

Band Steering	Steer dual band capable clients towards 5GHz radio.	Disable
Proxy ARP	Responds to ARP requests automatically on behalf of clients.	Enable
Unicast DHCP	Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients.	Enable
Insert DHCP Option-82	Enable DHCP Option-82.	Disable
Tunnel Mode	Enable tunneling of WLAN traffic over configured tunnel.	Disable
Fast-Roaming Protocol	One of the important aspect to support voice applications on Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one access point 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: • Pre-authentication: This roaming method was proposed in 802.11i standard. Access points supporting this method indicates their capability using pre-authentication flag in RSN capabilities element of the RSN-IE. **Note:** Pre-authentication is not supported from 3.1 release onwards. • 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 access point.	Disable

	- 802.11r: This is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT).	
802.11 w State	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. Select any one of the following: • Disable • Optional • Mandatory	Optional

You can configure the above parameters through the UI or CLI.

In the UI

To configure basic WLAN parameters:

1. Navigate to the **Configure > WLAN** tab. The following fields are displayed:
   a. Select the **Enable** checkbox to enable a particular WLAN.
   b. Enter the SSID name for this WLAN in the **SSID** textbox.
   c. Enter the default VLAN assigned to the clients on this WLAN in the **VLAN** textbox.
   d. Select the security type as Open, WPA2 Pre-shared Keys, or WPA2 Enterprise from the **Security** drop-down list.
   e. Select the Radio type from the drop-down list
      - 2.4GHz and 5GHz
      - 2.4GHz
      - 5GHz
   f. To enable **VLAN pooling** feature, select **Radius Based** from the drop-down list.
   g. Select the **Client Isolation** checkbox to prevent wireless clients from communicating to each other.
   h. Select the **Hide SSID** checkbox for not broadcast SSID in beacons.
   i. Enter the session timeout value in the **Session Timeout** textbox.
   j. Enter the inactivity timeout value in the **Inactivity timeout** textbox.

k. Select the **Drop Multicast Traffic** to enable dropping multicast traffic.

To configure advanced WLAN settings:

a. Select the **UAPSD** checkbox to enable UAPSD.
b. Select the **QBSS** checkbox to enable QBSS.
c. Enter the value in the **DTIM interval** text box to configure DTIM interval.
d. Enter the value for **Monitored Host** in the textbox.
e. Enter the Syslog server where all the client DNS requests will be logged in the **DNS Logging Host** textbox.
f. Enter the Syslog server IP where all wireless client connectivity events/logs should be displayed in the configured **Connection Logging Host**.
f. To enable band steering feature, select **Band Steering** checkbox.
g. Select the **Proxy ARP** checkbox to respond to ARP requests automatically on behalf of the clients.
h. Select **Unicast DHCP** checkbox to Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients.
i. Select **Option82 Circuit ID** to enable DHCP Option-82.
j. Choose **Option82 Remote ID** to select the MAC address of the AP.
k. Select **Tunnel Mode** checkbox to enable tunneling of WLAN traffic over configured tunnel.

l. Select the type of Roaming Protocol as **Pre-authentication**, **OKC,** or **802.11r**.

m. Enter the re-association timeout in seconds in the **Re-association Timeout** textbox.

n. Select **802.11w State** as **Disable**, **Optional**, or **Mandatory**.

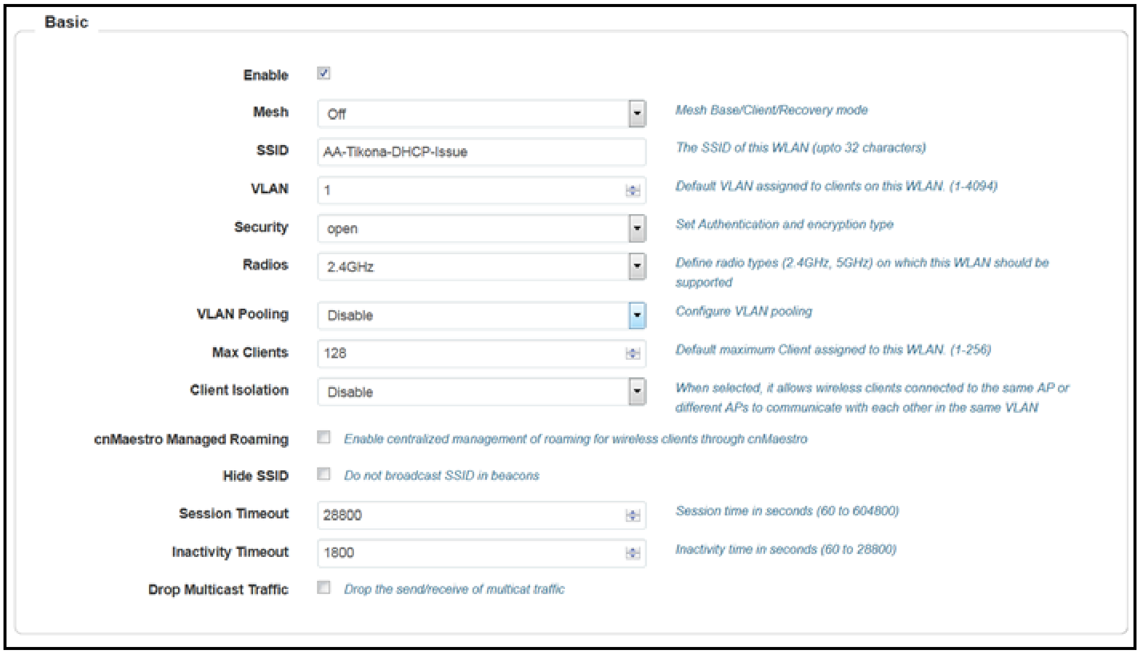
   [802.11w configuration is available, when user selects security as WPA2-PSK or WPA2-Entrprise. 802.11w supports both Optional & Mandatory.]

o. Select the SA query retry Time from the **SA Query Retry Time** list.

p. Select the association comeback time in the **Association comeback** textbox.

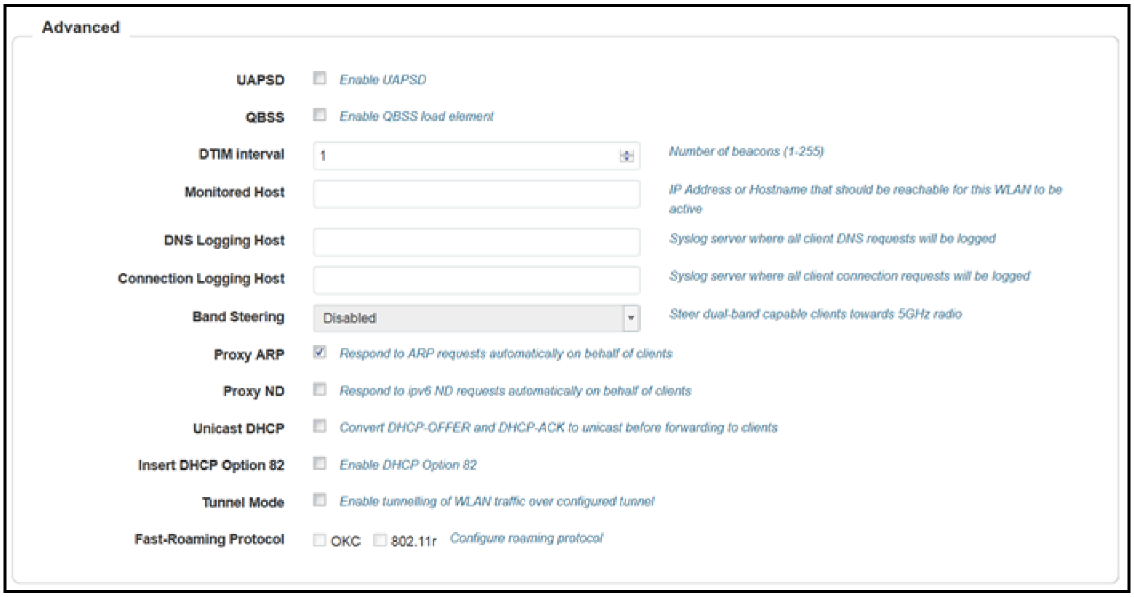
2. Click **Save**.

Figure 8: Configure: WLAN Configuration page



Basic

Enable	☑	
Mesh	Off	Mesh Base/Client/Recovery mode
SSID	AA-Tikona-DHCP-Issue	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
VLAN Pooling	Disable	Configure VLAN pooling
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
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 multicat traffic



Advanced

UAPSD	□	Enable UAPSD
QBSS	□	Enable QBSS load element
DTIM interval	1	Number of beacons (1-255)
Monitored Host		IP Address or Hostname that should be reachable for this WLAN to be active
DNS Logging Host		Syslog server where all client DNS requests will be logged
Connection Logging Host		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

In the CLI

```
To configure WLAN:
(cnPilot Enterprise AP) (configure)# wireless wlan 1
To configure SSID:
(cnPilot Enterprise AP) (config-wlan-1)# ssid<name>
To configure security:
(cnPilot Enterprise AP) (config-wlan-1)# security wpa2-enterprise
To configure VLAN pool:
```

```
(cnPilot Enterprise AP) (configure-wlan-1)# vlan-pool radius-based
```

To view the client status:

```
(cnPilot Enterprise AP) (config)#show wireless clients
```

To view the client statistics:

```
(cnPilot Enterprise AP) (config)#show wireless clients statistics
```

To configure 802.11w:

```
(cnPilot Enterprise AP) (config)# protected-mgmt-frames sa-query-retry-time msecs
(cnPilot Enterprise AP) (config)# protected-mgmt-frames association-comeback secs
(cnPilot Enterprise AP) (config)# [no] protected-mgmt-frames state optional | mandatory
```

To configure Fast Roaming Protocol:

```
(cnPilot Enterprise AP) (config)# fast-roaming pre-authentication
(cnPilot Enterprise AP) (config)# fast-roaming okc
(cnPilot Enterprise AP) (config)# fast-roaming 802.11r
(cnPilot Enterprise AP) (config)# fast-roaming 802.11r over-the-ds
(cnPilot Enterprise AP) (config)# fast-roaming 802.11r reassociation-timeout x #Reassociation time out in secs
```

To enable client isolation across AP:

```
(cnPilot Enterprise AP) (Config-wlan-1)# client-isolation dynamic
```

To disable client isolation within AP:

```
(cnPilot Enterprise AP)# no client-isolation
```

To disable client isolation across AP:

```
(cnPilot Enterprise AP)(config-wlan-1)# no client-isolation dynamic
```

Configuring Client Isolation

Client Isolation supported by cnPilot devices are of two methods:

1. Local: This feature is required when a wireless client to client traffic should not be allowed in the network.
2. Network Wide: This feature is required when wireless client communication across network/multiple APs should not be allowed in the network. To allow communication between two clients connected across two different APs, user has to whitelist MAC address of the clients.

   To configure this using CLI:

To add a client isolation whitelist:

```
Host (config-wlan-1)# client-isolation mac-list 50-9a-4c-17-75-3b
```

To delete a client isolation whitelist:

```
Host(config-wlan-1)# no client-isolation mac-list 50-9a-4c-17-75-3b
```

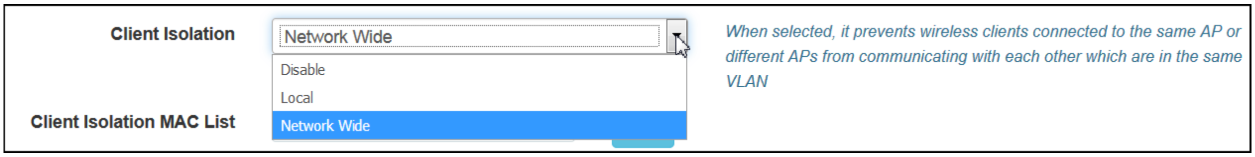
To view a configured client isolation whitelist:

```
Host(config-wlan-1)# client-isolation mac-list 50-9a-4c-17-75-3b
#show config
        wireless wlan 1
         ssid bg_client_isolation_test1
        no shutdown
```

vlan 1
security open
client-isolation dynamic
client-isolation mac-list 50-9a-4c-17-75-3b

To configure using UI:

Navigate to **WLAN> Basic** page:



Client Isolation: Network Wide

When selected, it prevents wireless clients connected to the same AP or different APs from communicating with each other which are in the same VLAN

Configuring RADIUS Servers

RADIUS accounting allows user activity and statistics to be reported from the device to RADIUS servers.

This section provides details on configuring parameters for RADIUS Servers.

The following table lists the fields that are displayed in the **Configure > WLAN > RADIUS Servers** page:

Table 10: Configure: **RADIUS Servers** parameters

Parameter	Description	Default Value
Authentication Server	IP address of the host for the authentication server.	–
Timeout	Timeout in seconds of each request attempt.	3
Attempts	Number of attempts before a request is given up.	1
Accounting Server	IP address of the host for the accounting server.	–
Timeout	Timeout in seconds of each request attempt.	3
Attempts	Number of attempts before a request is given up.	1
Accounting Mode	• start-stop • Start-interim-stop • None	None
Sync Accounting Records	Sync accounting records configuration is enabled when user want single accounting session for a client which is roaming across different AP's on the same WLAN. If this config is disabled, when the client roams from one AP to another then accounting session on previous AP is stopped and a new accounting is started on the new AP. This provides seamless accounting for clients in the network when they roam. The traffic counters and session ID for a given accounting session is synced across AP's when client roams.	Disabled

Server Pool Mode	**Load Balance:** Load balance requests equally among configured servers. **Failover:** Move down server list when earlier servers are unreachable.	Load Balance
NAS Identifier	NAS-Identifier attribute to use in request packets. Defaults to system name.	–
Interim Update Interval	Interval for accounting interim stats update (60-65535).	120
Dynamic Auth	By enabling Dynamic Auth, CoA request defined in RFC 5176 is supported by device, in which the request originates from external server such as AAA to the device attached in the network, and enables the dynamic reconfiguring of sessions from external authentication, authorization, and accounting (AAA) CoA Disconnect request is supported by device.	Disable
Dynamic VLAN	This field has to be enabled if VLANs are assigned by RADIUS server.	Enabled
Proxy through cnMaestro	Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP.	Disabled

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configure > WLAN > RADIUS Servers** tab. The following fields are displayed:
   a. Enter the IP address of the host for the authentication server in the **host** textbox.
   b. Enter the shared key for this host in the **Shared** textbox.
   c. Enter the Port in the **Port** textbox.
   d. Enter the time in seconds of each request attempt in **Timeout** textbox.
   e. Enter the number of attempts before a request is given up in the **Attempts** textbox.
   f. Enter the IP address of the host for the accounting server in the **host** textbox.
   g. Enter the shared key for this host in the **Shared** textbox.
   h. Enter the Port in the **Port** textbox.
   i. Enter the time in seconds of each request attempt in **Timeout** textbox.
   j. Enter the number of attempts before a request is given up in the **Attempts** textbox.
   k. Select any one of the Accounting Mode:
      - Start-stop
      - Start-interim-stop
   l. Select the **Sync Accounting Records** checkbox to enable sync accounting records configuration.
   m. Select any one of the Server Pool Mode:
      - Load Balance

  - Failover

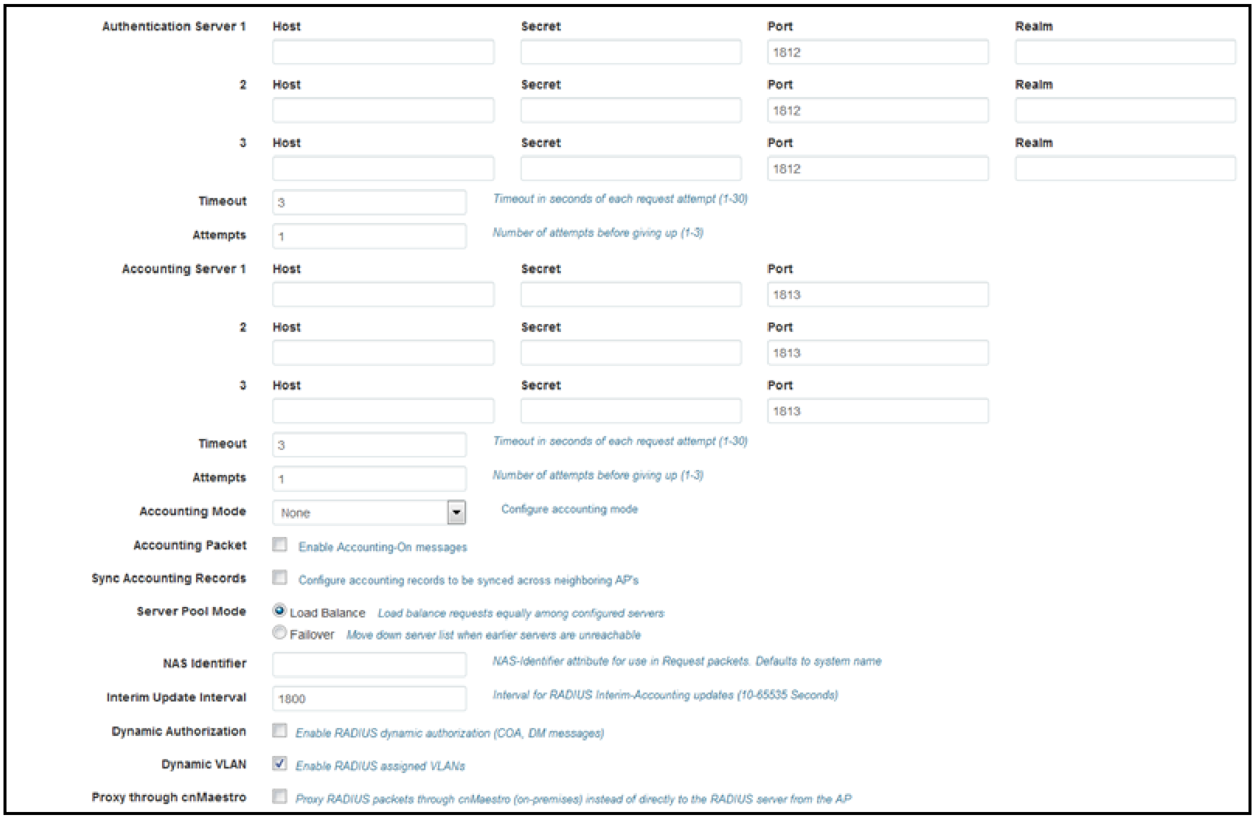
n. Enter the interval for accounting interim stats update (60-65535) in the **Interim Update Interval** textbox.

o. Enter the NAS identifier in the **NAS Identifier** textbox.

p. Select the **Dynamic Auth** checkbox to configure dynamic authorization for wireless clients.

2. Click **Save**.

Figure 9: Configure: **RADIUS Servers** page



	Host	Secret	Port	Realm
Authentication Server 1			1812	
2			1812	
3			1812	

Timeout	3	*Timeout in seconds of each request attempt (1-30)*
Attempts	1	*Number of attempts before giving up (1-3)*

	Host	Secret	Port
Accounting Server 1			1813
2			1813
3			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 ○ Failover	*Load balance requests equally among configured servers* *Move down server list when earlier servers are unreachable*
NAS Identifier		*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*

In the CLI

To configure RADIUS server:

```
(cnPilot Enterprise AP) (configure)# wireless wlan 1
(cnPilot Enterprise AP) (config)#wireless wlan <WLAN_IDX>
(cnPilot Enterprise AP) (config-wlan)#radius-server authentication host <1-3> <HOSTIP>
(cnPilot Enterprise AP) (config-wlan)#radius-server authentication port <1-3>
<1-65535>
(cnPilot Enterprise AP) (config-wlan)#radius-server authentication secret <1-3> <WORD>
(cnPilot Enterprise AP) (config-wlan)#radius-server authentication realm <1-3> <WORD>
(cnPilot Enterprise AP) (config-wlan)#radius-server authentication timeout <1-30>
(cnPilot Enterprise AP) (config-wlan)#radius-server authentication attempts <1-3>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting host <1-3> <HOST-IP>
```

```
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting port <1-3> <1-65535>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting secret <1-3> <WORD>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting realm <1-3> <WORD>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting timeout <1-30>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting attempts <1-3>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting interim-update-interval
<60-65535>
(cnPilot Enterprise AP) (config-wlan)#radius-server accounting mode <start-
stop|startinterim-
stop|none>
```

Wireless Mesh

Overview

With System release 3.1, cnPilot Enterprise APs support mesh connections between radios. Mesh links can form between radios of the same band of operation (2.4GHz or 5GHz), but the two peers of the mesh link don't have to be of the same AP-type. Given the larger set of available channels and typically cleaner RF environment we recommend using the 5GHz radio for mesh backhaul if the AP is 5GHz-capable.

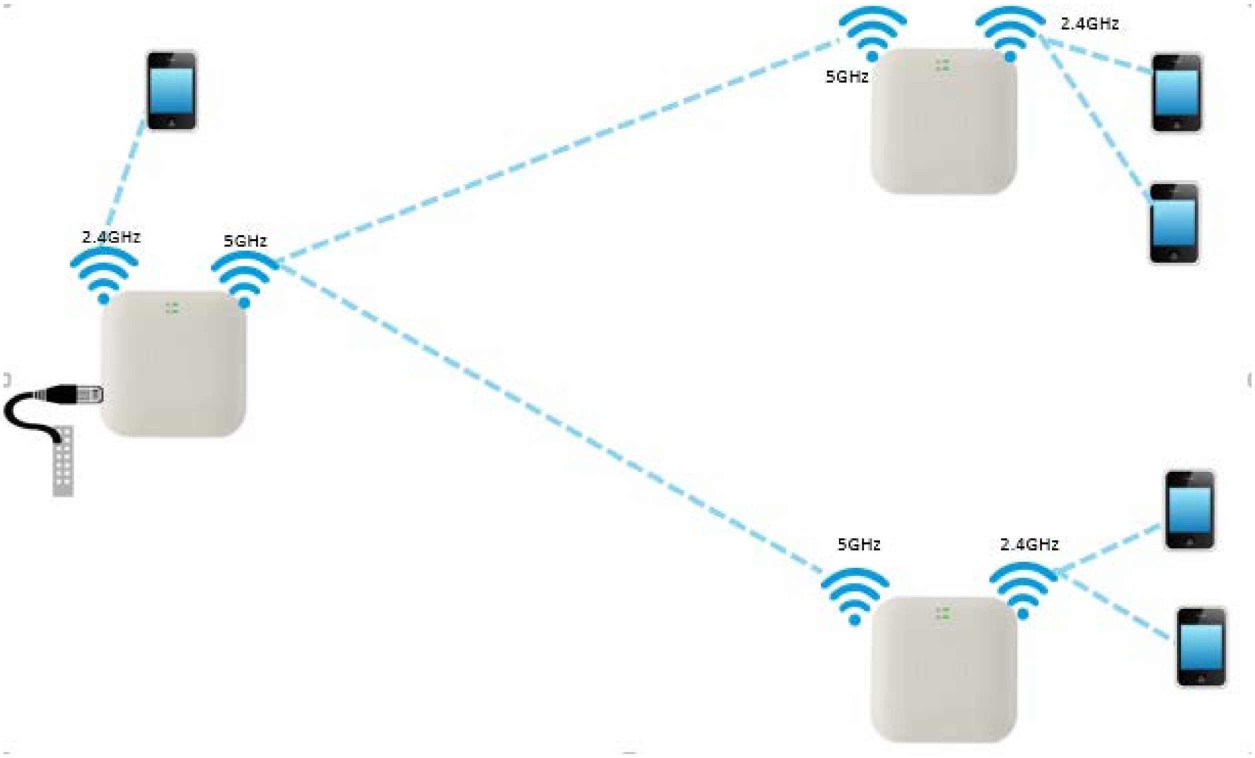
A mesh link can be created between two radios by configuring one of them as a BASE and the other as a CLIENT on the first WLAN of the AP. Typically the access point which has wired connectivity would be configured as a mesh base. The radio setup for mesh base will select a channel and start transmitting beacons as soon as the AP comes up. The radio setup for mesh client will scan all available channels, looking for a mesh base radio to connect with. The SSID in the mesh WLAN is how the client and base radios of a mesh link identify each other, the same SSID should be configured on the mesh BASE WLAN as well as the mesh CLIENT WLAN.

In addition to a simple topology between a base and a client, a "star" or "hub-and-spoke" mesh topology is also supported: a mesh radio can service upto 5 mesh clients connected to it. When a radio is configured with a mesh WLAN, on that WLAN other clients are not allowed to connect, however the radio can service clients on other WLANs mapped to it. Note that a client radio will start rescanning all available channels as soon as it loses connectivity to the base. During this scan period other WLANs mapped to it will not be operational.

The mesh link can also be secured with WPA2-Preshared-Keys. The same passphrase should be configured on both the mesh BASE as well as the mesh CLIENT. Standard 802.11 security handshakes and AES-CCM encryption are then used on the mesh link."

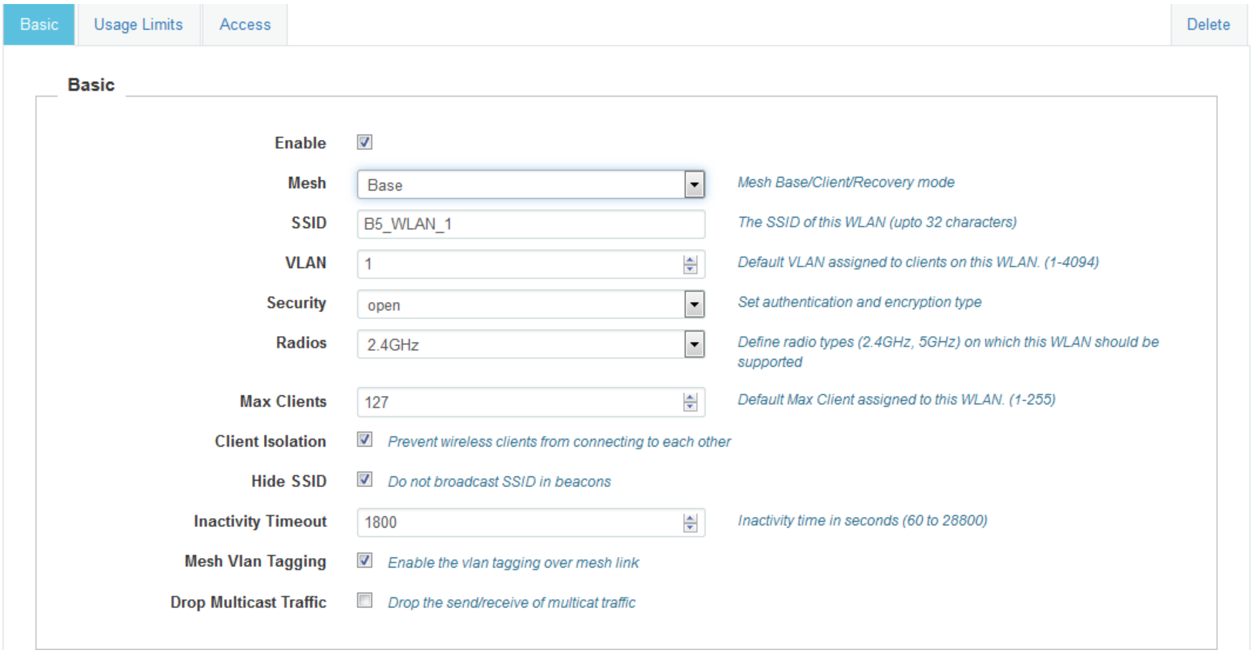
Installments

The following diagram illustrates the working scenario of wireless mesh network:



The following diagram shows the list of connected mesh peers in the dashboard:

Figure 10: Mesh Peers



Basic

Enable	☑	
Mesh	Base	*Mesh Base/Client/Recovery mode*
SSID	B5_WLAN_1	*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	127	*Default Max Client assigned to this WLAN. (1-255)*
Client Isolation	☑ *Prevent wireless clients from connecting to each other*	
Hide SSID	☑ *Do not broadcast SSID in beacons*	
Inactivity Timeout	1800	*Inactivity time in seconds (60 to 28800)*
Mesh Vlan Tagging	☑ *Enable the vlan tagging over mesh link*	
Drop Multicast Traffic	□ *Drop the send/receive of multicat traffic*	

Typical Use-Cases

- WiFi access in areas with no cable run

- Small retail location with one AP near an Ethernet outlet, another in the middle of lobby that has no easy cable run
- Extend range outdoors
- Provides WiFi within the building
- Plug coverage holes
- Add an AP indoor/outdoor for the areas that are difficult to reach

Configuring Wireless Mesh

The following table lists the fields that are displayed in the **Configure > WLAN > Basic** page:

Table 11: Configure: **WLAN > Basic** parameters

Parameter	Description	Default Value
Mesh	Configures the Mesh feature. Select Base, Client or Off from the Mesh list.	—
SSID	The WLAN name that is seen by the wireless clients.	—
VLAN	The VLAN ID to be used for this WLAN.	1
Security	Select the security type for this client.	—
Passphrase	WPA2 Pre-shared Security passphrase or key.	—
Radios	The RADIO type on which this WLAN should be supported.	—
VLAN Pooling	Configures VLAN pooling feature.	—
Max Clients	The default max number of clients associated to the WLAN.	127
Client Association	Prevents the wireless clients from connecting to each other.	—
Hide SSID	Select this option for not broadcasting the SSID in beacons.	—
Session Timeout	Session time in seconds (60 to 604800)	28800
Inactivity Timeout	Inactivity timeout in seconds.	1800
Mesh VLAN Tagging	When this parameter is enabled, 802.11 packets between Mesh devices will be tagged with VLAN ID as configured on the device.	—
Drop Multicast Traffic	Drop the send and receive of multicast traffic.	Disable

Notes

- There is a large throughput drop when using a radio for client access as well as mesh link (over 50%) since each packet would traverse the air twice, once from the client to the AP, then from the AP to its mesh peer.

- To form mesh link with out of the box devices, configure Mesh Recovery on mesh base. When out of the box device is not connected to Ethernet, device will scan for Mesh Recovery profile and connect to mesh base.

Multi-hop mesh

Multiple-Hop mesh allows the administrator to increase the range of the meshed network by daisy chaining wireless backhaul links across multiple Access Points. Note that since the mesh radio would typically receive, then transmit, on the same channel, throughput after each hop would degrade by 50-60%. However, for hard to cable areas the multi-hop mesh might be the only way to provide connectivity to clients.

Wired-Connection >=== AP1 ...(mesh)... AP2 ...(mesh)... AP3

Configuration

AP1:

```
Wlan1
<< mesh base>>
```

AP2:

```
Wlan1
{
<<mesh client>>
}
Wlan2
{
<<mesh base>>
}
```

AP3:

```
<<mesh client>>
```

Mesh recovery

Mesh recovery can be used in two cases.

- Recover a mesh AP that was stranded from the network because of a mismatched configuration in radio, Mesh SSID or security passphrase.
- An AP with default configuration, running firmware version 3.0.

Mesh Base

On mesh base user needs to configure mesh recovery profile in one of the WLAN
<<mesh recovery>>

Mesh Client

On Mesh Client, user need not configure Mesh Recovery profile. Mesh Recovery profile is enabled if it fails to form Mesh Link with Mesh Base.

Guest Access

Guest access feature is used to provide a web-based network access control process where a client is redirected to a login page to gain network access. The clients can have a simple click-through login process or a RADIUS authentication based access mode. Without a login no network traffic is allowed from the client apart from DHCP and DNS packets. Traffic to specific IP addresses can be allowed using the whitelist configuration for the un-authenticated clients.

Configuring Guest Access

Administrator can configure a set of whitelist IP address which guest access clients can access without doing a login. This configuration also becomes handy when an external web portal is being used for providing the login/welcome pages. Administrator can give a secured http connection for the login where the communication between the access point and the client will be secured. Administrator can also configure the page title and welcome message as per his own requirements.

The following table lists the fields that are displayed in the Configure > WLAN > Guest Access page:

Table 12: Configure: **Guest Access** parameters

Parameter	Description	Default Value
Enable	Enables the Guest Access feature.	Disable
Portal Mode	You can select any one of the following: • Internal Access Point • External Hotspot • cnMaestro	Internal Access Point
Guest Portal Name	The guest portal name hosted in cnMaestro.	–
Access Policy	There are four types of access types provided for the end user, Click-through, RADIUS, LDAP, and Local guest account. The click-through can also be combined with additional terms and condition content which can tell end users the terms of the network usage. LDAP redirects the users to a login page for authentication by a LDAP server.	Click Through
Redirect Mode	You can use http or https URLs for redirection.	HTTP
WISPr Clients External Server Login	Enable this configuration, if external web server is used for Guest Portal and if it is required to do HTTP POST to external server.	–
External Page URL	URL for the external web server which hosts captive portal.	–
External Portal Type	Custom xwf portal type or standard generic guest portal.	–
Success Action	Select any one of the following: • Internal Logout Page • Redirect User to External URL • Redirect user to Original URL	Internal Logout Page

Prefix Query Strings in Redirect URL	Provision to append query string in the redirection URL after successful authentication.	–
Redirect User Page	Page to redirect to after successful authentication.	–
Proxy Redirection Port	Port on which captive portal service is hosted.	–
Title	Title text in splash page.	–
Contents	Main contents of the splash page.	–
Terms	The admin can configure his own text for the terms and condition in the CLI/UI or he can load terms and condition content file from CLI using a service command. If a terms and condition content file is loaded then it will be common across all WLAN configuration if guest access is enabled on them.	–
Logo	Logo to be displayed in the splash page.	–
Background Image	Background image to be displayed on the splash page	–
Success message	The message to be displayed in the login page after successful authentication.	–
Session Timeout	Administrator can configure a limited session time for each session after which a re-login will be enforced.	28800 Sec
Inactivity Timeout	Administrator can also configure an inactivity time for deleting those clients which went away without doing a proper guest access logout and free up the consumed resources by that client. Such a configuration is very helpful for public hotspots where free network is provided and clients go away without doing a logout.	1800 Sec
MAC Authentication Fallback	Use guest-access only as fallback for clients failing MAC-authentication.	Disable
Extend Interface	Configures the interface which is configured for guest access.	-

The RADIUS server configuration is used for RADIUS access type guest access and one can also enable RADIUS accounting for the guest access clients.

LDAP guest access

LDAP guest access authenticates a guest user from Lightweight Directory Access Protocol (LDAP) server like Active Directory (AD) as the backend database.

When the user enters a valid username and password on the web authentication login page and clicks **Submit**, the user is authenticated based upon the credentials submitted and a successful authentication from the backend database (LDAP in this case). The web authentication system then displays a successful login page and redirects the authenticated client to the requested URL.

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configure > WLAN > Guest Access** tab. The following fields are displayed:
   a. Select **Enable** checkbox to enable guest access feature.
   b. Choose the Access Policy as **Click through, Radius, LDAP, or Local Guest Account.**

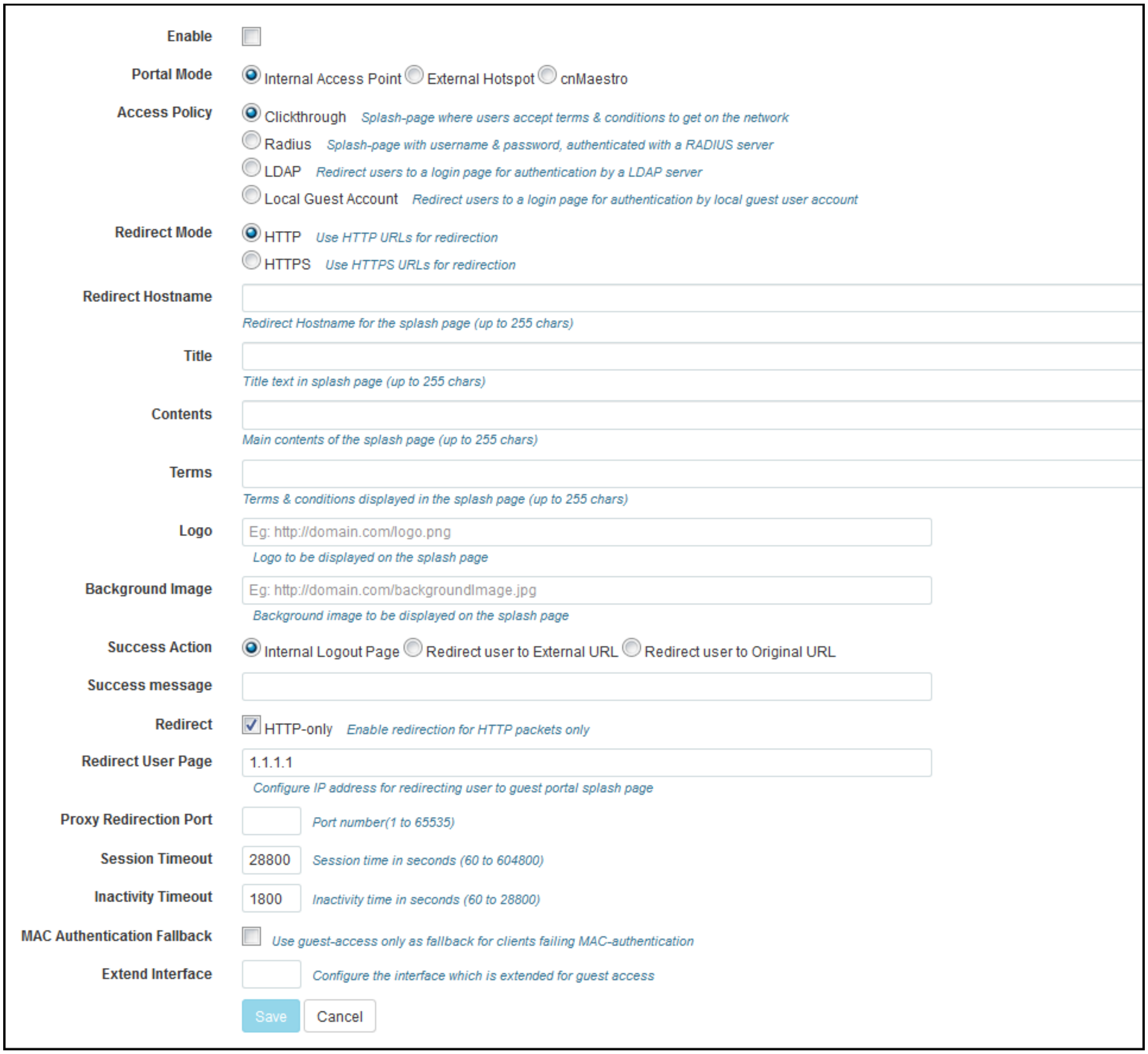
   To configure LDAP:
   a. Select **Access Policy** as **LDAP**.
   b. In the **BaseDN** field, if user domain name is corporation.com, then enter **dc=corporation** and **dc=com**.
   c. In **UserDN** field, enter the distinguished name (DN) of the subtree in **LDAP server** that contains a list of all the users. For example, ou=organizational unit and dc=corporation, dc=com.

   In **Services configure** page, enter the IP address of the LDAP server and its port number.
   a. Choose the Redirect Mode as **HTTP** or **HTTPS**.
   b. Select the **WISPr Clients External Server Login** checkbox.
   c. Choose the login page to be on device login page or an external URL.
   d. Choose the external portal type as **standard** or **XWF**.
   e. Select any one of the success action options:
      - Internal Logout Page
      - Redirect User to External URL
      - Redirect user to Original URL
   f. Enter the success message to appear in the **Success Message** textbox.
   g. Enter the port number in the **Redirection Port** textbox.
   h. Enter the title to appear in the splash page in the **Title** textbox.
   i. Enter the content to appear in the splash page in the **Contents** textbox.
   j. Enter the terms and conditions to appear in the splash page in the **Terms** textbox.
   k. Enter the logo to be displayed in the **Logo** textbox.
   l. Select the background image to be displayed on the splash page.
   m. Enter the session timeout in seconds in the **Session Timeout** textbox.
   n. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.
   o. Choose the **Prefix Query Strings in Redirect URL** checkbox.
   p. Enter the URL in the **Redirect URL** textbox.
   q. Select the **MAC Authentication Fallback** checkbox if guest-access is used only as fallback for clients failing MAC-authentication.
   r. Enter the name of the interface that is extended for guest access in the **Extend Interface** textbox.
2. Click **Save**.

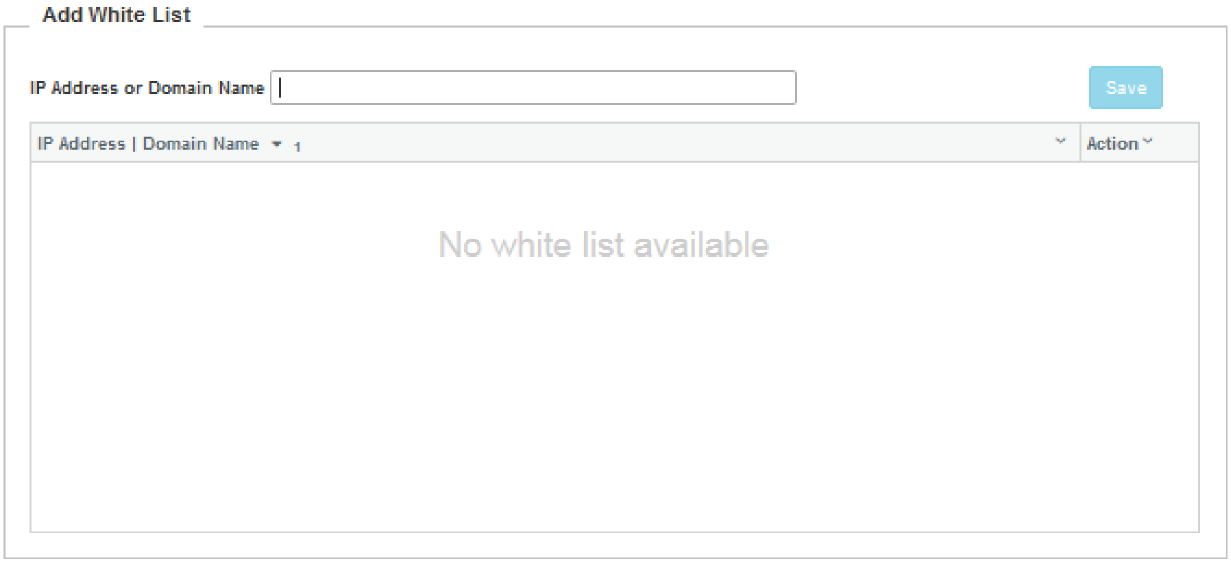
To configure the whitelist parameter:

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

Figure 12: Configure: **Guest Access** page



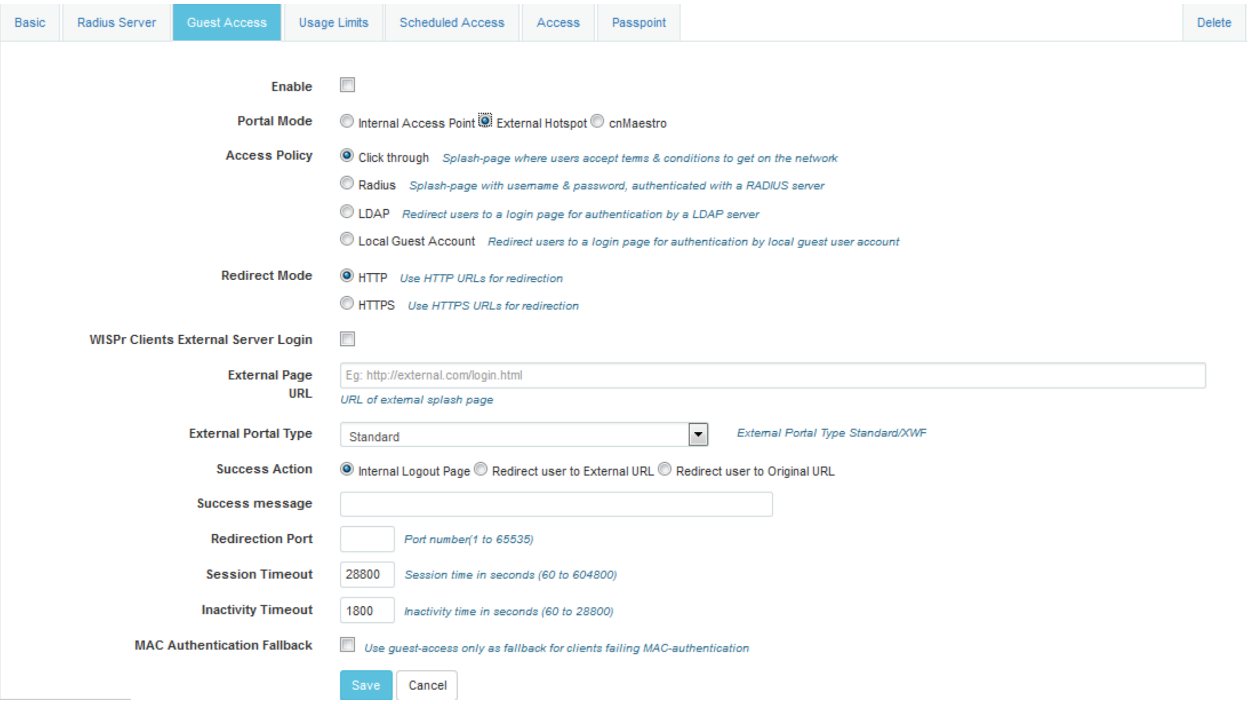
Enable	□
Portal Mode	● Internal Access Point ○ External Hotspot ○ cnMaestro
Access Policy	● Clickthrough *Splash-page where users accept terms & conditions to get on the network* ○ Radius *Splash-page with username & password, authenticated with a RADIUS server* ○ LDAP *Redirect users to a login page 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 604800)*
Inactivity Timeout	1800 *Inactivity time in seconds (60 to 28800)*
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*



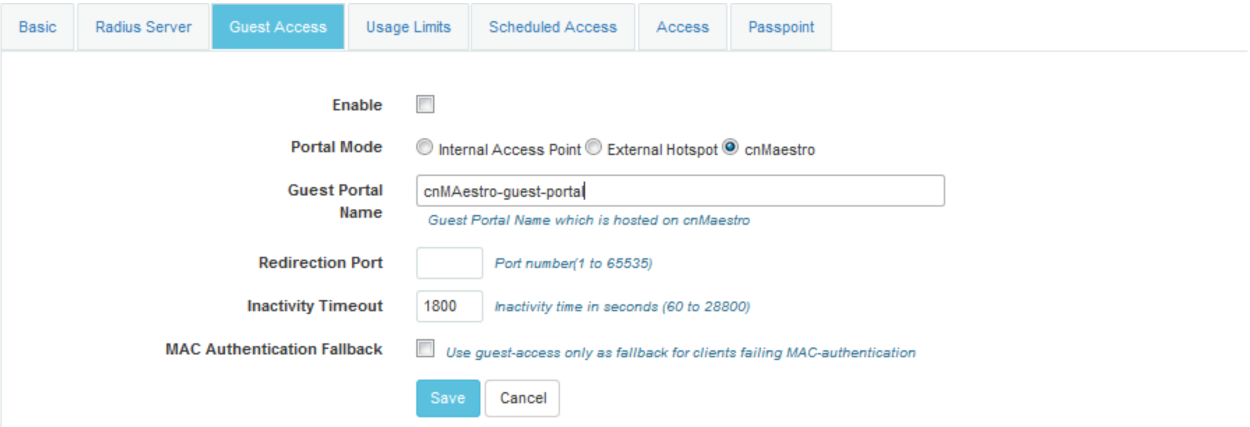
Add White List

IP Address or Domain Name

IP Address | Domain Name	Action
No white list available	



Enable	□
Portal Mode	○ Internal Access Point ● External Hotspot ○ cnMaestro
Access Policy	● Click through *Splash-page where users accept tems & conditions to get on the network* ○ Radius *Splash-page with usemame & 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*
WISPr Clients External Server Login	□
External Page URL	Eg: http://external.com/login.html *URL of extemal splash page*
External Portal Type	Standard *Extemal Portal Type Standard/XWF*
Success Action	● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL
Success message	
Redirection Port	*Port number(1 to 65535)*
Session Timeout	28800 *Session time in seconds (60 to 604800)*
Inactivity Timeout	1800 *Inactivity time in seconds (60 to 28800)*
MAC Authentication Fallback	□ *Use guest-access only as fallback for clients failing MAC-authentication*



Enable □

Portal Mode ○ Internal Access Point ○ External Hotspot ● cnMaestro

Guest Portal Name cnMAestro-guest-portal
Guest Portal Name which is hosted on cnMaestro

Redirection Port *Port number(1 to 65535)*

Inactivity Timeout 1800 *Inactivity time in seconds (60 to 28800)*

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

Express Wi-Fi (XWF) Support on Wired Port

The Express Wi-Fi (XWF) is Facebook/Internet.org proprietary standard for Guest Access which works over RADIUS MAC Authentication for controlling guest client state. XWF Lite/XWF-FULL comprises of a server where the actual guest client state is maintained and the server talks to a centralized RADIUS server for sending the client state change messages to the end Access Points.

Usually the RADIUS server is located in the NOC for a given XWF Lite/XWF-FULL installation where it can talk directly to Wi-Fi Access points. The Wi-Fi WLAN is configured with guest-access enabled along with RADIUS based MAC Authentication and the MAC-AUTH-FALLBACK policy. The external page for the guest access configuration points to a XWF Server. It also requires the dynamic authorization to be enabled as the client state changes are dynamically updated by the XWF Server through the centralized RADIUS server to the Wi-Fi Access Points.

The RADIUS responses or the COA update contains Facebook vendor attributes along with quota limits for the given clients.

You can configure this feature in any of the interface (except management port).

To enable this feature:

1. Create a WLAN and configure the details for XWF to work with wireless clients.
2. To extend the support to wired port,
    a. Under **WLAN > Guest Access > Extend Interface**, enter the interface number.
    b. Click **Save.**

Bypassing Captive Portal User-Agent

Many mobile OS'es today, including Apple iOS and various Android releases include a Captive Portal Network Assist (CNA) browser which is an auto-popup to detect if an internet connection is possible on a WiFi Hotspot. The CNA attempts to connect to specific URLs which either indicates to it that the Internet connection is available, or results in a redirection to a splash-page where a user can then log into the WiFi network.

Firmware version 3.8 adds a feature to allow custom responses based on matches to some key words in the HTTP User-Agent. If matching keyword is found, the AP responds with a configured reply to the CNA assisted requests which simulates the condition of client having Internet access. Eventually the smart device logic of detecting Internet is successful and it does not bring up the auto sign-up sheet even though it is connected on a Captive Portal network.

Syntax:

```
(Cambium AP)(config-wlan-<wlan-index>)# guest-access captive-portal-bypass user-agent
2 “Mozilla/5.0(Macintosh;Intel Mac OS X 10_11_6) AppleWebkit/601.7.7 (KHTML, like
Gecko)” 200.
```

Example:

A sample HTTP request for detecting Captive Portal on IOS and Android devices:

Android 8.0.0 OS on Motorola Z Play mobile phone:

HTTP Request:

GET /generate_204 HTTP/1.1
User-Agent: ***Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.82 Safari/537.36***
Host: connectivitycheck.gstatic.com
Connection: Keep-Alive
Accept-Encoding: gzip

Reply:
HTTP/1.1 204 No Content

IOS:

HTTP Request:GET /hotspot-detect.html HTTP/1.0
Host: captive.apple.com
Connection: close
User-Agent: CaptiveNetworkSupport-355.30.1 wispr
Reply:

HTTP/1.0 200 OK
<HTML><HEAD><TITLE>Success</TITLE></HEAD><BODY>Success</BODY></HTML>

In the CLI

To configure Guest Access:

```
(cnPilot Enterprise AP) (configure)# wireless wlan 1
(cnPilot Enterprise AP) (config)#wireless wlan <WLAN_IDX>
(cnPilot Enterprise AP) (config-wlan)#guest-access access-type <click-through|radius>
(cnPilot Enterprise AP) (config-wlan)#guest-access connection-mode <http|https>
(cnPilot Enterprise AP) (config-wlan)#guest-access splash-page terms-message <TEXT>
(cnPilot Enterprise AP) (config-wlan)#guest-access splash-page text <TEXT>
(cnPilot Enterprise AP) (config-wlan)#guest-access splash-page title <TITLE>
```

```
(cnPilot Enterprise AP) (config-wlan)#guest-access splash-page URL <URL>
(cnPilot Enterprise AP) (config-wlan)#guest-access success-action <redirect-url|
logout-page>
(cnPilot Enterprise AP) (config-wlan)#guest-access success-action logout-page text
<TEXT>
(cnPilot Enterprise AP) (config-wlan)#guest-access session-time <60-86400>
(cnPilot Enterprise AP) (config-wlan)#guest-access inactivity-time <60-28800>

(cnPilot Enterprise AP) (config-wlan)#guest-access whitelist <IP_ADDRESS>
```

Passpoint (Hotspot 2.0)

The Passpoint feature provides WPA2 hotspot network access and online sign up.

Passpoint enables a secure, automatic connection experience for users and supports operator goals of leveraging Wi-Fi technology for data offload of cellular networks. The Passpoint feature is configurable per WLAN.

The following table lists the fields that are displayed in the **Configure > WLAN > Passpoint** page:

Table 13: Configure: **Passpoint** parameters

Parameter	Description	Default Value
Passpoint/Hotspot 2.0		
Enable	Enables a secure hotspot network access, online sign up and policy provisioning.	Disable
DGAF	Downstream Group Addressed Forwarding (DGAF), when enabled the WLAN does not transmit any multicast and broadcast packets.	Disable
ANQP Domain ID	AP's ANQP domain identifier (0-65535) and is included when the HS2.0 Indication element is in Beacon and Probe Response frames.	0
Access Network Type	The configured Access Network Type is advertised to STAs. The following types of Access Network Types are supported: • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with guest • Wildcard	Private
ASRA	Indicates that the network requires a further step for access.	–
Internet	The network provides connectivity to the Internet if not specified.	–
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 (Access Network Query Protocol)	Select any one of the following: • 3GPP Cellular Network Information • Connection Capability • Domain Name List • IP Address Type information • Network Authentication Type • Operating Class Indication • Operator friendly Names • Venue Name Information • WAN Metrics	–

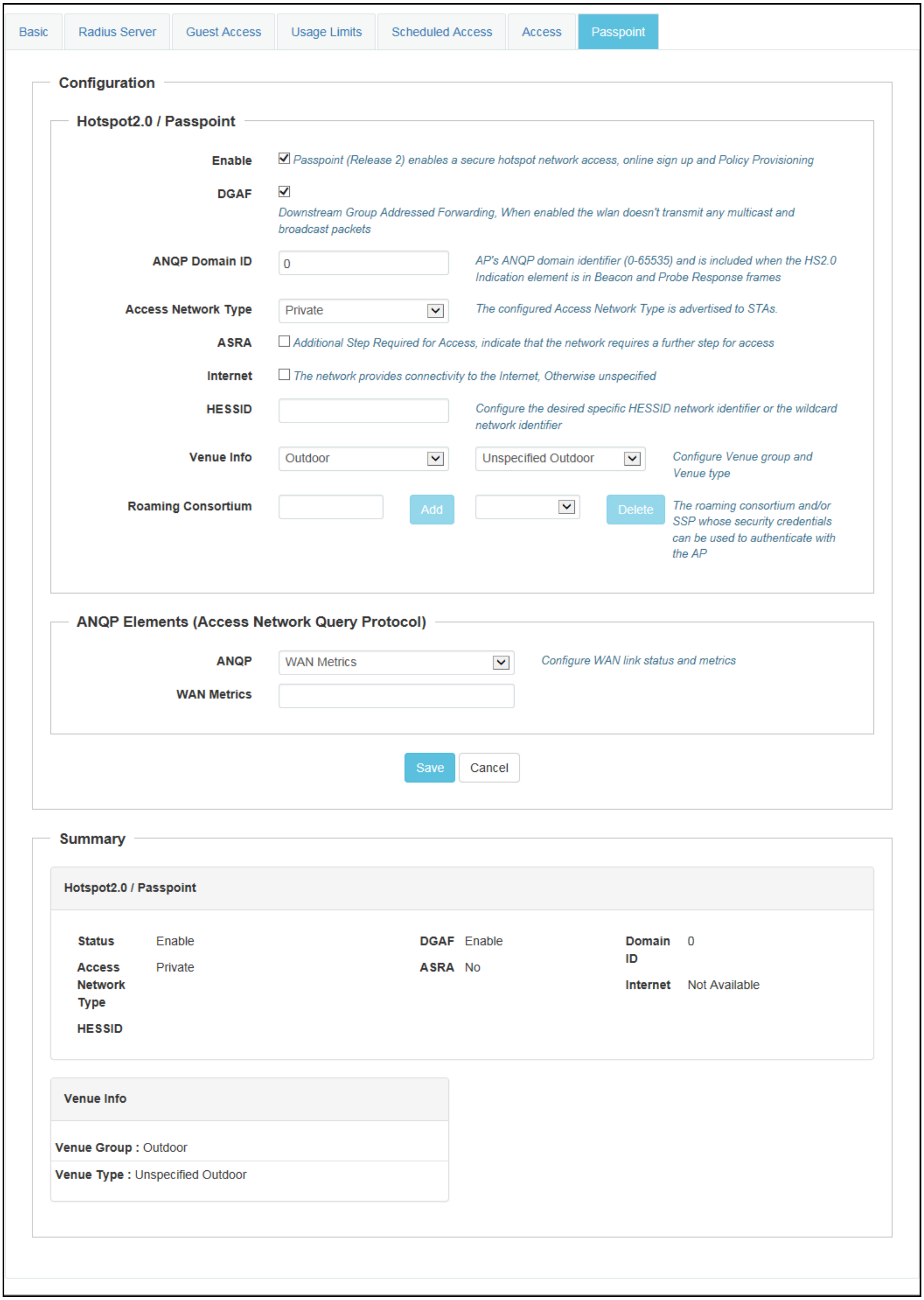
Configuring Passpoint

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to **Configure > WLAN > Passpoint** tab. The following fields are displayed.
    a) Select **Enable** checkbox to enable passpoint functionality.
    b) Select **DGAF** checkbox to enable Downstream Group Addressed Forwarding functionality.
    c) Enter the domain identifier value in **ANQP Domain ID** textbox.
    d) Choose the **Access Network Type** value from the drop-down list.
    e) Select the **ASRA** checkbox if the network requires additional steps for access.
    f) Select the **Internet** checkbox for the network to provide connectivity to the Internet.
    g) Enter the **HESSID** to configure the desired specific HESSID network identifier or the wildcard network identifier.
    h) Choose the **Venue Info** from the drop-down list.
    i) To add **Roaming Consortium** value, enter the value in the textbox and click **Add**.
    To delete a Roaming Consortium value, choose it from the drop-down list and click **Delete**.

Figure 13: Configure: **Passpoint** page



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 *AP's ANQP domain identifier (0-65535) and is included when the HS2.0 Indication element is in Beacon and Probe Response frames*

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 Outdoor Unspecified Outdoor *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 WAN Metrics *Configure WAN link status and metrics*

WAN Metrics

Summary

Hotspot2.0 / Passpoint

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

Venue Info

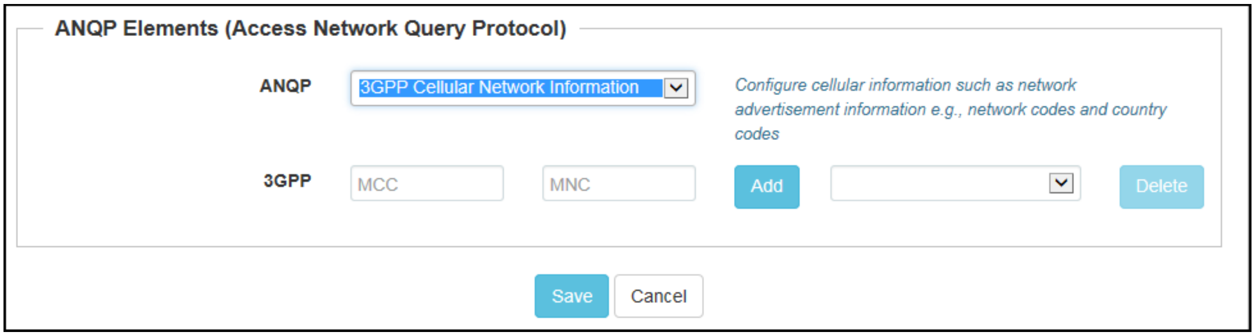
Venue Group : Outdoor

Venue Type : Unspecified Outdoor

Configuring ANQP Elements

3GPP Cellular Network Information

Configure cellular information such as network advertisement information e.g., network codes and country codes.


ANQP Elements (Access Network Query Protocol)

ANQP: 3GPP Cellular Network Information

Configure cellular information such as network advertisement information e.g., network codes and country codes

3GPP: MCC MNC

Parameter	Description
ANQP	3GPP Cellular Network Information.
3GPP	Network Advertisement Information such as network code and country code.

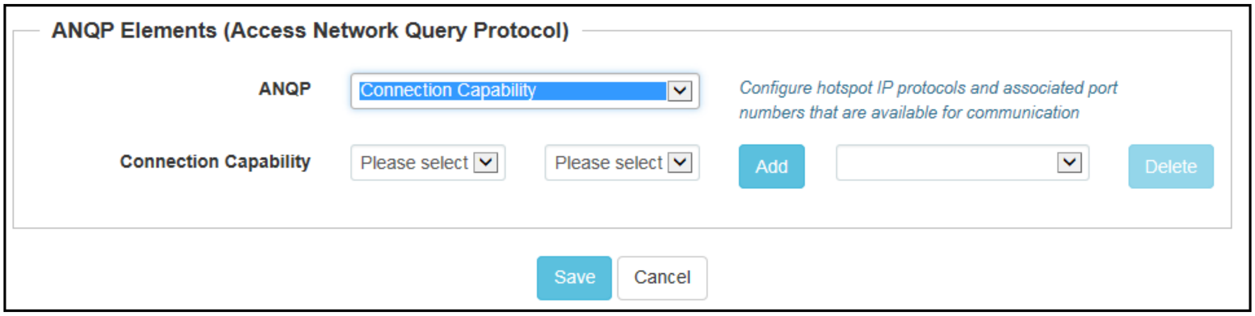
Configuring 3GPP Cellular Network Information

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:
   a. Select **3GPP Cellular Network Information** from the drop-down list.
   b. Enter the country code and network code in the textboxes next to 3GPP.
   c. Click **Add** and **Save**.

Note: To delete the configured 3GPP, choose it from the drop-down list and click **Delete.**

Connection Capability

Configure hotspot IP protocols and associated port numbers that are available for communication.


ANQP Elements (Access Network Query Protocol)

ANQP: Connection Capability

Configure hotspot IP protocols and associated port numbers that are available for communication

Connection Capability: Please select Please select

Parameter	Description
ANQP	Connection Capability.
Connection Capability	Select any one of the following: • ESP VPN • ICMP • TCP FTP • HTTP • TCP PPTP VPNs • TCP SSH • TCP TLS VPN • TCP VOIP • UDP IKEV2 • IPSEC VPN • UDP VOIP

Configuring Connection Capability

1. Navigate to **Configuration** > **WLAN** > **Passpoint** tab.
2. Under ANQP Elements, perform the following:

   a. Select **Connection Capability** from the drop-down list.

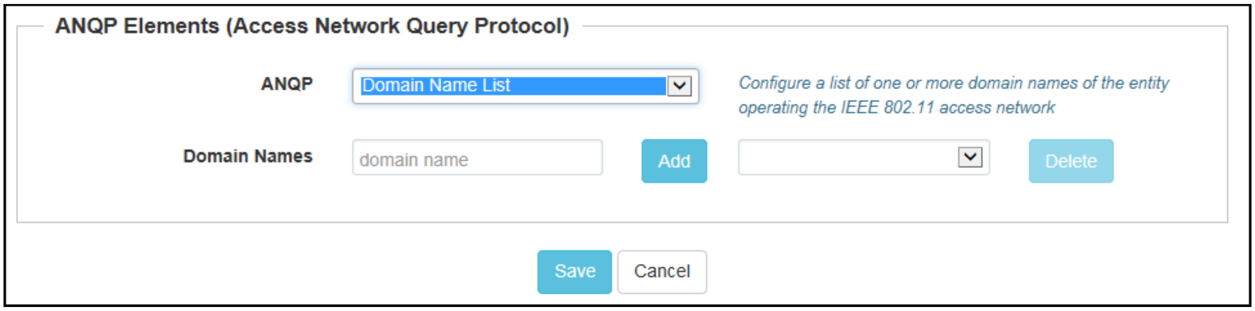
   b. Select the Hotspot IP Protocols and the associated port numbers from the drop-down list next to Connection Capability.

   c. Click **Add** and **Save**.

Note: To delete the configured connection capability, choose it from the drop-down list and click **Delete**.

Domain Name List

Configure a list of one or more domain names of the entity operating the IEEE 802.11 access network.


ANQP Elements (Access Network Query Protocol)

ANQP: Domain Name List

Configure a list of one or more domain names of the entity operating the IEEE 802.11 access network

Domain Names: domain name

Parameter	Description

ANQP	Domain Name List
Domain Names	Domain names of the entity operating the IEEE 802.11 access network.

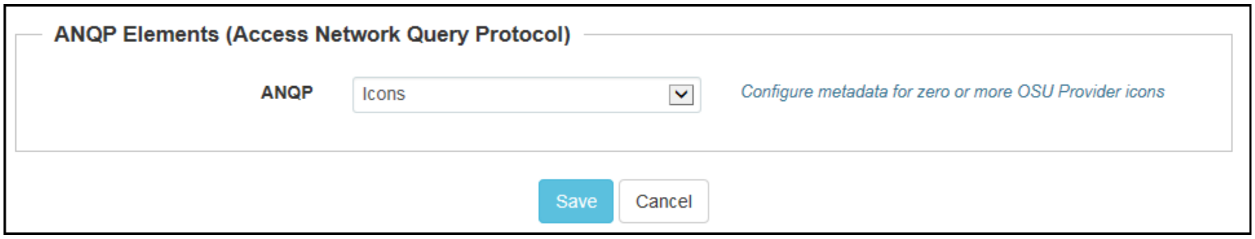
Configuring Domain Name List

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:
    a. Select **Domain Name List** from the drop-down list.
    b. Enter the domain name in the textbox next to Domain Names field.
    c. Click **Add** and **Save**.

Note: To delete the configured domain name list, choose it from the drop-down list and click **Delete.**

Icons

Configures metadata for zero or more OSU provider icons.


ANQP Elements (Access Network Query Protocol)

ANQP: Icons

Configure metadata for zero or more OSU Provider icons

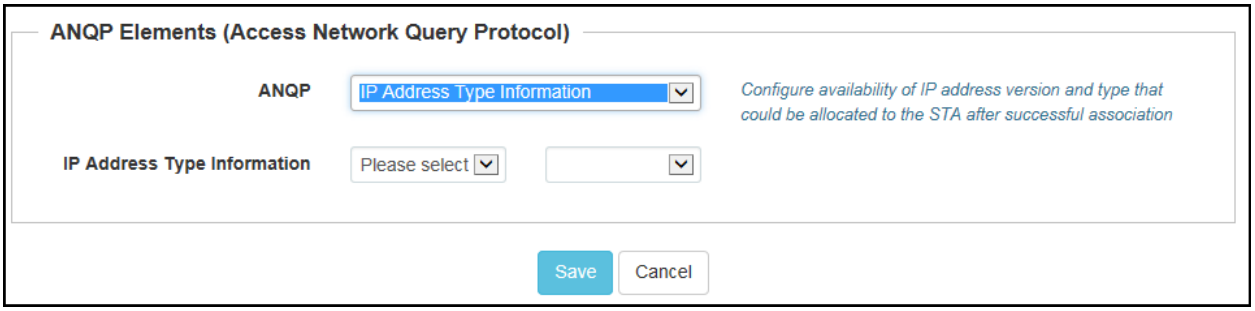
Parameter	Description
ANQP	Domain Name List

Configuring Icons

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:
    a. Select **Icons** from the drop-down list.
    b. Click **Add** and **Save**.

IP Address Type information

Configure availability of IP address version and type that could be allocated to the STA after successful association.


ANQP Elements (Access Network Query Protocol)

ANQP: IP Address Type Information

Configure availability of IP address version and type that could be allocated to the STA after successful association

IP Address Type Information: Please select

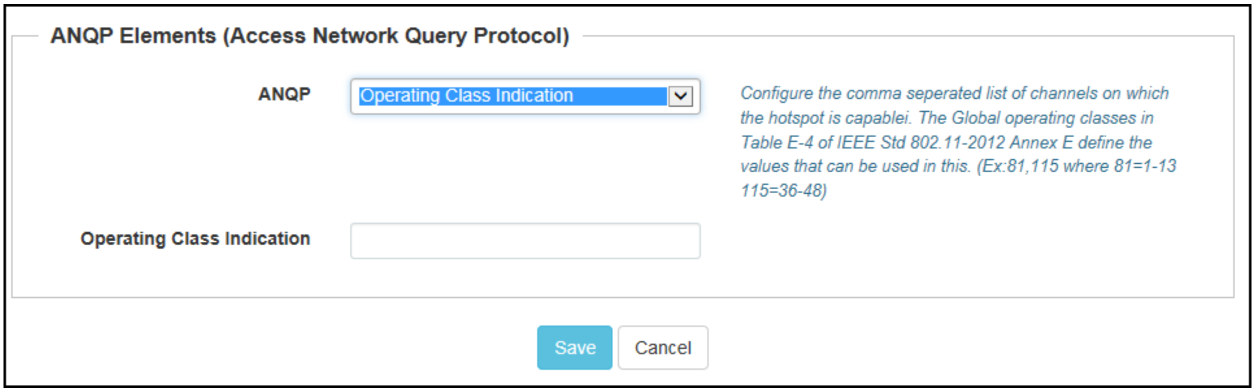
Parameter	Description
ANQP	IP address type information.
IP Address Type Information	Configures availability of IP address version (IPv4 and IPv6) and the type that could be allocated to the STA after successful authentication.

Configuring IP Address Type Information

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:
   a. Select **IP Address Type Information** from the drop-down list.
   b. Select the IP address type information from the drop-down list next to IP Address Type Information field.
   c. Click **Add** and **Save**.

Operating Class Indication

Configure the comma separated list of channels on which the hotspot is capable. The Global operating classes in Table E-4 of IEEE standard 802.11-2012 Annex E define the values that can be used in this. (Example: 81, 115 where 81=1-13 115=36-48).


ANQP Elements (Access Network Query Protocol)

ANQP: Operating Class Indication

Configure the comma seperated list of channels on which the hotspot is capablei. The Global operating classes in Table E-4 of IEEE Std 802.11-2012 Annex E define the values that can be used in this. (Ex:81,115 where 81=1-13 115=36-48)

Operating Class Indication:

Parameter	Description

ANQP	Operating Class Indication
Operating Class Indication	Channels on which the Hotspot is capable.

Configuring Operating Class Indication

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:

   a. Select **Operating Class Indication** from the drop-down list.

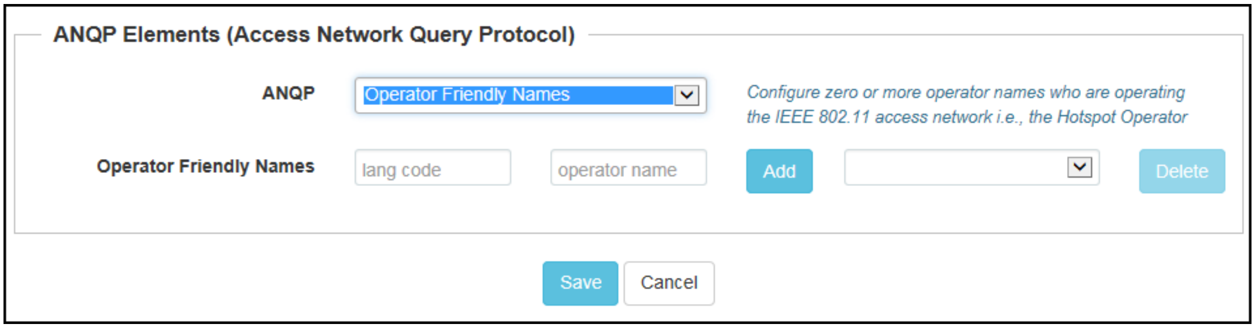
   b. Enter the list of channels separated by commas in the textbox next to Operating Class Indication field.

   c. Click **Add** and **Save**.

Note: To delete the configured Operating Class Indication, choose it from the drop-down list and click **Delete.**

Operator friendly Names

Configure zero or more operator names who are operating the IEEE 802.11 access network i.e., the Hotspot Operator.


ANQP Elements (Access Network Query Protocol)

ANQP: Operator Friendly Names

Configure zero or more operator names who are operating the IEEE 802.11 access network i.e., the Hotspot Operator

Operator Friendly Names: lang code, operator name

Parameter	Description
ANQP	Operator Friendly Names.
Operator Friendly Names	Name of the operator who operators the network.

Configuring Operating Class Indication

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:

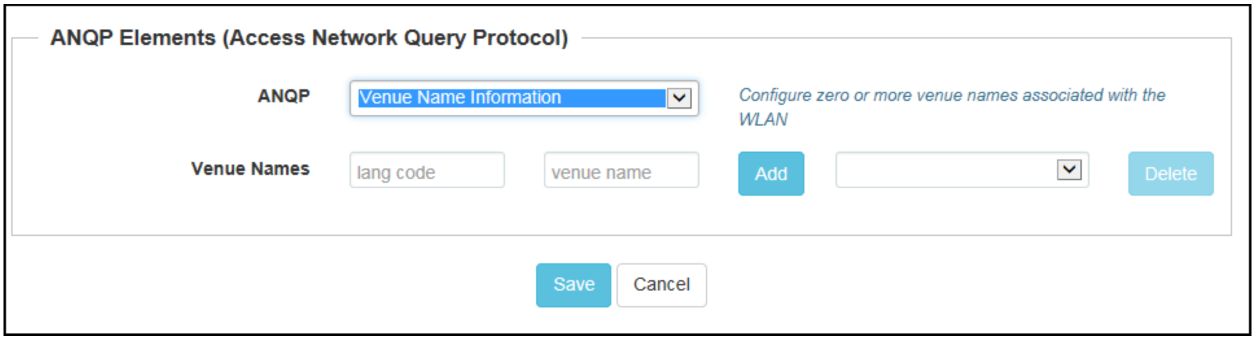
   a. Select **Operator Friendly Names** from the drop-down list.

b. Enter the name of the operator and lang code in the textboxes next to Operator Friendly Names field.

c. Click **Add** and **Save**.

Venue Name Information

Configure zero or more venue names associated with the WLAN.



ANQP Elements (Access Network Query Protocol)

ANQP: Venue Name Information

Configure zero or more venue names associated with the WLAN

Venue Names: lang code, venue name

Parameter	Description
ANQP	Venue Name Information.
Venue Names	Name of the venue associated with the WLAN.

Configuring Venue Name Information

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:

a. Select **Venue Names Information** from the drop-down list.

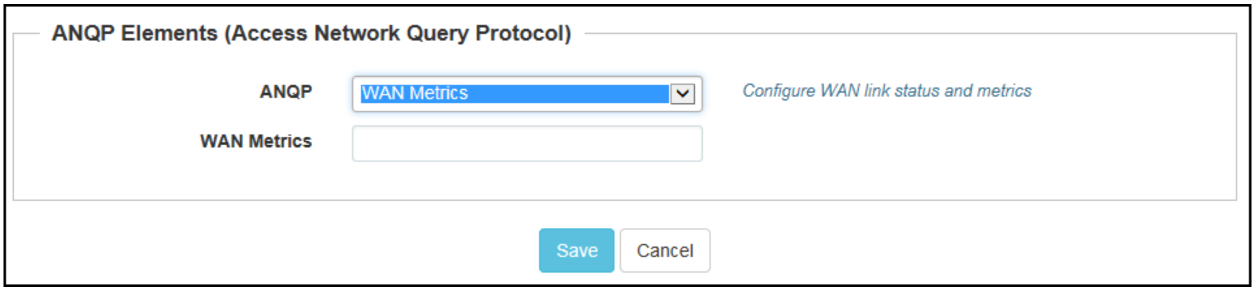
b. Enter the name of the venue and lang code in the textboxes next to Venue Names field.

c. Click **Add** and **Save**.

Note: To delete the configured Venue Name, choose it from the drop-down list and click **Delete**.

WAN Metrics

Configure WAN link status and metrics.



ANQP Elements (Access Network Query Protocol)

ANQP: WAN Metrics

Configure WAN link status and metrics

WAN Metrics:

Parameter	Description

ANQP	WAN MEtrics
WAN Metrics	Link status and metrics of WAN.

Configuring WAN Metrics

1. Navigate to **Configuration > WLAN > Passpoint** tab.
2. Under ANQP Elements, perform the following:

    a. Select **WAN Metrics** from the drop-down list.

    b. Enter the WAN Metrics in the textbox next to WAN Metrics field.

c. Click **Add** and **Save**.

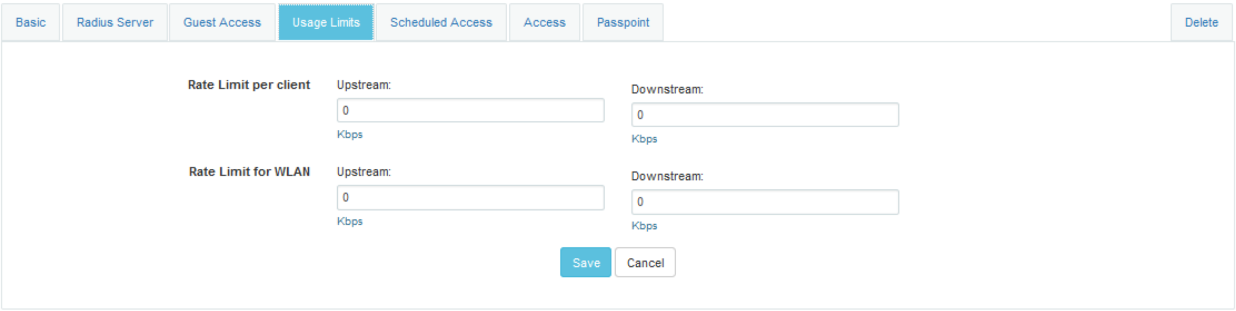
Using CLI

To configure passpoint feature using CLI:

In wlan scope use *passpoint* command

Usage Limit

Usage limit is a WLAN feature that allows to configure the maximum threshold value of bandwidth allowed either per client or per WLAN in both downlink and uplink traffic directions.



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

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

Parameter	Description
Rate Limit per client	Upstream and downstream values for the client.
Rate Limit for WLAN	Upstream and downstream values for WLAN.

Configuring Usage Limit

1. Navigate to **Configuration > WLAN > Usage Limit** tab.
2. Under Rate Limit per client, enter the following:

a. Enter the value for upstream in the **Upstream** textbox.

b. Enter the value for downstream in the **Downstream** textbox.

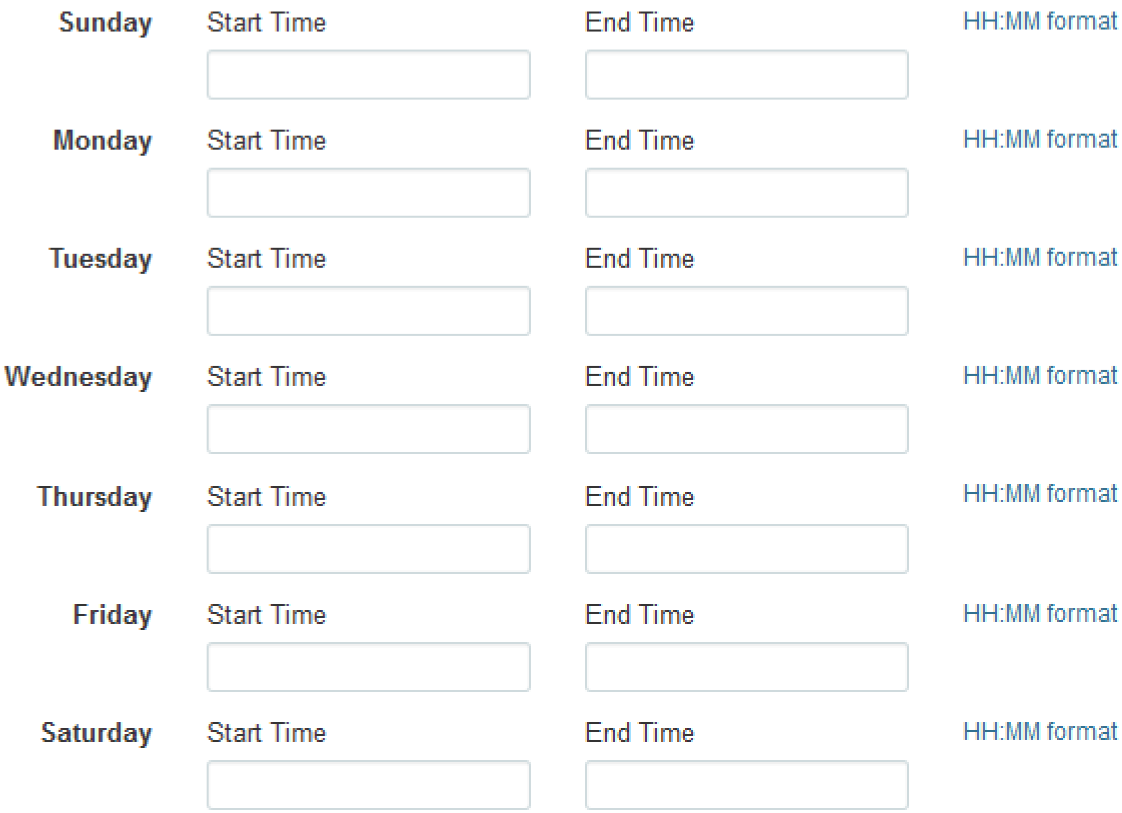
3. Under Rate Limit for WLAN, enter the following:

a. Enter the value for upstream in the **Upstream** textbox.

b. Enter the value for downstream in the **Downstream** textbox.

Scheduled Access

It is a mechanism in which you can enable WiFi access for the configured duration. Time format accepted is in Hours and is in the range of 00:00-23:59. Scheduled access can be configured either for a single or multiple day or for all the days.



Sunday	Start Time	End Time	HH:MM format
Monday	Start Time	End Time	HH:MM format
Tuesday	Start Time	End Time	HH:MM format
Wednesday	Start Time	End Time	HH:MM format
Thursday	Start Time	End Time	HH:MM format
Friday	Start Time	End Time	HH:MM format
Saturday	Start Time	End Time	HH:MM format

Configuring Scheduled Access

1. Navigate to **Configuration > WLAN > Scheduled Access** tab.
2. Enter the start and end time to enable the WiFi access in the respective texboxes
3. Click **Save**.

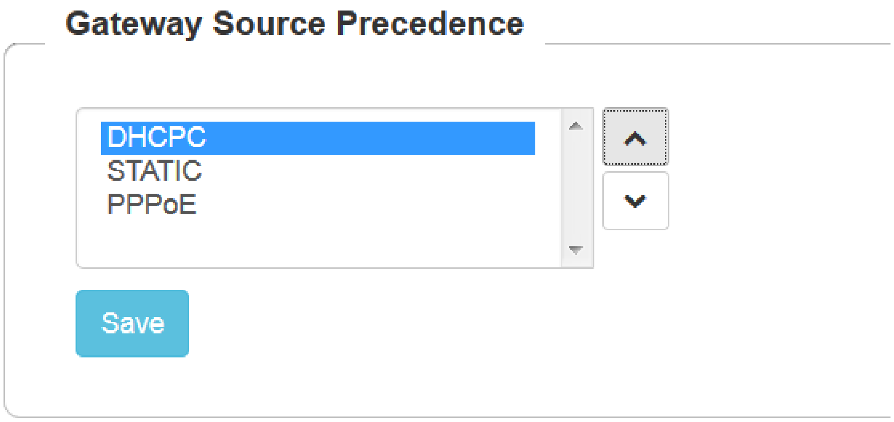
Network Configuration

This section introduces the configuration of various network elements such as Ethernet ports, SVIs, DHCP servers, DNS proxy, management VLAN access, NAT, and port forwarding. Depending of the use case, the required elements can be configured.

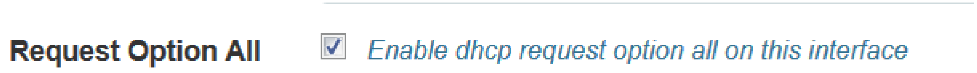
Router Gateway Priorities

This feature enables administrator to select the gateways based on the priority. Currently, there are three sources from which the Gateway, Domain Name Server, domains etc can be learnt and these sources are DHCP, PPPoE and STATIC. Now the administrator has the control on which gateway to install.
To change the priority of the sources and to install the gateway, navigate to **Configuration > Network > Routes** page.

Figure 12: Configure: **Network Configuration > Routes** page



If multiple SVI interfaces are there and if all these interfaces have DHCP clients enabled on them, the gateway learnt from the DHCP server sends the OFFER at the end installs the gateway. Use the ip dhcp request-option-all CLI to enable this feature and in the UI, enable the Request Option All checkbox in the VLAN page.



Request Option All ☑ *Enable dhcp request option all on this interface*

Ethernet Ports

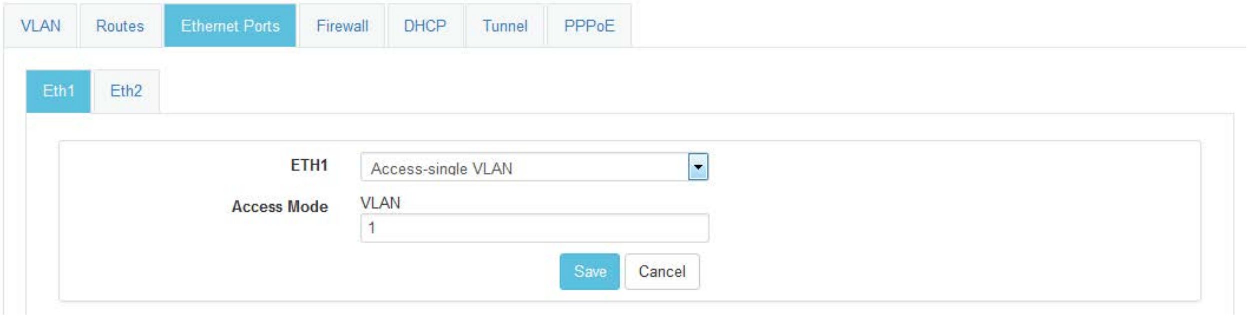
The following table describes the parameters displayed in the **Network Configuration > Ethernet Ports** page.

Table 14: Configure: **Ethernet Ports** parameters

Parameter	Description	Values
Mode	Configure Ethernet port in either trunk or access mode.	trunk/access

	Trunk Mode: Allows traffic with different user defined VLANs (refer allowed VLANs list) to egress & ingress. One of these VLANs can be defined as native VLAN. Traffic with native VLAN will map to untagged traffic based on whether native VLAN is tagged or untagged. **Access Mode**: Allows traffic with specific user defined VLAN (called access VLAN) to egress as untagged and allowed only untagged traffic to ingress and map to access VLAN.	Default mode for Eth1 and Eth2 is access.
Access VLAN*	Untagged traffic on access port will map to the access VLAN inside the device.	1 - 4094
Allowed VLANs^	List of all VLANs which are allowed to ingress and egress from the trunk port and are separated by commas. E.g. 1,14,100,200-567	VLAN List
Native VLAN^	Marks one of the VLANs from allowed VLAN list as native VLAN.	1-4094
Native Tagged^	Maps native VLAN traffic of device to untagged traffic on Ethernet (when enabled) otherwise keep it tagged on Ethernet side.	Enable/Disable
*: valid only in access mode ^: valid only in trunk mode		

Figure 13: Configure: **Network Configuration > Ethernet Ports** page



ETH1: Access-single VLAN

Access Mode: VLAN 1

In the CLI

To switch from configuration context to interface context:

```
(cnPilot Enterprise AP) (configure)# interface eth port-num
```

To configure port mode (default is trunk mode):

```
(cnPilot Enterprise AP) (configure)# switchport mode access/trunk
```

To configure default VLAN of access port (default 1):

```
(cnPilot Enterprise AP)(configure)# switchport access vlan vlan-id
```

To configure allowed VLAN range for trunk port (defaults 1 to 4094):

```
(cnPilot Enterprise AP) (configure)# switchport trunk allowed vlan vlan-range
```

To specify native VLAN for the trunk port (default 1):

```
(cnPilot Enterprise AP) (configure)# switchport trunk native vlan vlan-id
```

To enable native VLAN tagging:

```
(cnPilot Enterprise AP) (configure)# switchport trunk native tagged
```

To disable native VLAN tagging:

```
(cnPilot Enterprise AP) (configure)# no switchport trunk native tagged
```

To display L2 parameters of the ports:

```
(cnPilot Enterprise AP) (configure)# show interface brief
```

Switched Virtual Interface (SVI)

SVI represents virtual interfaces each mapped to a specific VLAN. Each SVI can have static IP or assigned from external DHCP server.

Table 15: Configure: **SVI** parameters

Parameter	Description	Values
IP Address	Configures either IP mode to DHCP or static IP to the SVI. Note: Each SVI should have IP in unique subnet.	• DHCP • Static IP/Network Mask
NAT	When NAT is enabled, IP addresses under this SVI are hidden.	Disable
Zeroconf IP	Creates additional zeroconf IP (169.254.x.y) on the interface alias. Only valid for SVI with VLAN 1.	Enable/Disable
Management Access	The CLI/GUI/SNMP access via this interface.	Wired and Wireless
DHCP Relay Agent	Enables relay agent and assign DHCP server to it.	–
DHCP Option82	DHCP option 82 is also known as the DHCP Relay Agent. When this option is enabled either in WLAN configuration or VLAN section, device appends DHCP Option 82 to DHCP packets initiated from the device. The following parameters are supported in Circuit ID and Remote ID of DHCP Option 82: • Hostname	–

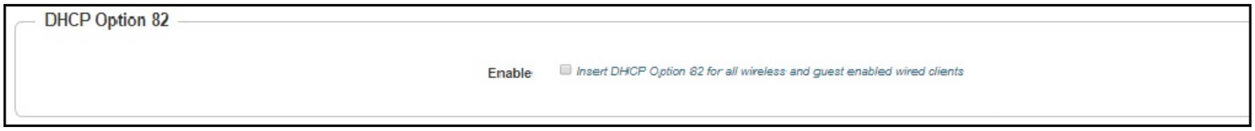
	• AP MAC • BSSID • SSID • Custom	

DHCP Option 82

DHCP option 82 should be enabled, based on the following installments scenario:

- A network that does not contain DHCP Relay Agent should enable DHCP Option 82 parameter in **WLAN > Basic** page.
- A network that has DHCP Relay Agent should enable DHCP Option 82 parameter in **Network > VLAN** page.
- You can enable DHCP Option 82 globally by selecting the **Configuration > Services** page and selecting the **Enable DHCP-Option82** checkbox.

If you enable DHCP-Option82 under Configuration > Services, it will be treated as high priority.



DHCP Option 82

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

You can configure the above parameters through the CLI.

In the CLI

To switch from configuration context to SVI context:

```
(cnPilot Enterprise AP) (configure)# interface vlan vlan-id
```

To configure IP address mode to DHCP client:

```
(cnPilot Enterprise AP) (configure)# ip address dhcp
```

To configures static IP address with a network mask of x bits:

```
(cnPilot Enterprise AP)(configure)# ip address a.b.c.d /x
```

To configures zeroconf (169.254.x.y) IP on SVI:

```
(cnPilot Enterprise AP) (configure)# ip address zeroconf
```

To disable zeroconf IP on an interface:

```
(cnPilot Enterprise AP) (configure)# no ip address zeroconf
```

To display all the created SVIs along with their VLAN and IP address information:

```
(cnPilot Enterprise AP) (configure)# show ip interface brief
```

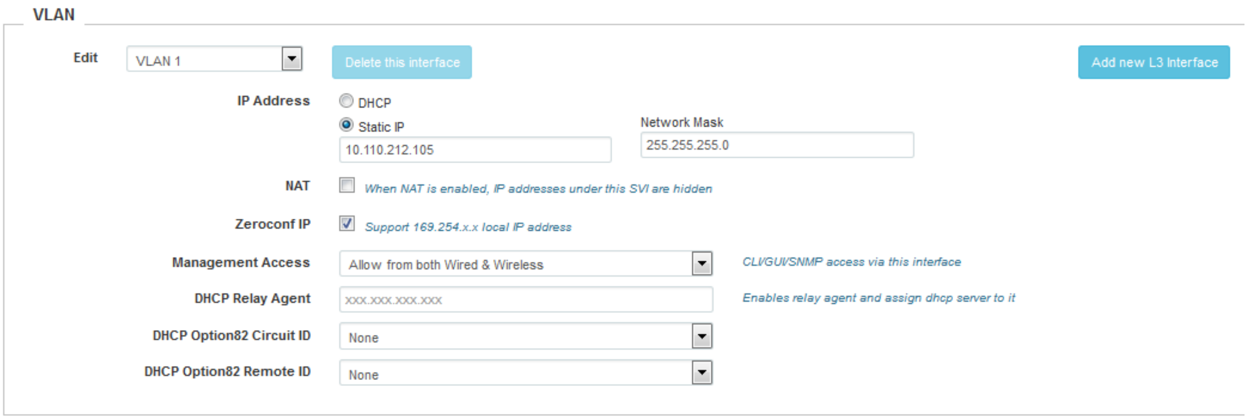
To enable DHCP-Option-82:

```
(Cambium AP) (config)# dhcp-option82 {circuit-id, remote-id, vlan}
```

Example:

```
(Cambium AP) (config)# dhcp-option82 {apmac, hostname, 1}
```

Figure 14: Configure: **Network > VLAN** page



Edit: VLAN 1

IP Address: ○ DHCP ● Static IP 10.110.212.105 Network Mask 255.255.255.0

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 Option82 Circuit ID: None

DHCP Option82 Remote ID: None

DHCP Server

Configures on board DHCP server on a particular SVI. User can configure different DHCP servers on up to 16 SVIs. Mapping between DHCP server and SVI is done through SVI IP address & network parameter of DHCP server configuration.

Table 16: Configure: **DHCP Server** parameters

Parameter	Description	Values
IP Address Range	Specifies the range of IP address to be used for assigning to the clients.	start-ip-address to end-ip-address
Default Router IP	Specifies IP address of the default gateway to be assigned to the clients	ip-addr
Primary & Secondary DNS Server IP	Specifies IP address of the domain name servers. Default values: 8.8.8.8 & 8.8.4.4 (when dns proxy is configured at device) SVI IP & none (when dns proxy is not configured on device)	ip-addr1 ip-addr2 (optional)
Domain Name	Specifies the domain name to be assigned to clients.	string
Lease Time	Specifies the lease time.	days – hours - minutes
network	Specifies subnet of SVI to which this DHCP server should attach.	ip-addr/mask
MAC-IP Bindings	Specifies specific binding between MAC address and IP address.	mac-addr ip-addr

You can configure the above parameters through the CLI.

In the CLI

To switch from configuration context to DHCP pool context:

```
(cnPilot Enterprise AP) (configure)# ip dhcp pool pool-num
```

To configure IP address range to be assigned to the clients:

```
(cnPilot Enterprise AP) (configure)# address-range a.b.c.d A.B.C.D
```

To configure default router IP to be assigned to clients. Default router, if present in address range is excluded.

```
(cnPilot Enterprise AP) (configure)# default-router a.b.c.d
```

To configure primary and secondary DNS server IP to be assigned to clients. Default Value: 8.8.8.8 for primary & 208.67.222.222 for secondary:

```
(cnPilot Enterprise AP) (configure)# dns-server primary-server-ip secondary-server-ip
```

To configure domain name to be assigned to clients:

```
(cnPilot Enterprise AP) (configure)# domain-name
```

To configure lease time:

```
(cnPilot Enterprise AP) (configure)# lease days hrs min
```

To specify subnet (SVI) to attach with DHCP server:

```
(cnPilot Enterprise AP) (configure)# network a.b.c.d /x
```

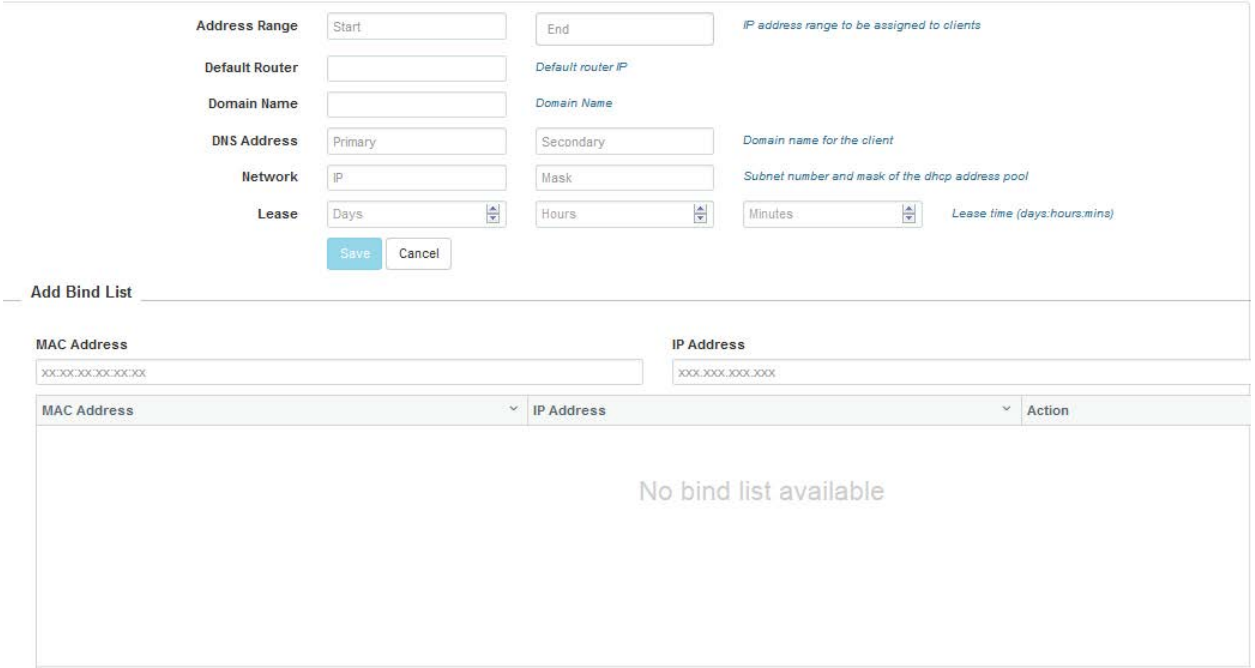
To bind IP address with MAC address. Up to 32 bindings can be specified:

```
(cnPilot Enterprise AP) (configure)# bind xx:xx:xx:xx:xx:xx a.b.c.d
```

```
To destroy the specified DHCP pool:
(cnPilot Enterprise AP) (configure)# no ip dhcp pool pool-num
```

```
To display the pool status, SVI on which DHCP pool is attached & assigned leases to
all client from this pool:
(cnPilot Enterprise AP) (configure)# show dhcp-pool pool-num
```

Figure 15: Configure: **Network > DHCP** page



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	Days	Hours	Minutes	Lease time (days:hours:mins)

Add Bind List

MAC Address	IP Address
xx:xx:xx:xx:xx:xx	xxx.xxx.xxx.xxx

MAC Address	IP Address	Action

No bind list available

DHCP Relay

DHCP relay allows DHCP server in one subnet to be shared by clients in other subnet by relaying DHCP requests. Relay agent configuration is specific to SVI. i.e. any SVI / subnet looking for DHCP server in different subnet needs to have relay agent configured for it.

Table 17: Configure: **DHCP Relay** parameters

Parameter	Description	Value
DHCP Server IP	Specifies the IP address of the DHCP server which should be used of the given subnet. **Note:** It automatically enables relay without any additional command.	ip-address

You can configure the above parameters through the CLI.

In the CLI

To switch from configuration context to SVI context.

```
(cnPilot Enterprise AP) (configure)# interface vlan vlan-id
```

To configure DHCP relay for the SVI with *a.b.c.d* as the DHCP server IP address.

```
(cnPilot Enterprise AP) (configure)# ip dhcp relay server a.b.c.d
```

To display relay:

```
(cnPilot Enterprise AP) (configure)# no ip dhcp relay
```

DNS Proxy

DNS proxy enables local caching of DNS entries from all the interfaces configured on the device. For the queries which cannot be answered from the local cache, external servers are referred.

Table 18: Configure: **DNS Proxy** Parameters

Parameter	Description	Value
State	Configures the state of DNS proxy on the device.	Enable/Disable
External name server	IP address of external name server to be referred by DNS proxy. Up to two name server can be defined. Additionally, any name servers passed by external DHCP servers will also be used as external DHCP server.	Ip-address

You can configure the above parameters through CLI.

In the CLI

To enable DNS server / proxy:

```
(cnPilot Enterprise AP) (configure)# ip dns server
```

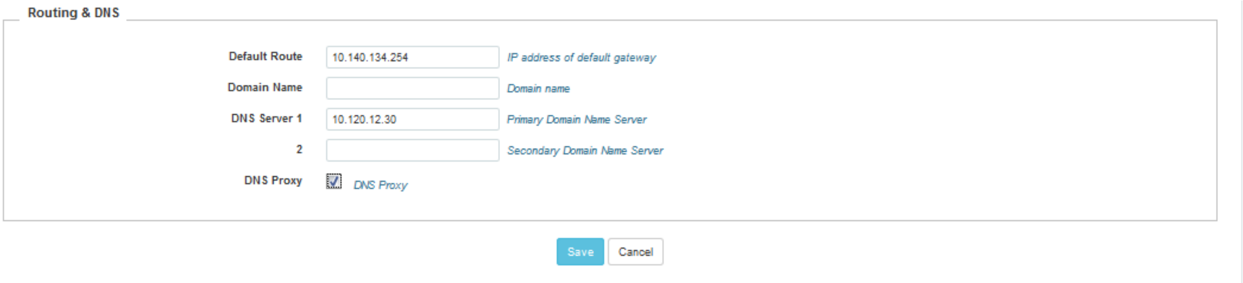
To disable DNS server / proxy:

```
(cnPilot Enterprise AP) (configure)# no ip dns server
```

To configure single external name server:

```
(cnPilot Enterprise AP) (configure)# ip name-server a.b.c.d
```

Figure 16: Configure: **Network > VLAN** page



Routing & DNS

Default Route: 10.140.134.254 — IP address of default gateway

Domain Name: — Domain name

DNS Server 1: 10.120.12.30 — Primary Domain Name Server

2: — Secondary Domain Name Server

DNS Proxy: ☑ DNS Proxy

Management VLAN Access

The management VLAN access allows to restrict device access using a given set (one or more) VLANs. Additionally, access using a given VLAN can be allowed only from wired connection.

Table 19: Configure: **Management VLAN Access** Parameters

Parameter	Description	Values
state	Management VLAN access is per SVI configuration. Disabled: No access of device using this SVI's VLAN Allow-from-wired: Access of device is allowed from wired side using this SVI's VLAN Allow-from-both-wired-wireless: Access of device is allowed from both wired & wireless side using this SVI's VLAN	Disable / allow-from-wired / allow-from-both-wired-wireless

You can configure the above parameters through the CLI.

In the CLI

To switch from configuration context to SVI context:

```
(cnPilot Enterprise AP) (configure)# interface vlan vlan-id
```

To enable management access through given SVI. Access from both wired and wireless is allowed:

```
(cnPilot Enterprise AP)  (configure)# management-access all
```

To enable management access through given SVI. Access from only wired side is permitted:

```
(cnPilot Enterprise AP) (configure)# management-access wired
```

To disable management access through given SVI:

```
(cnPilot Enterprise AP) (configure)# no management-access
```

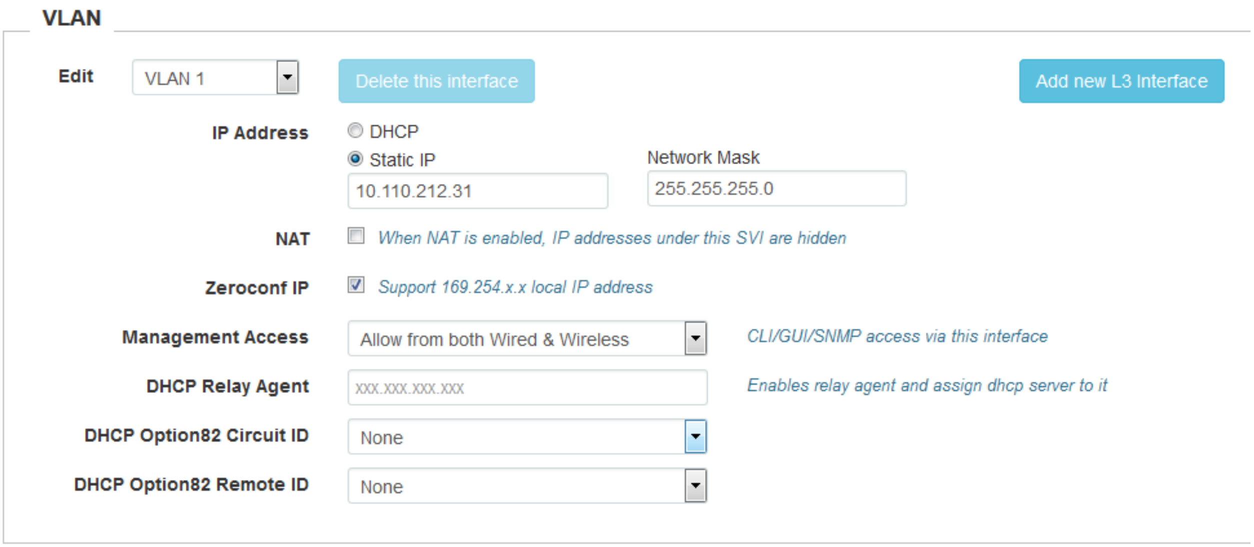
NAT and Port Forwarding

NAT allows to hide IP addresses of a subnet while accessing IP addresses in another subnet. Each SVI / Subnet needs to be individually configured for NAT.

You can configure NAT using the UI and CLI:

In the UI

Figure 17: Configure: **NAT**



Edit: VLAN 1

IP Address: ○ DHCP ● Static IP 10.110.212.31 Network Mask 255.255.255.0

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 Option82 Circuit ID: None

DHCP Option82 Remote ID: None

In the CLI

To switch from configuration context to SVI context:

```
(cnPilot Enterprise AP) (configure)# interface vlan vlan-id
```

To enable NAT for the SVI:

```
(cnPilot Enterprise AP) (configure)# ip nat inside
```

To disable NAT for the SVI:

```
(cnPilot Enterprise AP) (configure)# no ip nat
```

Port Forwarding allows to forward traffic with specific TCP / UDP ports to specific server in NAT enabled subnet. As oppose to NAT which is SVI specific, port forwarding is a global configuration.

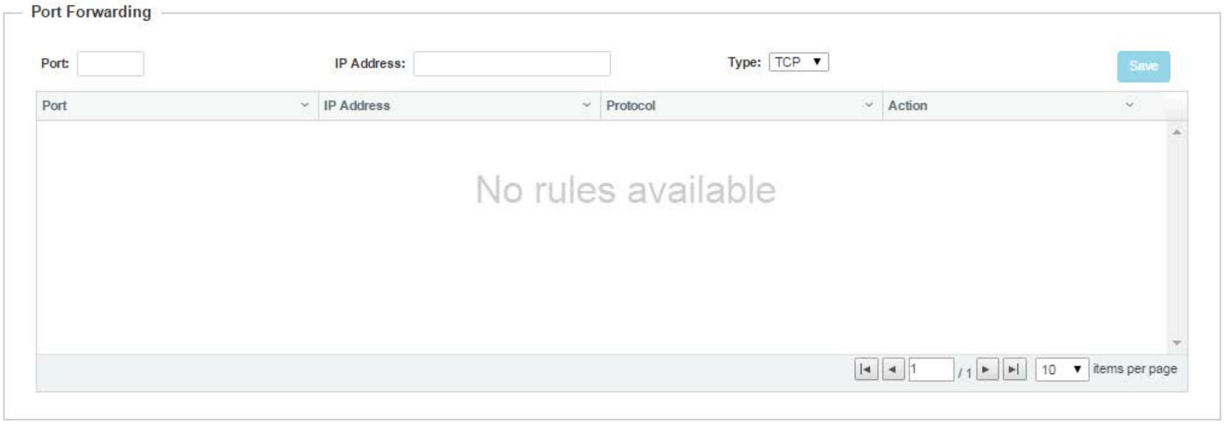
You can configure NAT using UI and the CLI:

In the UI

1. Navigate to the **Configure > Network > Routes** tab. The following fields are displayed:
   a. Enter the port number in the **Port** textbox.
   b. Enter the IP address in the **IP Address** textbox.
   c. Select the type as TCP or UDP from the **Type** drop-down list.

2. Click **Save**.

Figure 18: Configure: **Network > Routes > Port Forwarding** page



In the CLI

To forward TCP port-num to a.b.c.d server:

```
(cnPilot Enterprise AP) (configure)# ip port-forward tcp port-num a.b.c.d
```

To forward UDP port-num to a.b.c.d server:

```
(cnPilot Enterprise AP) (configure)# ip port-forward udp port-num a.b.c.d
```

To disable forwarding of TCP port-num to a.b.c.d server:

```
(cnPilot Enterprise AP) (configure)# no ip port-forward tcp port-num a.b.c.d
```

To disable forwarding of UDP port-num to a.b.c.d server

```
(cnPilot Enterprise AP) (configure)# no ip port-forward udp port-num a.b.c.d
```

L2TPv2 tunnel

This section provides details on L2TPv2 tunnels that are created with external routers such as Microtik's RB750r2, RB3011 (or any other router which provides L2TPv2 tunnel concentration capability).

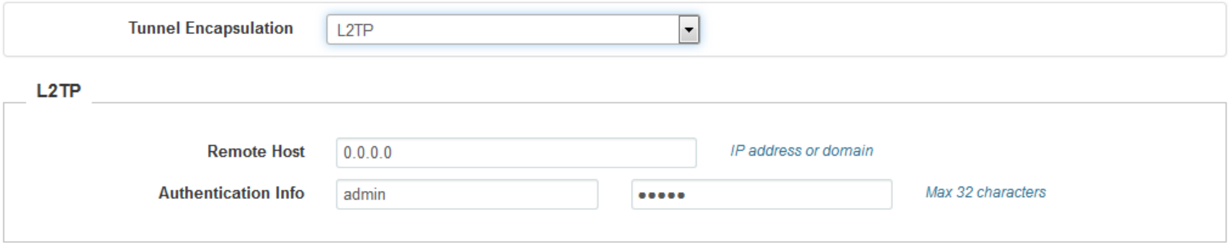
You can configure L2TPv2 tunnel using the UI and CLI.

In the UI

To create L2TPv2 tunnel:

1. Navigate to **Configure > Networks** page.
2. Select **L2TP** Tunnel tab.
3. Select **Enable** checkbox.
4. Enter **Remote IP** and **Authentication Info** details.
5. Click **Save.**

Figure 18: Configure: **Network > L2TP Tunnel** page



Tunnel Encapsulation	L2TP		

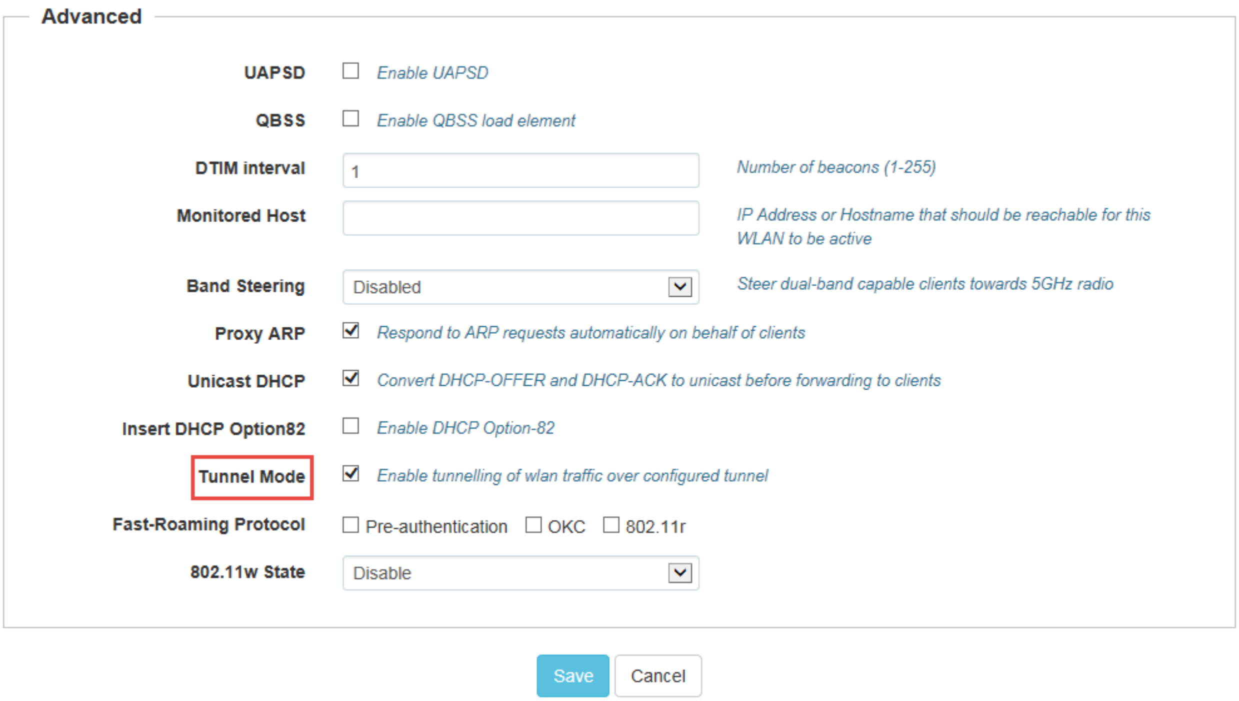
L2TP

Remote Host	0.0.0.0		IP address or domain
Authentication Info	admin	●●●●●	Max 32 characters

To create tunnel mode per WLAN:

Navigate to **Configure > WLAN** page and provide the details.

Figure 19: Configure > WLAN page



Advanced

UAPSD	□ Enable UAPSD	
QBSS	□ Enable QBSS load element	
DTIM interval	1	Number of beacons (1-255)
Monitored Host		IP Address or Hostname that should be reachable for this WLAN to be active
Band Steering	Disabled	Steer dual-band capable clients towards 5GHz radio
Proxy ARP	☑ Respond to ARP requests automatically on behalf of clients	
Unicast DHCP	☑ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients	
Insert DHCP Option82	□ Enable DHCP Option-82	
Tunnel Mode	☑ Enable tunnelling of wlan traffic over configured tunnel	
Fast-Roaming Protocol	□ Pre-authentication □ OKC □ 802.11r	
802.11w State	Disable	

In the CLI

To create L2TPv2 tunnel using CLI:

tunnel l2tp
no shutdown
remote-ip <ip-addr>
auth admin password

To create tunnel mode per WLAN:
host (config)# wireless wlan<id>
host (config-wlan-1)# tunnel-mode

Layer-2 GRE tunnel

As a tunnel peer, the AP encapsulates the packet payload for transport through the tunnel to a destination network. The layer-2 packets are first encapsulated in a GRE packet, and then the GRE packet is encapsulated in an IP protocol. The remote tunnel peer extracts the tunneled packet and forwards the packet to its destination. This allows the source and destination peers to operate as if they have a virtual point-to-point connection with each other.

L2GRE tunnels are stateless, and the endpoint of the tunnel does not contain any information about the state or availability of the remote tunnel end point. Hence the AP operating as a tunnel source peer, cannot change the state of the GRE tunnel interface as per the tunnel interface on the remote peer.

Path MTU Discovery

The AP supports path MTU discovery feature to request the wireless clients to send smaller packets, so that the extra headers addition (GRE and IP header added by the AP) may not lead to fragmentation. This improves the throughput over L2GRE throughput. The path MTU discovery is disabled by default.

TCP MSS CLAMPING

The tcp mss clamping is a technique to reduce the segment size of TCP packets to make compactable with the path MTU. Which in turn avoids fragmentation after adding extra headers from the AP and improves throughput. This feature is enabled by default. The TCP MSS field is a configurable parameter. This feature boosts the TCP throughput over the GRE tunnel.

DSCP

The AP supports DSCP configuration. When a network experiences congestion and delay, some packets might get dropped while the rest are allowed. This is decided by the DSCP value of the packet. DSCP configuration provides flexibility to prioritize the tunnel traffic between the L2GRE peers.

The following table lists the fields that are displayed in the **Configuration > Networks> Tunnel >** page:

Table 21: Configuration: **L2GRE** parameters

Parameter	Description	Default Value
Tunnel Encapsulation	To select any one of the options: • L2GRE • L2TP • OFF	OFF
L2GRE		
Remote Host	IP address or domain name of the remote host.	-
DSCP (Optional)	Differentiated Service Code Point.	0
PMTU Discovery (Optional)	Path MTU discovery.	Disabled

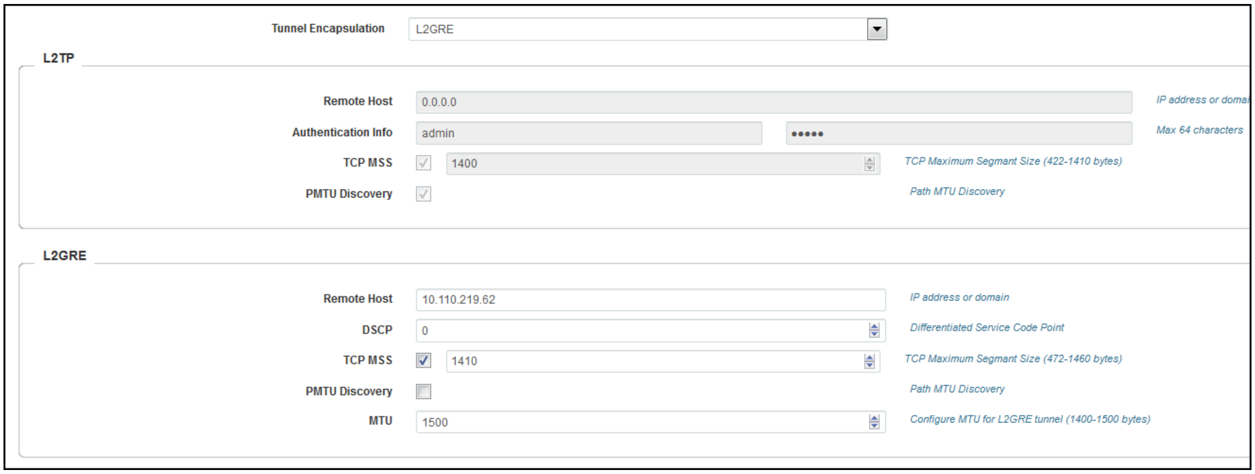
You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > Networks** tab.
2. Select **L2GRE** option from the **Tunnel Encapsulation** drop-down list.

3. Under **L2GRE**, enter the following details:
   a. IP address or domain name of the remote host in the **Remote Host** textbox.
   b. DSCP value in the **DSCP** textbox. By default, the DSCP value is 0.
   c. Select the **PMTU discovery** checkbox to enable path MTU functionality.
4. Click **Save**.

Figure 20: Configuration: **Network > Tunnel** page



Tunnel Encapsulation: L2GRE

L2TP

Remote Host	0.0.0.0		IP address or domai
Authentication Info	admin	•••••	Max 64 characters
TCP MSS	☑	1400	TCP Maximum Segmant 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 Segmant Size (472-1460 bytes)
PMTU Discovery	☐		Path MTU Discovery
MTU	1500		Configure MTU for L2GRE tunnel (1400-1500 bytes)

In the CLI

To enable L2GRE:
(cnPilot Enterprise AP) (configure)# *tunnel encapsulation l2gre*

To configure L2GRE tunnel:
(cnPilot Enterprise AP) (configure)# *tunnel l2gre*
remote-host<ip-addr>
dscp<0-63>
pmtudisc
tcp-mss<472-1460 bytes>

To disable the configured L2GRE tunnel:
(cnPilot Enterprise AP) (configure)# *no tunnel encapsulation*

To view the status of configured L2GRE tunnel:
(cnPilot Enterprise AP) (configure)# *show tunnel-status*

Wired port L2GRE tunnel

L2GRE has its own configuration. Once that is configured, it must be enabled on the indented interface (Wired or Wireless).

Enable tunnel mode on an Interface

The data from both the wired and wireless clients can be tunnelled over L2GRE.

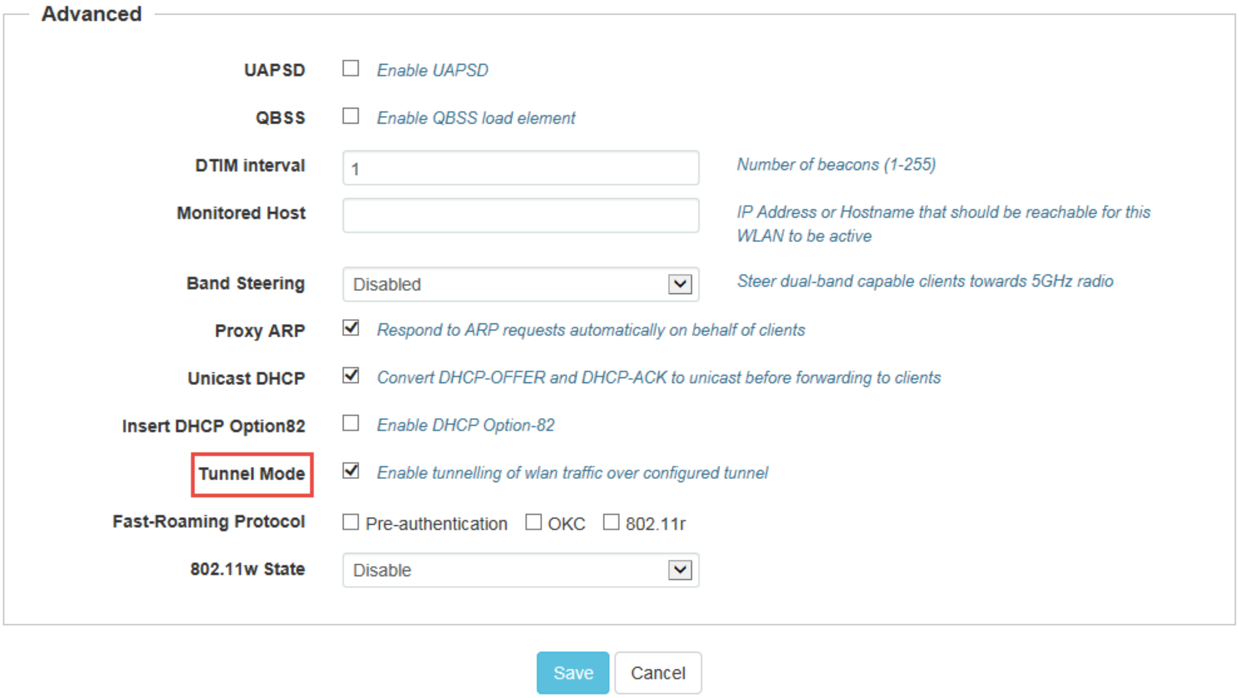
TUNNEL WIRELESS TRAFFIC OVER L2GRE

To create tunnel mode per WLAN:

In the UI

Navigate to **Configure > WLAN** page and provide the details.

Figure 19: Configure > WLAN page



Advanced

UAPSD	☐ *Enable UAPSD*	
QBSS	☐ *Enable QBSS load element*	
DTIM interval	1	*Number of beacons (1-255)*
Monitored Host		*IP Address or Hostname that should be reachable for this WLAN to be active*
Band Steering	Disabled	*Steer dual-band capable clients towards 5GHz radio*
Proxy ARP	☑ *Respond to ARP requests automatically on behalf of clients*	
Unicast DHCP	☑ *Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients*	
Insert DHCP Option82	☐ *Enable DHCP Option-82*	
Tunnel Mode	☑ *Enable tunnelling of wlan traffic over configured tunnel*	
Fast-Roaming Protocol	☐ Pre-authentication ☐ OKC ☐ 802.11r	
802.11w State	Disable	

In the CLI

To create tunnel mode per WLAN:
host (config)# wireless wlan<id>
host (config-wlan-1)# tunnel-mode

TUNNEL WIRED TRAFFIC OVER L2GRE

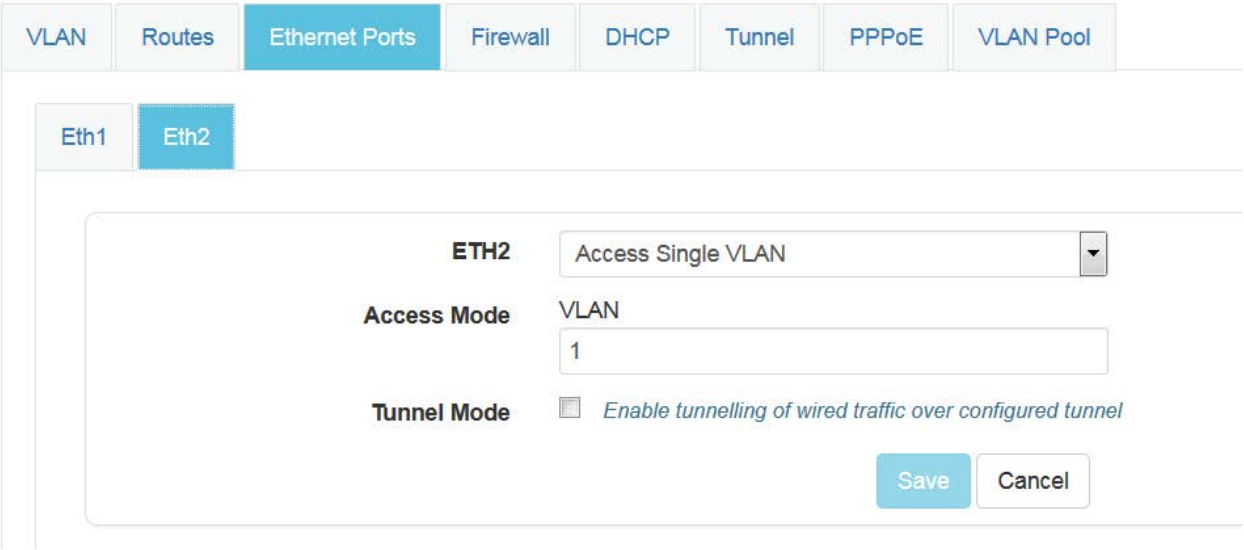
The data from the clients connected to the auxiliary Ethernet ports (Except the primary port, eth0) can be tunnelled over L2GRE.

To configure tunnel wired traffic over L2GRE,

In the UI,

1. Navigate to **Configure** > **Network** > **Ethernet Ports** > **Eth2** tab.
2. Select the **Tunnel Mode** checkbox.

Figure 20: Configure > Ethernet Ports page



ETH2 Access Single VLAN

Access Mode VLAN 1

Tunnel Mode □ *Enable tunnelling of wired traffic over configured tunnel*

In the CLI,

```
host (config)# interface eth 2
host (config-eth-2) # tunnel-mode
```

PPPoE

Point-to-Point Protocol over Ethernet is a method for connecting the users on an Ethernet to the Internet through a DSL line, wireless device or a cable modem.

The following table lists the fields that are displayed in the **Configuration > Networks> PPPoE** page:

Table 22: Configuration: **PPPoE** parameters

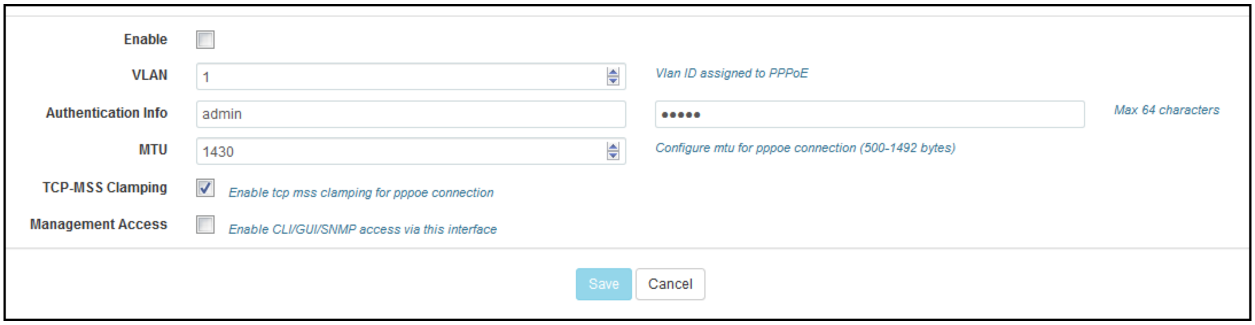
Parameter	Description	Default Value
Enable	To enable the PPPoE functionality.	–
VLAN	The VLAN ID assigned to the PPPoE.	–
Authentication Info	The user name and password for the PPPoE connection.	–
MTU	MTU for PPPoE connection (500-1492 bytes)	–
TCP-MSS Clamping	Enable tcp mss clamping for pppoe connection	Disable

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > Networks** tab. The following fields are displayed:
   a. Select the **Enable** checkbox to enable PPPoE functionality.
   b. Enter the VLAN ID assigned to the PPPoE in the VLAN text box.
   c. Enter the user name and password for the device in the **Authentication Info** text box.
   d. Enter the MTU value PPPoE connection in the **MTU** textbox.
   e. Enable the TCP MSS clamping for the PPPoE connection in the **TCP-MSS Clamping** textbox.
2. Click **Save**.

Figure 21: Configuration: **Network > PPPoE** page



Enable ☐

VLAN 1 — *Vlan ID assigned to PPPoE*

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*

In the CLI

To configure PPPoE:

```
(cnPilot Enterprise AP) (configure)# PPPoE server
(cnPilot Enterprise AP) (configure-server)#
auth
vlan
```

VLAN Pool

VLAN pool is a feature that assigns VLANs to clients from a pool of multiple VLANs by using load balancing mechanism. VLAN pool is useful to segregate clients into multiple VLANs to load balance the network. By assigning different VLANs to clients, a large broadcast domain is divided into small broadcast domains. By using VLAN pool, the chances of data collision and the issues that may occur in the network can be avoided. You can configure a maximum of 16 VLAN pools.

Table 23: Defining VLAN Pool parameters

Parameter	Description	Default Value
VLAN Pool Name	Name of the VLAN pool.	–
VLAN ID List	VLAN ID.	–
Action	To edit or delete the VLAN pool.	–

You can configure the above parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > Networks** tab. The following fields are displayed:
   a. Enter the name of the VLAN pool in the **VLAN Pool Name** functionality.
   b. Enter the VLAN ID in the **VLAN ID** text box.

2. Click **Save**.

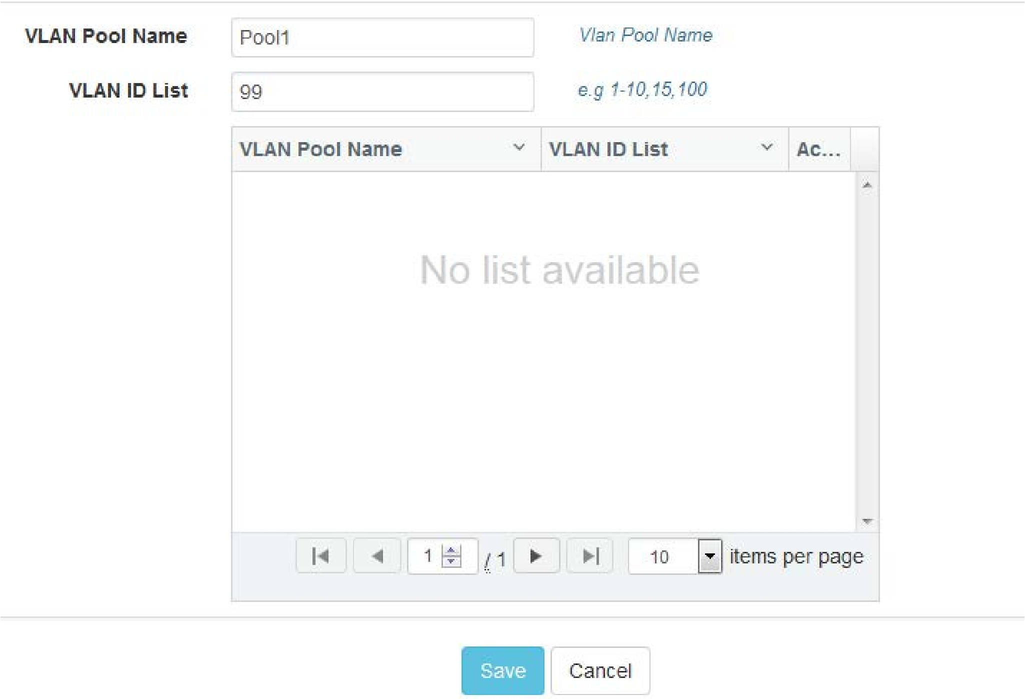
To configure VLAN pool feature:

1. Navigate to **Configure** > **WLAN** > **Basic** page
2. Select any one of the following options for VLAN Pooling:
   - Radius Based
   - Static

If you select **Static**, choose the Static VLAN pool name from the **VLAN Pool Name** drop-down list.

3. Click **Save**.

Figure 22: Defining VLAN Pool page

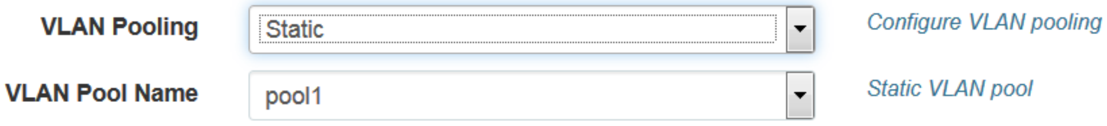


VLAN Pool Name	Pool1	*Vlan Pool Name*
VLAN ID List	99	*e.g 1-10,15,100*

VLAN Pool Name	VLAN ID List	Ac...

No list available

Figure 22: Configuring VLAN Pool



VLAN Pooling: Static — Configure VLAN pooling

VLAN Pool Name: pool1 — Static VLAN pool

In the CLI

To configure VLAN Pool:

```
(cnPilot Enterprise AP) (configure-wlan-1)# vlan-pool radius-based
(cnPilot Enterprise AP) (configure)# vlan-pool pool3 100,110,120
(cnPilot Enterprise AP) (configure)# vlan-pool pool1 10,20,30,40
(cnPilot Enterprise AP) (configure)# vlan-pool pool4 130,140,90
```

Firewall

Firewall options are used to configure options to protect form denial of service (DoS) attacks. By configuring these options AP prevents attacks on its Ethernet and wireless interface so that it does not enter in DoS state for its wireless clients.

Configuring Firewall

You can configure Firewall using the UI or CLI:

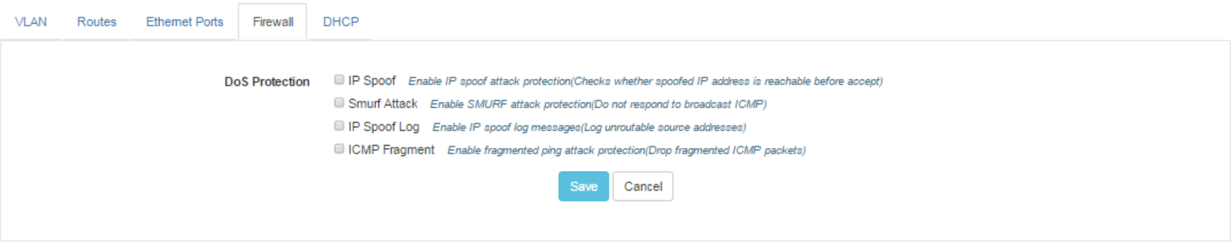
In the UI

1. Navigate to the **Configure > Network** tab. The following fields are displayed:

a. To enable IP spoof, select **IP Spoof** checkbox.
b. To enable smurf attack protection, select **Smurf Attack** checkbox.
c. To enable IP spoof log, select **IP Spoof Log** checkbox.
d. To enable fragmented ping attack protection, select **ICMP Fragment** checkbox.

2. Click **Save.**

Figure 23: Configure: **Network > Firewall** page



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)*

In the CLI

```
(cnPilot Enterprise AP) (configure)# firewall dos-protection {icmp-frag, ip-spoof, ip-spoof-log, smurf-atttack}
```

ACL

ACL provides basic traffic filtering capabilities based on selected type of ACL, for example if user configures an IP ACL then from A.B.C.D. IP address to M.N.O.P IP address traffic will be dropped. The AP examines each packet to determine whether to forward or drop the packet, on the basis of the criteria such as:

- Allow or Deny criterion
- Source or Destination IP address of the traffic
- Source or Destination MAC address of the traffic
- Upper-layer protocol types

- Source or destination port information.

A maximum of 256 rules per network interface and rules are processed in the order of precedence (1=high; 256=low).

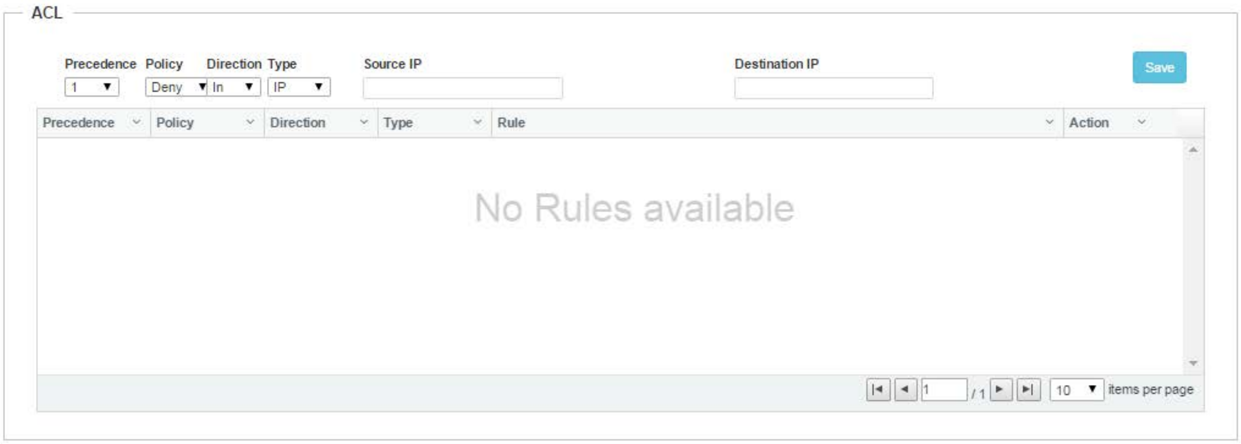
Configuring ACL

You can configure ACL using the UI and the CLI.

In the UI

1. Navigate to the Configure > WLAN > Access tab. The following fields are displayed:
   a. Select preference from the Preference drop-down list.
   b. Select type of policy from Policy drop-down list.
   c. Select direction from the Direction drop-down list.
   d. Select type from the Type drop-down list.
   e. Enter IP address of source in the Source IP text box.
   f. Enter IP address of destination in the Destination IP text box.
2. Click Save.

Figure 24: Configure: **Network > ACL** page



Precedence: 1
Policy: Deny
Direction: In
Type: IP
Source IP:
Destination IP:
10 items per page

In the CLI

```
(cnPilot Enterprise AP) (config-wlan-1# acl {deny, permit}

(cnPilot Enterprise AP) (config-wlan-1# acl deny {ip, mac, proto}

(cnPilot Enterprise AP) (config-wlan-1)# acl permit ip

  acl permit ip PRECEDENCE (SOURCE-IP{/{mask|prefix-length}}|any) (DESTINATION-
IP{/{mask|/prefix-length}}|any) (in|out|any)

 Example: acl permit ip 255 any any any
```

```
(cnPilot Enterprise AP) (config-wlan-1)# acl permit mac
```

acl permit mac PRECEDENCE (SOURCE-MAC{(optional)/{mask|prefix-length}}|any) (DESTINATION-MAC{(optional)/{mask|prefix-length}}|any) (in|out|any)<(optional)//description>

Example:

acl permit mac 50 00-01-02-03-04-05 00-01-02-09-08-07 in

(examples of mask based mac acl rule)

acl permit mac 50 00-01-02-03-04-06/ff-ff-ff-00-00-00 00-01-02-09-08-07/ff-ff-ff-00-00-00 in

acl permit mac 50 00-01-02-03-04-05/24 00-01-02-09-08-07/24 in

```
(cnPilot Enterprise AP) (config-wlan-1)# acl permit proto

acl permit proto PRECEDENCE (tcp|udp|icmp|any) (SOURCE-IP{/{mask|prefix-length}}|any)
(SOURCE-PORT|any) (DESTINATION-IP{/{mask|prefix-length}}|any) (DESTINATION-PORT|any)
(in|out|any) #Please ignore port for ie
```

Example: acl permit proto 30 tcp any any any 10000 out

Note

If ACL rules are configured and there is no matching rule exist then by default packets will be dropped. So it is advised to add default rule with lower priority to allow or deny un-matched traffic.

DNS ACL

DNS ACL gives URL filtering based on the domain name in DNS Requests. User can configure allow or deny list based on the requirements. If a domain has been configured as allow then the wireless clients can load that URL. If a domain has been kept as deny then those URLs will be blocked by AP Wildcards as domain names are supported (Eg: *.google.com). You can configure upto 256 entries per WLAN.

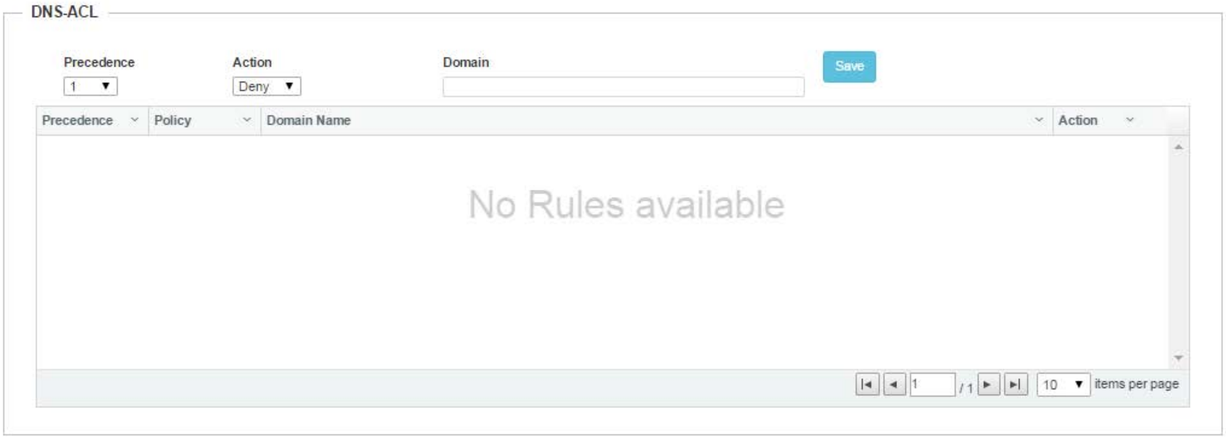
Configuring DNS ACL

You can configure DNS ACL using the UI or CLI:

In the UI

1. Navigate to the **Configure > WLAN > Access** tab. The following fields are displayed:
   a. Select preference from the Preference drop-down list.
   b. Select type of action from Action drop-down list.
   c. Enter domain name in the Domain text box.
2. Click **Save**.

Figure 25: Configure: **Network > WLAN > DNS-ACL** page



Precedence: 1

Action: Deny

Domain:

In the CLI

```
(cnPilot Enterprise AP) (config-wlan-1# dns-acl {deny, permit}
```

MAC Authentication

MAC Authentication is a feature supported by Wi-Fi products to authorize wireless station that tries to associate AP.

Configuring MAC Authentication

The following table lists the fields that are displayed in the **Configuration > WLAN > Access** page:

Table 24: Configuration: **MAC Authentication** parameters

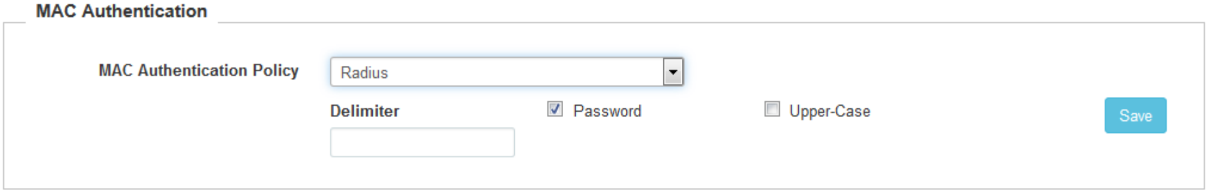
Parameter	Description	Default Value
MAC Authentication Policy	**Permit** - If this option is selected, • Wireless station MAC addresses listed will be allowed to associate to AP. • Wireless station MAC address that are not listed will be de-authenticated from the AP. Wireless station entries that are disassociated or de-authenticated due to MAC Access Control List [ACL] or MAC authentication is displayed in UI under **Troubleshoot > Unconnected Clients** section. **Deny** - This option is set as default. It allows all wireless stations to associate to AP. When user configures a MAC Address, those wireless station shall be denied to associate	–

	and the non-listed MAC address will be allowed. **Radius** - Wireless station MAC is authenticated using RADIUS server. If denied, AP transmits disassociation or de-authentication frame to wireless station with reason code 0x01. • User can select the MAC address format that needs to be communicated with RADIUS server. Following parameters are available to user to select MAC address format: o Delimiter ▪ By default, ‘:’ delimiter is used by AP. ▪ User can select supported delimiter as configured on RADIUS server. o Upper Case ▪ This is disabled by default. ▪ If selected, AP transmits upper case letter. o Password ▪ By default, this is selected and AP sends MAC address as password to RADIUS server. **cnMaestro –** Centralized method of MAC authentication is supported by cnPilot devices using Association ACL feature supported in cnMaestro.	

In the UI

1. Navigate to the **Configuration > WLAN > Access > MAC Authentication** section.
2. Select the MAC Authentication option as **Permit**, **Deny**, **Radius** or **cnMaestro.**
3. If you choose Permit or Deny, enter the MAC in the **MAC** textbox.
4. If you choose cnMaestro, then AP follows ACL list which is configured on On-Premises/cnMaestro
5. Click **Save**.

Figure 26: Configurations: **WLAN > Access> MAC Authentication** page



MAC Authentication

MAC Authentication Policy: Radius

Delimiter:

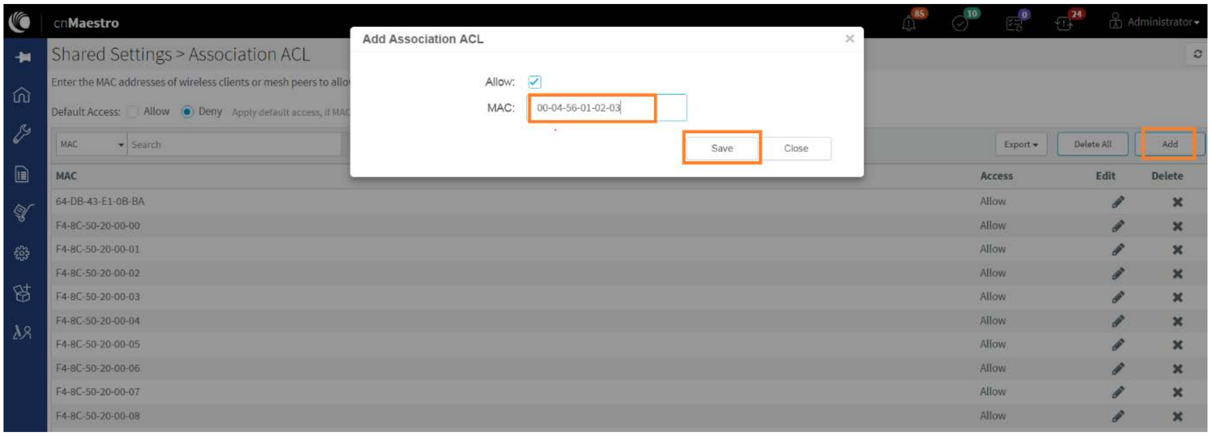
☑ Password

☐ Upper-Case

Configuring Association ACL in cnMaestro

To configure the Access Control List (ACL) in cnMaestro:

1. Navigate to **Shared Settings** > **Association ACL** page.
2. Click **Add** to add a MAC under **Association ACL**..



Shared Settings > Association ACL

Enter the MAC addresses of wireless clients or mesh peers to allo

Default Access: ○ Allow ● Deny Apply default access, if MAC

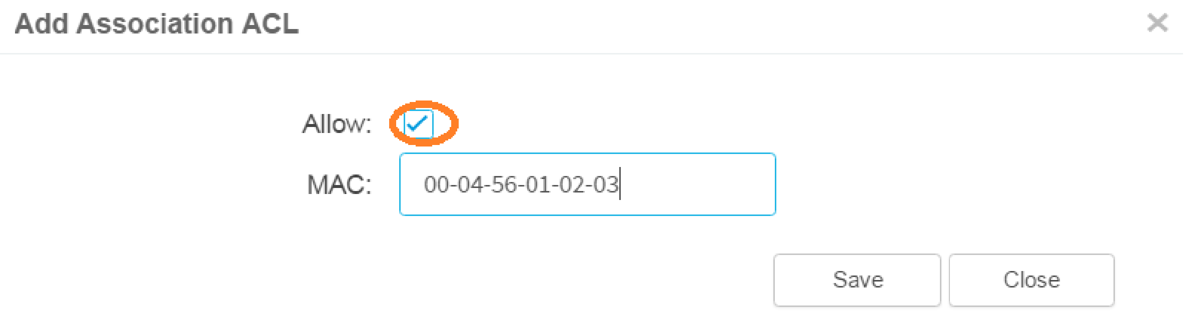
Add Association ACL

Allow: ☑

MAC: 00-04-56-01-02-03

MAC	Access	Edit	Delete
64-DB-43-E1-0B-BA	Allow	✎	✖
F4-8C-50-20-00-00	Allow	✎	✖
F4-8C-50-20-00-01	Allow	✎	✖
F4-8C-50-20-00-02	Allow	✎	✖
F4-8C-50-20-00-03	Allow	✎	✖
F4-8C-50-20-00-04	Allow	✎	✖
F4-8C-50-20-00-05	Allow	✎	✖
F4-8C-50-20-00-06	Allow	✎	✖
F4-8C-50-20-00-07	Allow	✎	✖
F4-8C-50-20-00-08	Allow	✎	✖

3. Enter the required MAC and select the **Allow** check box. If Allow is selected, client is able to associate with the AP, if it is unchecked then it will be added in the denied list.

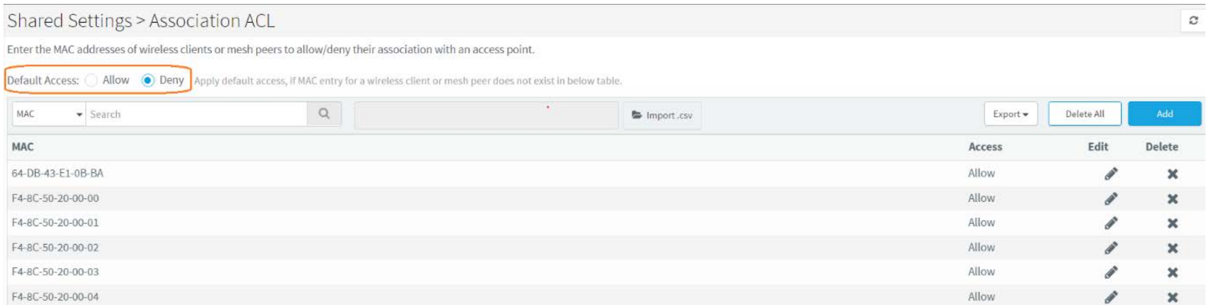


Add Association ACL

Allow: ☑

MAC: 00-04-56-01-02-03

4. Click **Save**.
5. If client is not present in the MAC list then it will follow Default Access the policy (either Deny or Allow).



Shared Settings > Association ACL

Enter the MAC addresses of wireless clients or mesh peers to allow/deny their association with an access point.

Default Access: ○ Allow ● Deny Apply default access, if MAC entry for a wireless client or mesh peer does not exist in below table.

MAC	Access	Edit	Delete
64-DB-43-E1-0B-BA	Allow	✎	✖
F4-8C-50-20-00-00	Allow	✎	✖
F4-8C-50-20-00-01	Allow	✎	✖
F4-8C-50-20-00-02	Allow	✎	✖
F4-8C-50-20-00-03	Allow	✎	✖
F4-8C-50-20-00-04	Allow	✎	✖

AutoPilot

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

- Configuration
- Statistics
- Events
- Firmware

Configuration and Onboarding

This section provides required information to:

- Configure Member AP to Autopilot Master
- Configuring the Master AP
- Configuring WLAN in Default WLAN Group
- Configuring WLANs with User Created WLAN Group
- Configuring WPA2-Enterprise WLAN
- Onboard Member APs to Autopilot Master
- WLAN-Group Override
- Connect clients to the WLANs and check statistics

Configure Member AP to Autopilot Master

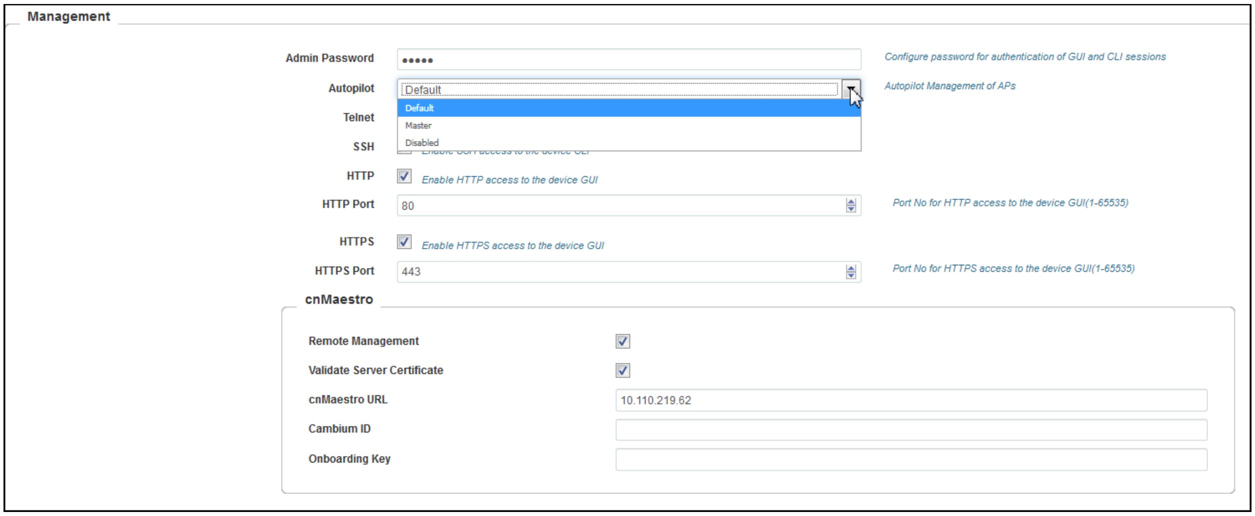
To configure member APs to a Master,

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

Note

The AP needs to be upgraded with autopilot firmware.

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



Management

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

Autopilot: Default — Autopilot Management of APs

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)

cnMaestro

Remote Management: ☑

Validate Server Certificate: ☑

cnMaestro URL: 10.110.219.62

Cambium ID:

Onboarding Key:

3. Save the configuration.
4. Refresh the web page and AP brings up the Autopilot GUI.

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

Configuring the Master AP

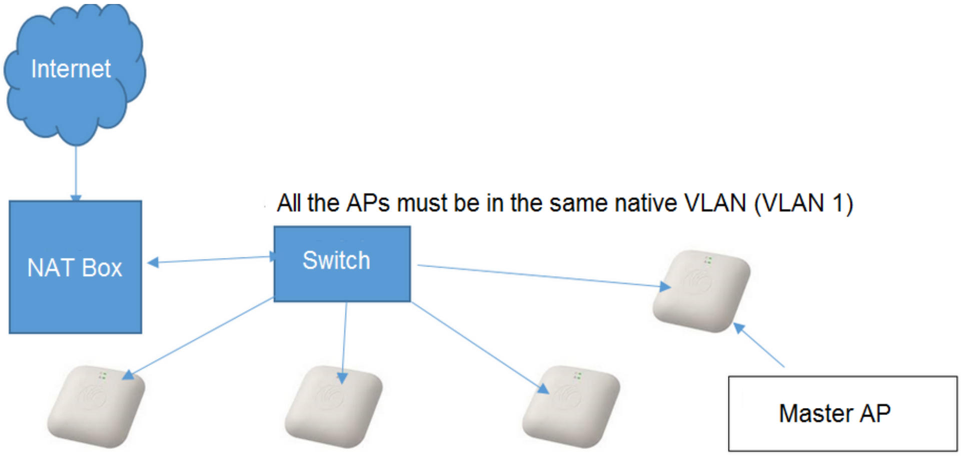
You can configure an AP in the following ways:

- Configuring an AP with Internal DHCP Server
- Configuring an AP with Enternal 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 as shown in the following figure.



Configure an AP with default WLAN group

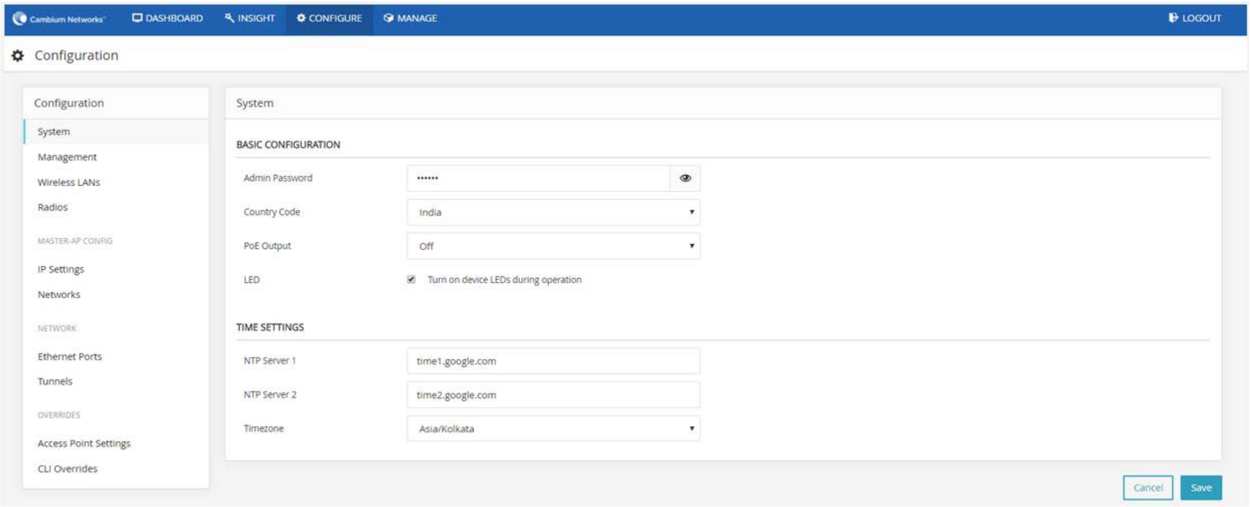
To configure an AP with default WLAN group:

1. Connect all the APs to the native VLAN; for example, VLAN 1 as shown in the above figure.
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

Configure Master AP

To configure the Master AP,

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



System

BASIC CONFIGURATION

Admin Password: ••••••

Country Code: India

PoE Output: Off

LED: ☑ Turn on device LEDs during operation

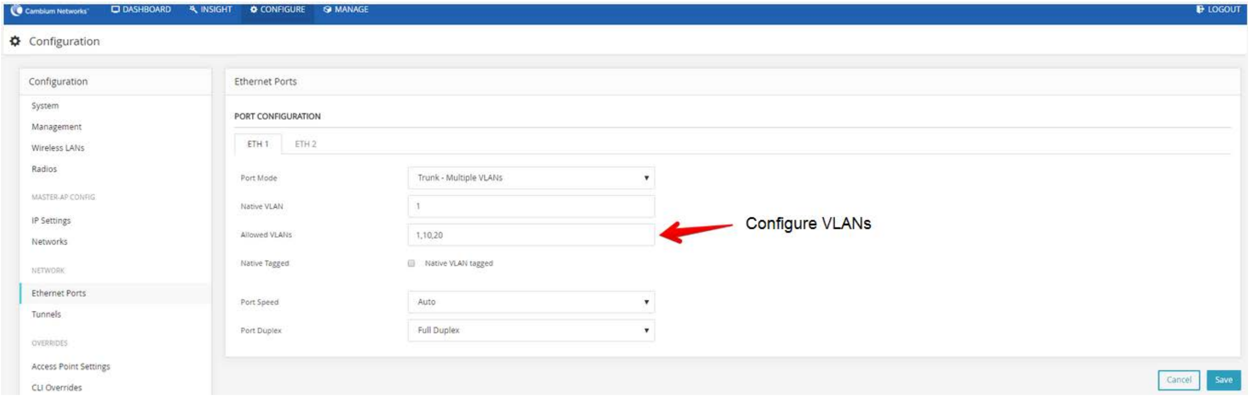
TIME SETTINGS

NTP Server 1: time1.google.com

NTP Server 2: time2.google.com

Timezone: Asia/Kolkata

2. Go to **CONFIGURE** tab -> **NETWORK** -> **Ethernet Ports** and configure the Ethernet ports as trunk.



Ethernet Ports

PORT CONFIGURATION

ETH 1 | ETH 2

Port Mode: Trunk - Multiple VLANs

Native VLAN: 1

Allowed VLANs: 1,10,20

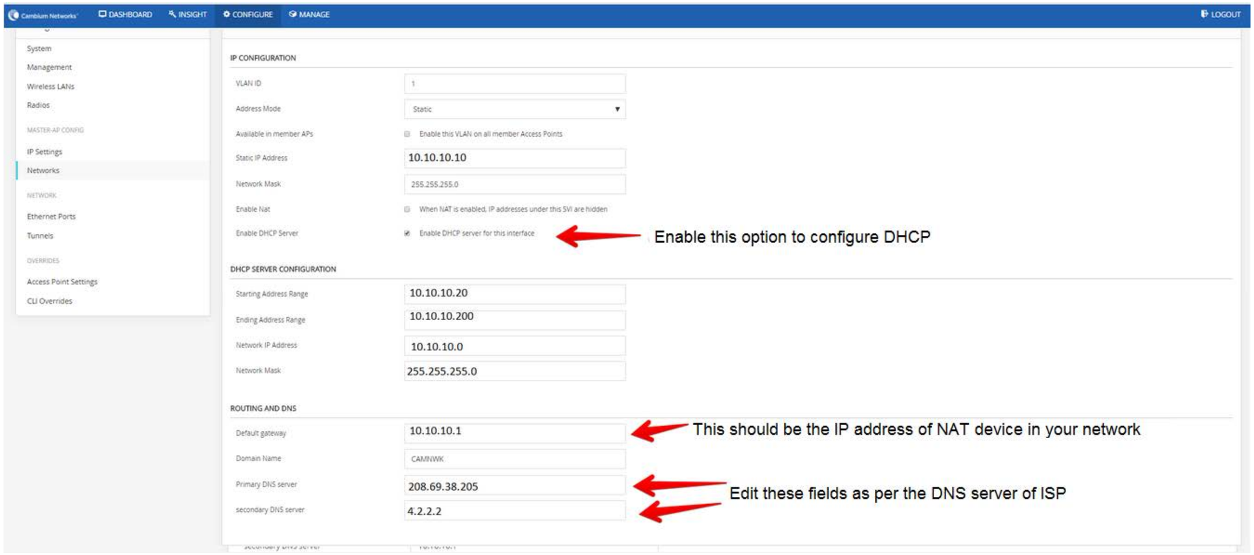
Configure VLANs

Native Tagged: □ Native VLAN tagged

Port Speed: Auto

Port Duplex: Full Duplex

3. Go to **CONFIGURE** tab -> **MASTER AP CONFIG** -> **Networks** and configure the Static IP Address and the DHCP Server for VLAN 1 (native VLAN).
4. 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.



IP CONFIGURATION

VLAN ID: 1

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

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

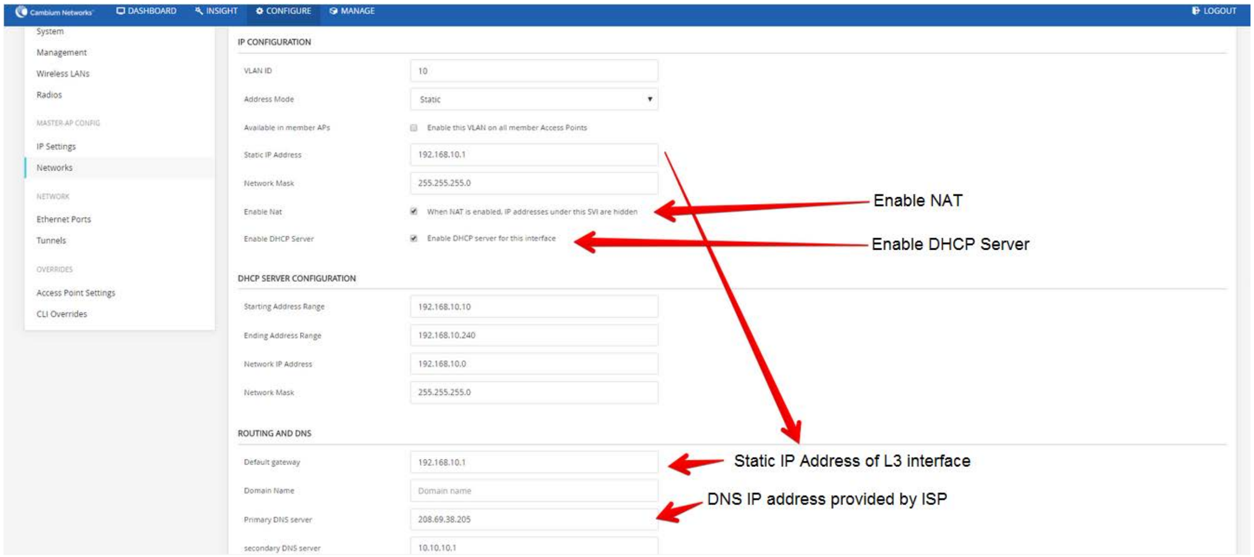
Domain Name: CAMNWK

Primary DNS server: 208.69.38.205

secondary DNS server: 4.2.2.2

Edit these fields as per the DNS server of ISP

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



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	192.168.10.10
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	Domain name
Primary DNS server	208.69.38.205
secondary DNS server	10.10.10.1

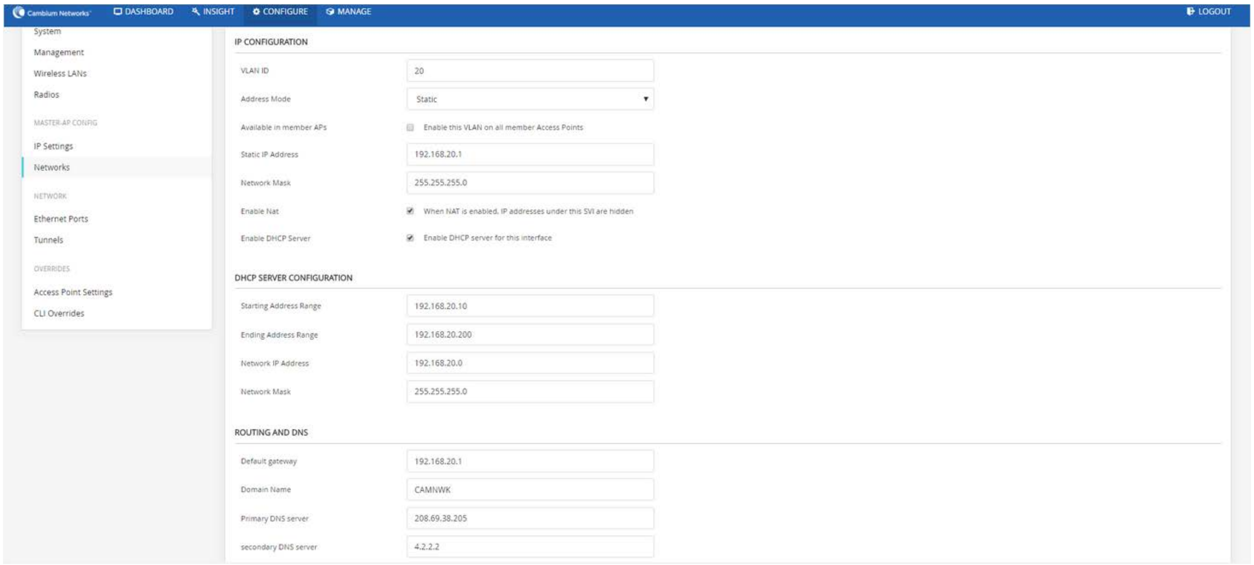
Enable NAT

Enable DHCP Server

Static IP Address of L3 interface

DNS IP address provided by ISP

6. Add L3 interface of VLAN 20 and enable DHCP server and NAT as shown in the following figure.



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	192.168.20.10
Ending Address Range	192.168.20.200
Network IP Address	192.168.20.0
Network Mask	255.255.255.0

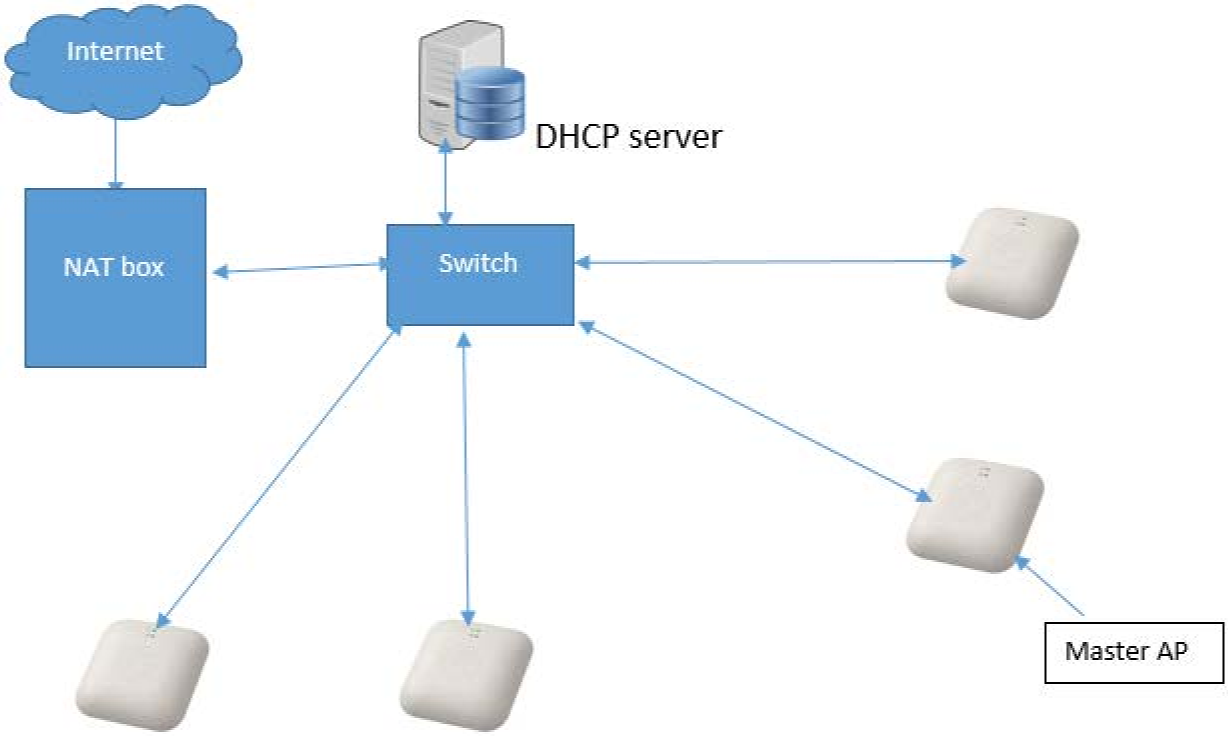
ROUTING AND DNS

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

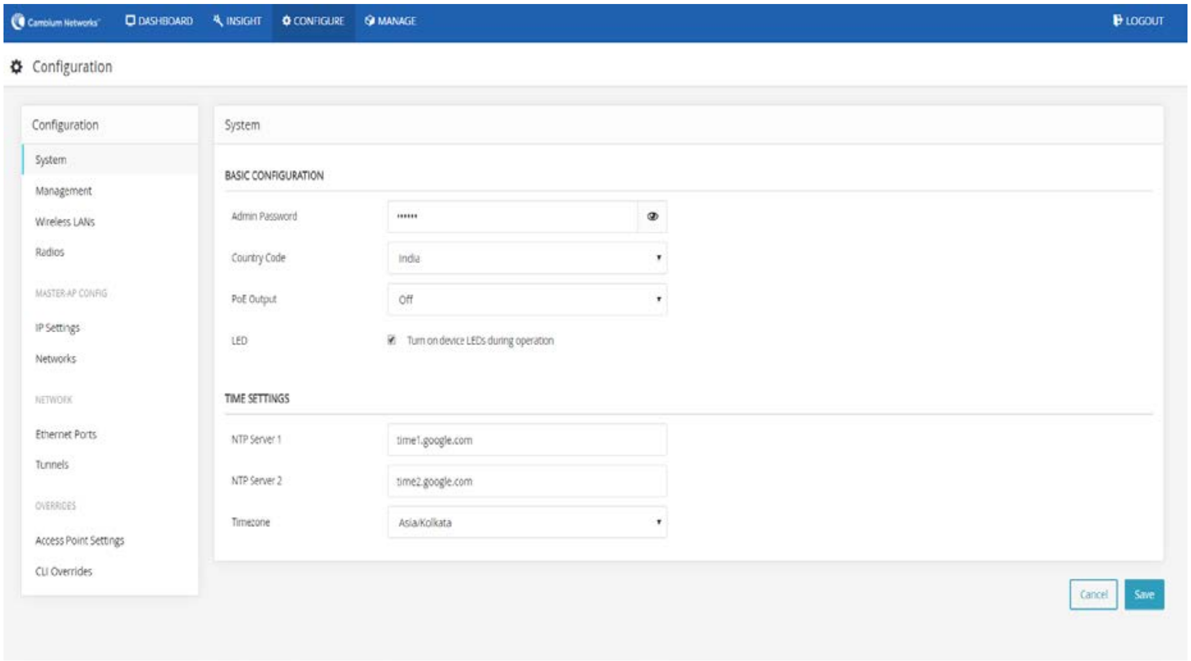
Initial network installments with external DHCP server and NAT box. The complete network is connected to VLAN 1.



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

Configure Master AP

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



System

BASIC CONFIGURATION

Admin Password: ••••••

Country Code: India

PoE Output: Off

LED: ☑ Turn on device LEDs during operation

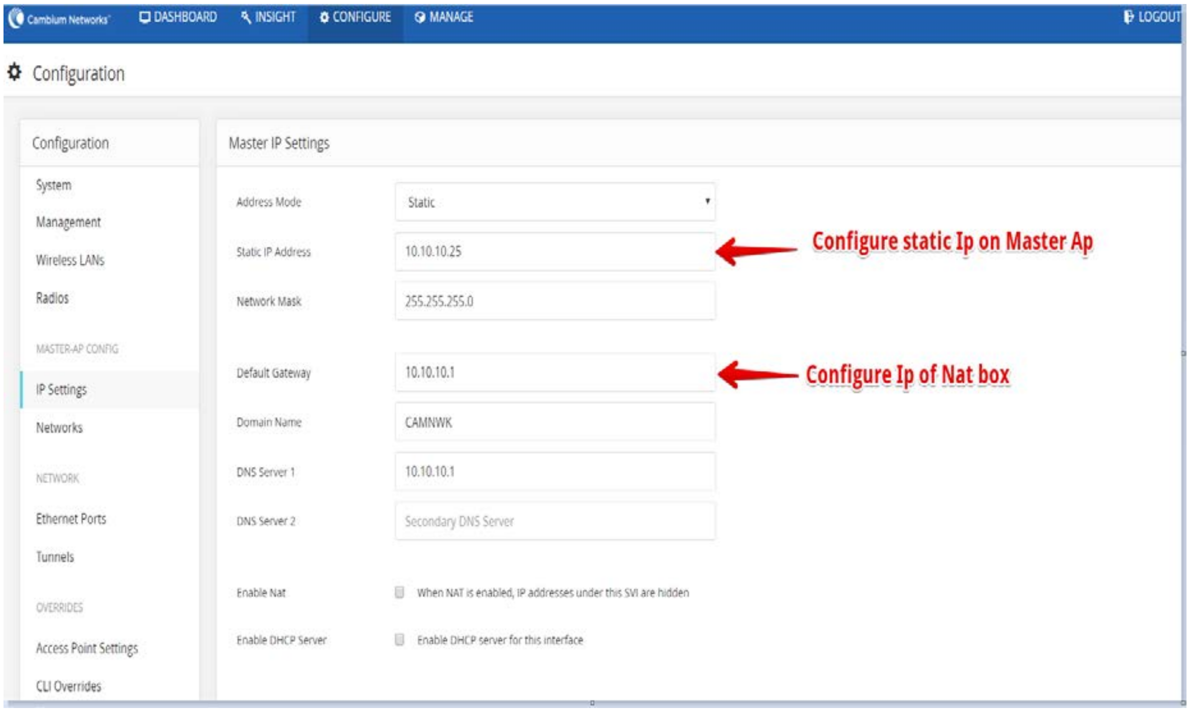
TIME SETTINGS

NTP Server 1: time1.google.com

NTP Server 2: time2.google.com

Timezone: Asia/Kolkata

2. Configure static IP on Master



Master IP Settings

Address Mode	Static
Static IP Address	10.10.10.25
Network Mask	255.255.255.0
Default Gateway	10.10.10.1
Domain Name	CAMNWK
DNS Server 1	10.10.10.1
DNS Server 2	Secondary DNS Server
Enable Nat	□ When NAT is enabled, IP addresses under this SVI are hidden
Enable DHCP Server	□ Enable DHCP server for this interface

Configure static Ip on Master Ap

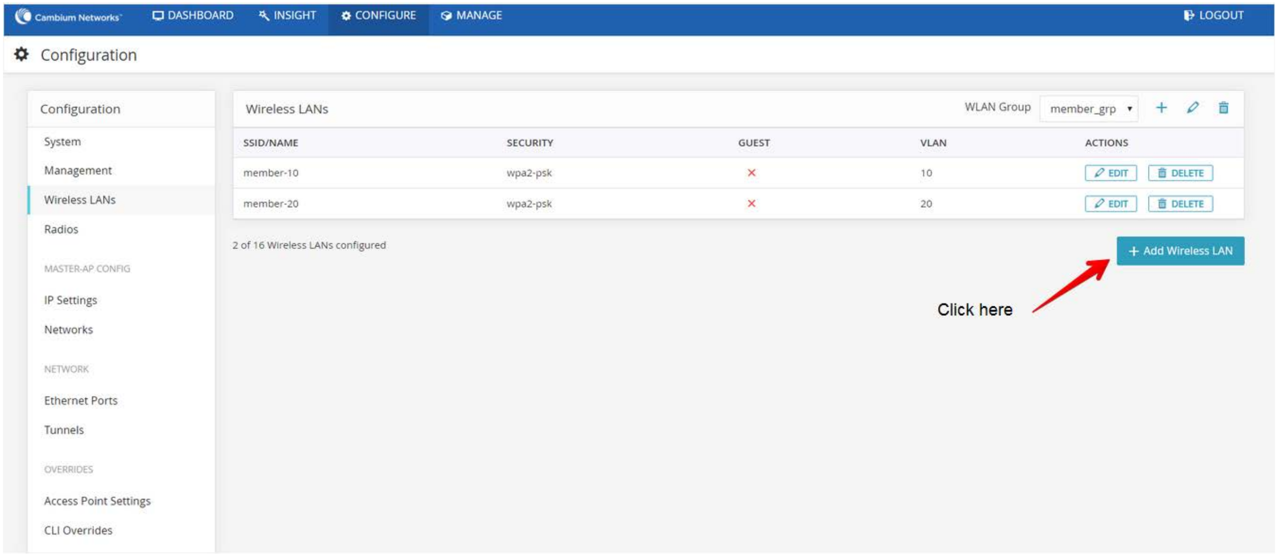
Configure Ip of Nat box

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.



Wireless LANs

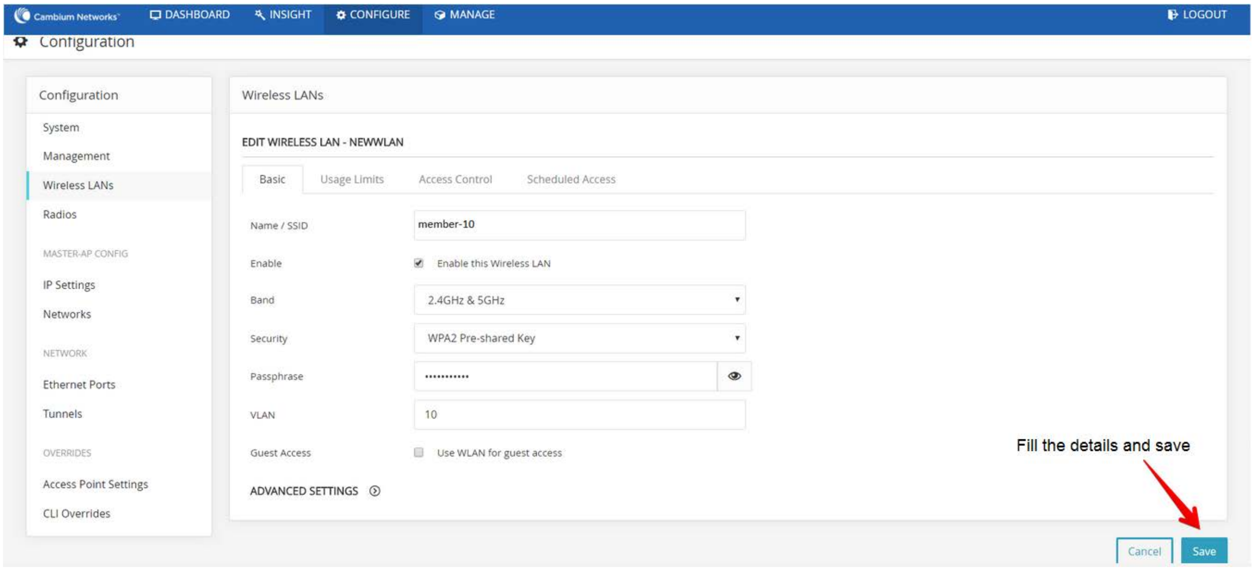
WLAN Group member_grp

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

Click here

2. Provide SSID and password in respective fields. Configure **VLAN** as 10 and save.



EDIT WIRELESS LAN - NEWWLAN

Name / SSID: member-10

Enable: ☑ Enable this Wireless LAN

Band: 2.4GHz & 5GHz

Security: WPA2 Pre-shared Key

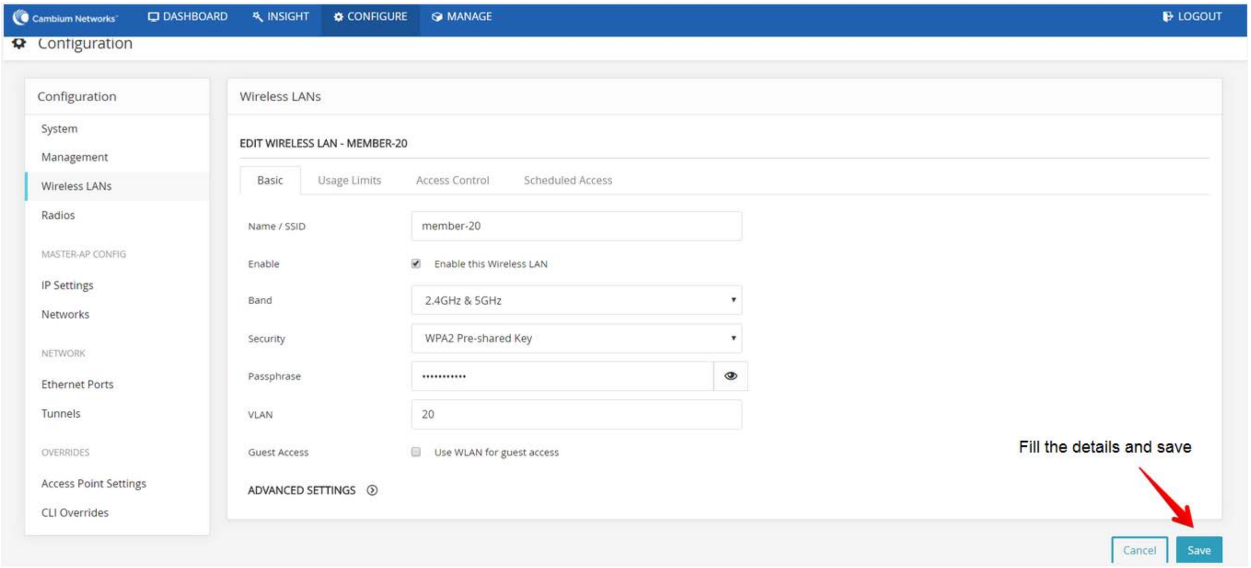
Passphrase: •••••••••••

VLAN: 10

Guest Access: □ Use WLAN for guest access

Fill the details and save

3. Add another WLAN with VLAN 20. Edit SSID and password as required. Configure VLAN as 20 and save.



EDIT WIRELESS LAN - MEMBER-20

Name / SSID: member-20

Enable: ☑ Enable this Wireless LAN

Band: 2.4GHz & 5GHz

Security: WPA2 Pre-shared Key

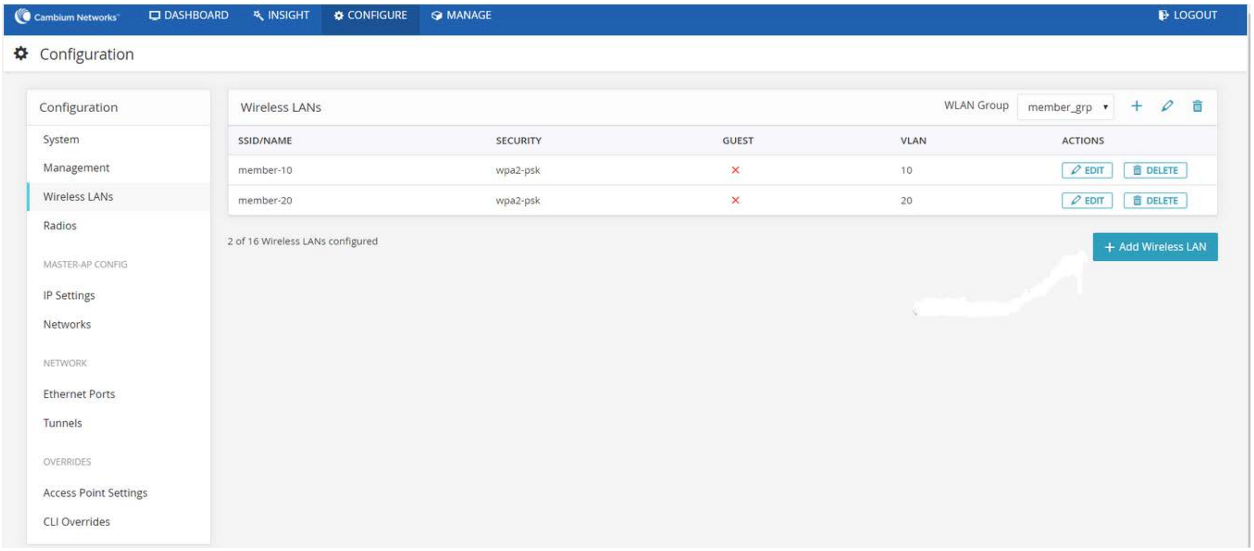
Passphrase: •••••••••••

VLAN: 20

Guest Access: □ Use WLAN for guest access

Fill the details and save

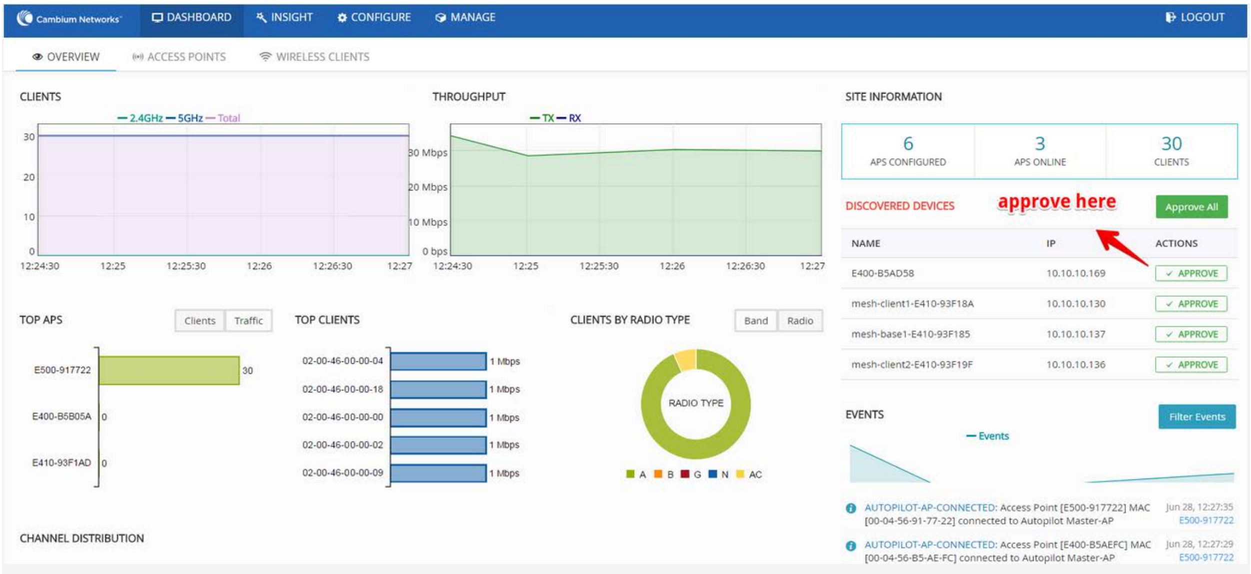
4. Check the configured WLANs.



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

5. 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.



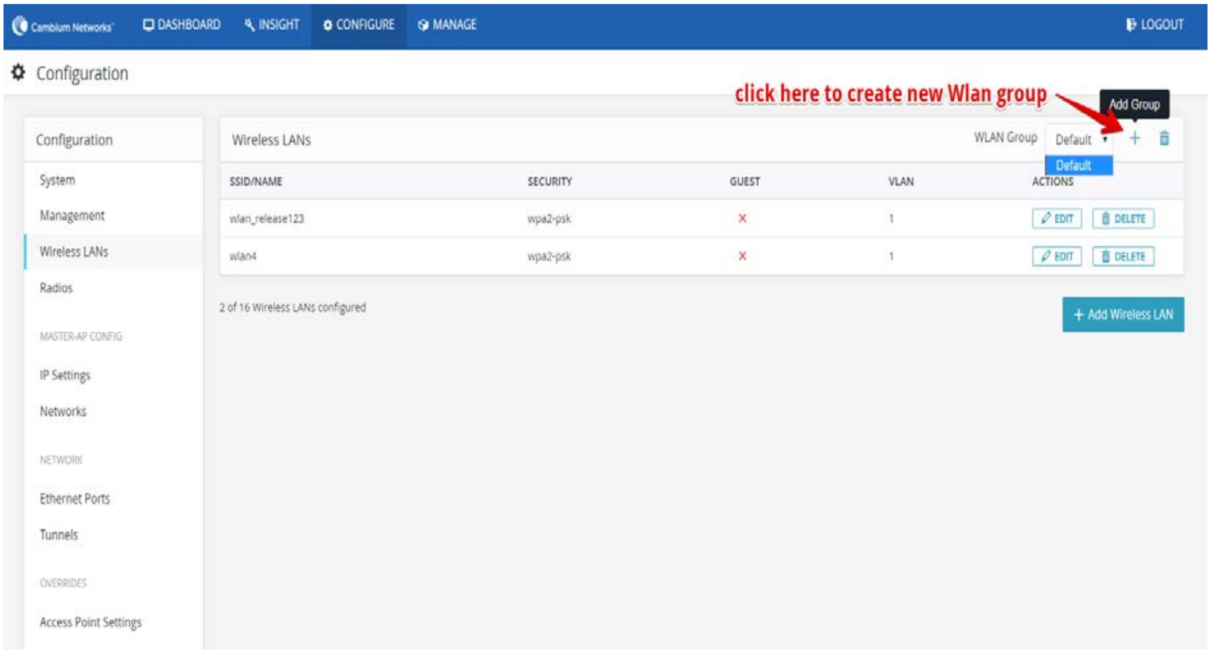
NAME	IP	ACTIONS
E400-B5AD58	10.10.10.169	✓ APPROVE
mesh-client1-E410-93F18A	10.10.10.130	✓ APPROVE
mesh-base1-E410-93F185	10.10.10.137	✓ APPROVE
mesh-client2-E410-93F19F	10.10.10.136	✓ APPROVE

```
AUTOPILOT-AP-CONNECTED: Access Point [E500-917722] MAC    Jun 28, 12:27:35
[00-04-56-91-77-22] connected to Autopilot Master-AP            E500-917722
AUTOPILOT-AP-CONNECTED: Access Point [E400-B5AEFC] MAC    Jun 28, 12:27:29
[00-04-56-B5-AE-FC] connected to Autopilot Master-AP            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

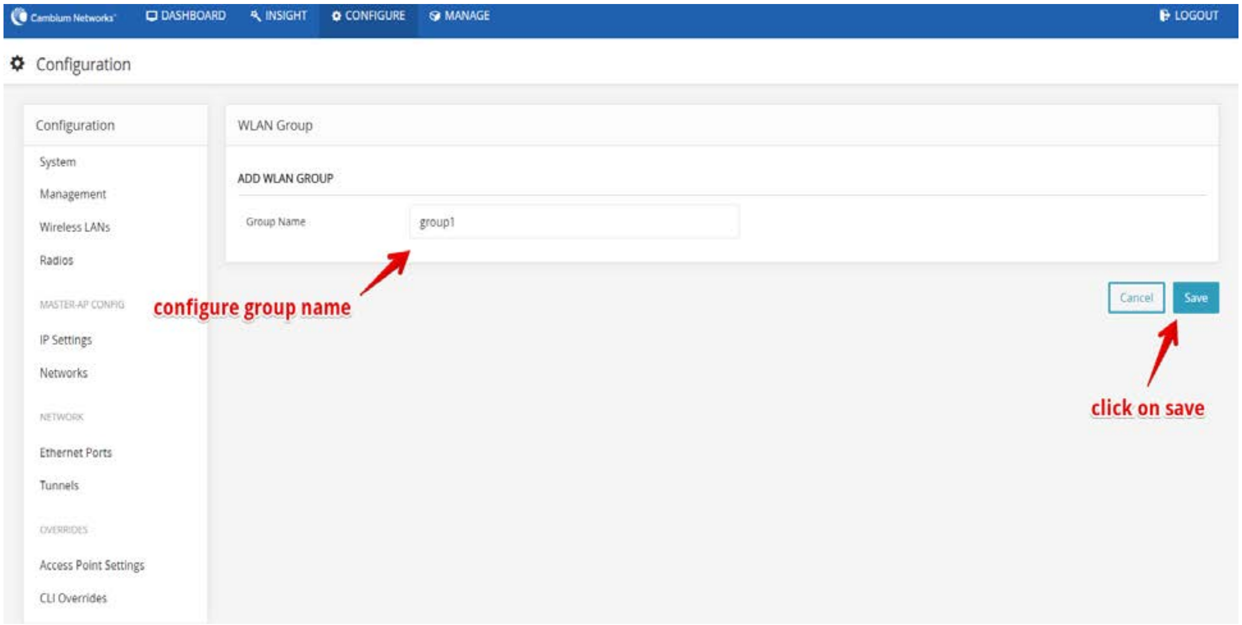


click here to create new Wlan group

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

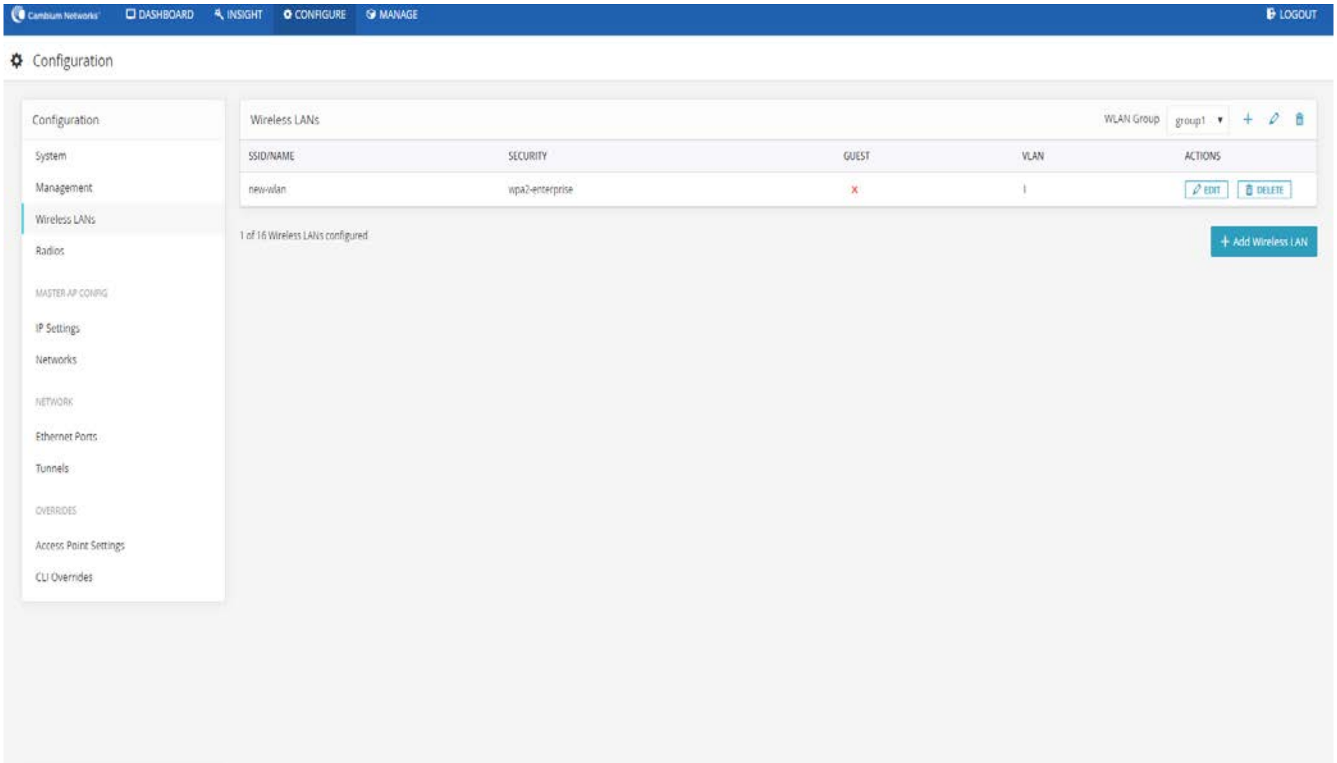


Group Name: group1

configure group name

click on save

3. Configure WLAN under the newly created WLAN-group



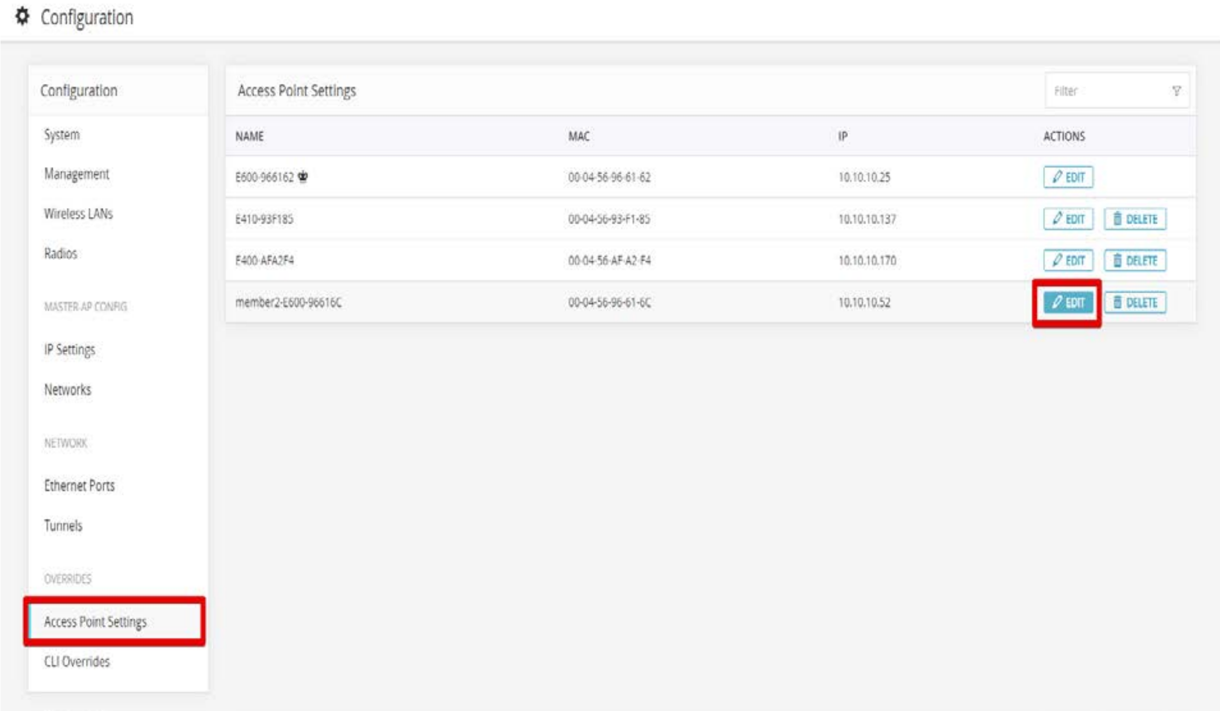
SSID/NAME	SECURITY	GUEST	VLAN	ACTIONS
new-wlan	wpa2-enterprise	×	1	EDIT DELETE

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.

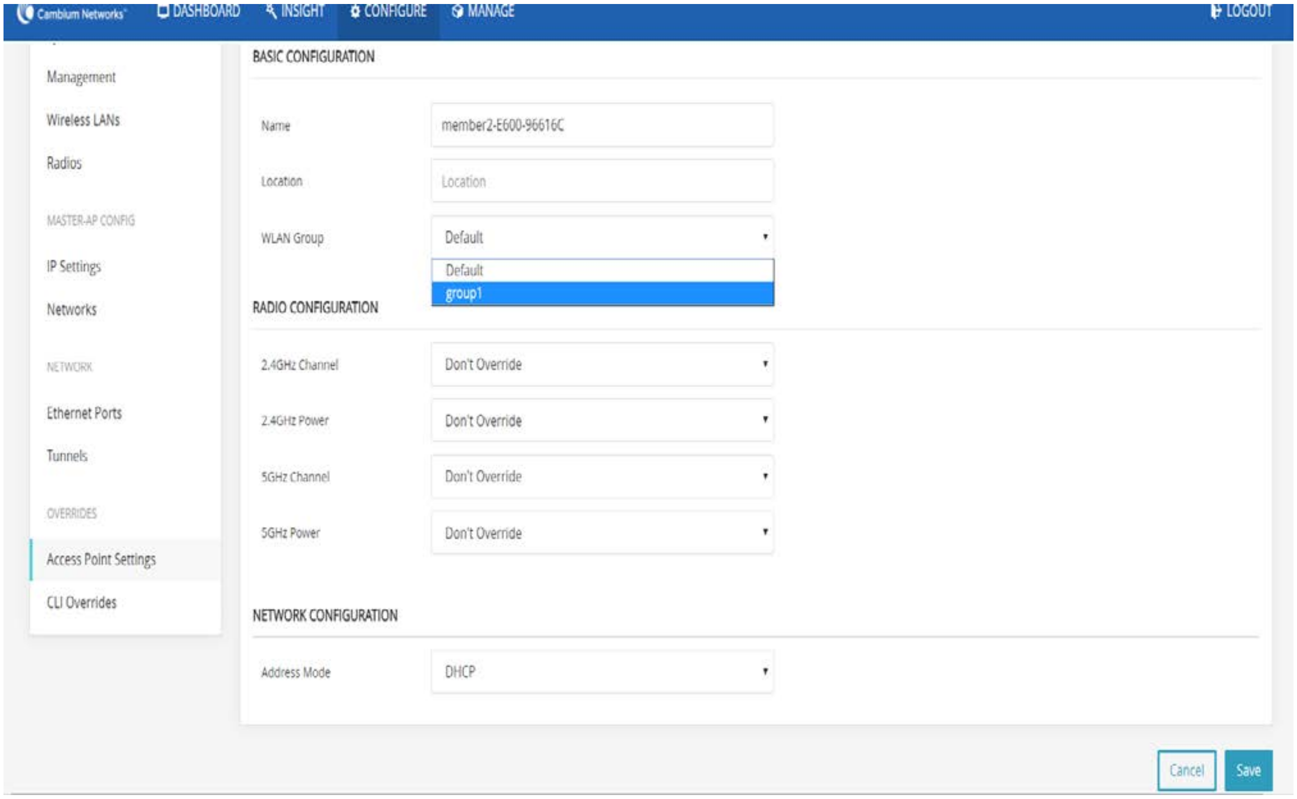
1. Select the device and click **Edit** button.



Access Point Settings

NAME	MAC	IP	ACTIONS
E600-966162 ♛	00-04-56-96-61-62	10.10.10.25	EDIT
E410-93F185	00-04-56-93-F1-85	10.10.10.137	EDIT DELETE
E400-AFA2F4	00-04-56-AF-A2-F4	10.10.10.170	EDIT DELETE
member2-E600-96616C	00-04-56-96-61-6C	10.10.10.52	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.



BASIC CONFIGURATION

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

RADIO CONFIGURATION

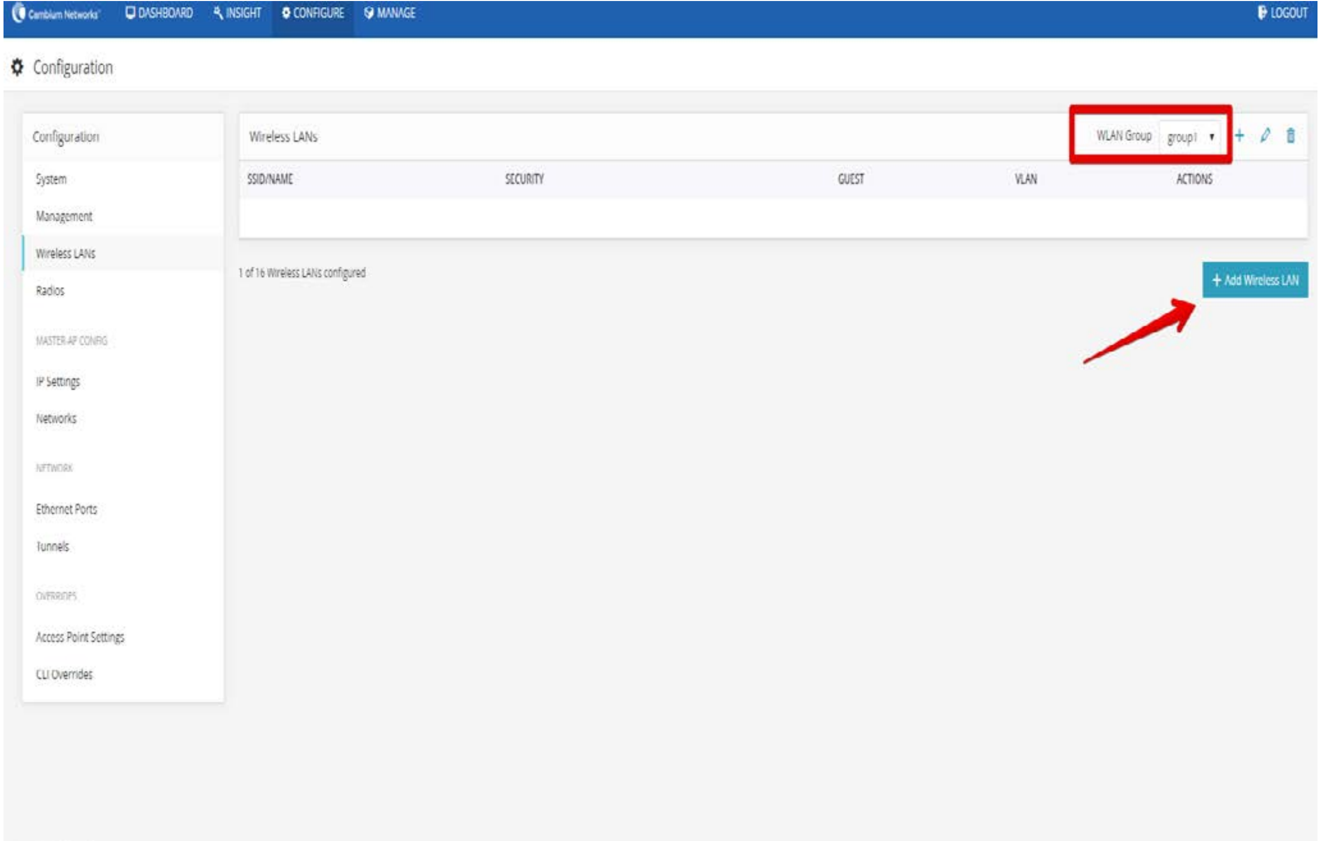
2.4GHz Channel	Don't Override
2.4GHz Power	Don't Override
5GHz Channel	Don't Override
5GHz Power	Don't Override

NETWORK CONFIGURATION

Address Mode	DHCP

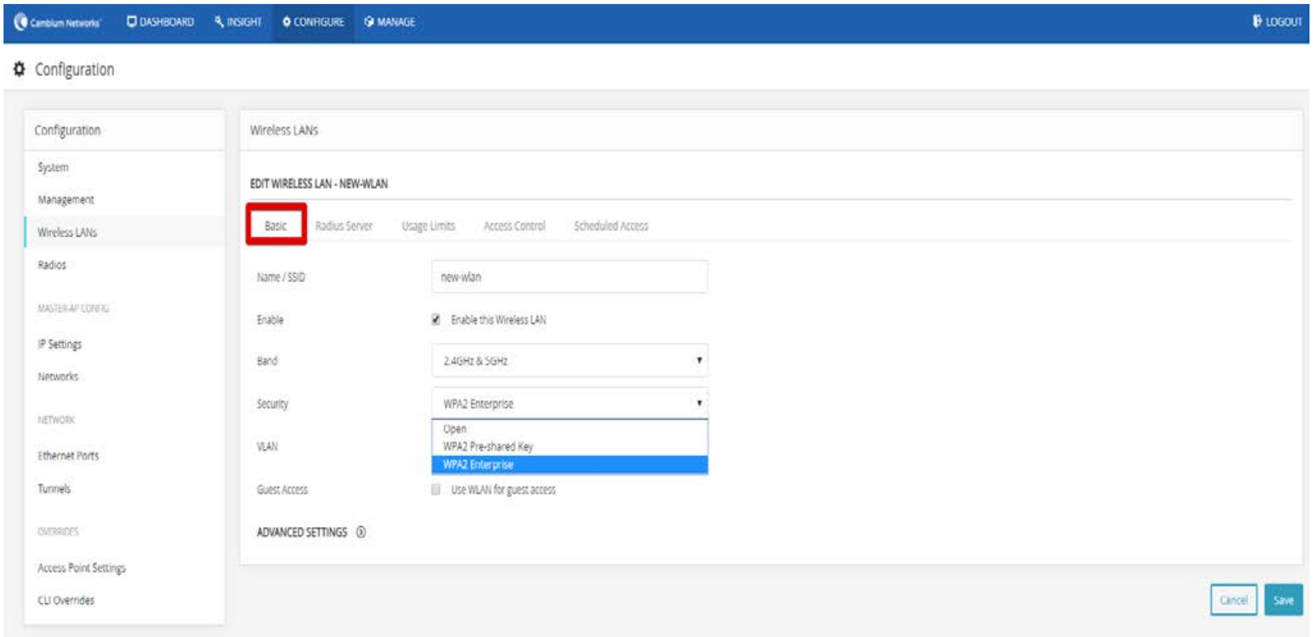
Configuring WPA2-Enterprise WLAN

Follow the below steps to create a WLAN with Enterprise security under **user created Wlan-group**.



1 of 16 Wireless LANs configured

1. Enter details in the WLAN page.
2. Choose security as WPA2-Enterprise.
3. Keep VLAN as 1.
4. Do not press save button before configuring Radius configurations for authentication.



EDIT WIRELESS LAN - NEW-WLAN

Name / SSID: new-wlan

Enable: ☑ Enable this Wireless LAN

Band: 2.4GHz & 5GHz

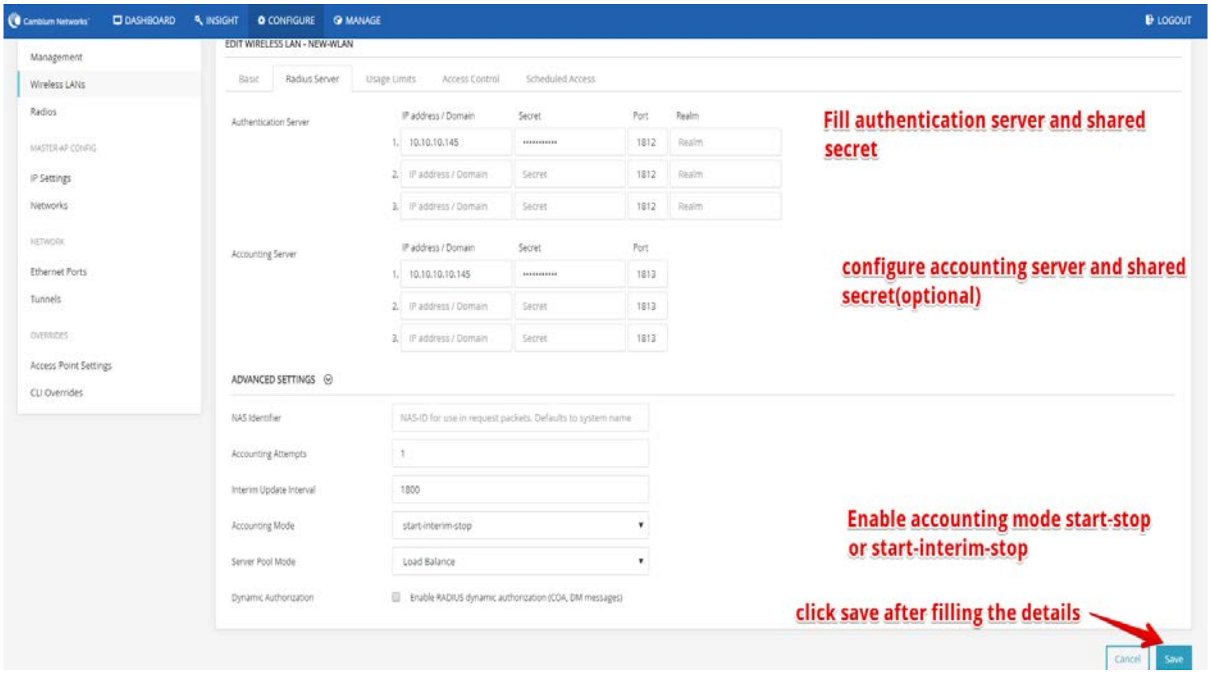
Security: WPA2 Enterprise

VLAN

Guest Access: □ Use WLAN for guest access

ADVANCED SETTINGS

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



EDIT WIRELESS LAN - NEW-WLAN

Authentication Server

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

Fill authentication server and shared secret

Accounting Server

	IP address / Domain	Secret	Port
1.	10.10.10.10.145	•••••••••••	1813
2.	IP address / Domain	Secret	1813
3.	IP address / Domain	Secret	1813

configure accounting server and shared secret(optional)

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)

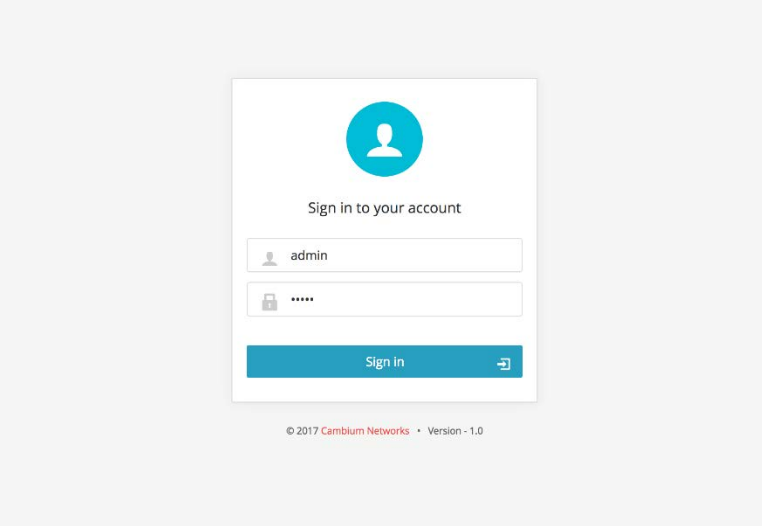
Enable accounting mode start-stop or start-interim-stop

click save after filling the details

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 as **admin** with default password **admin**.



Sign in to your account

admin

•••••

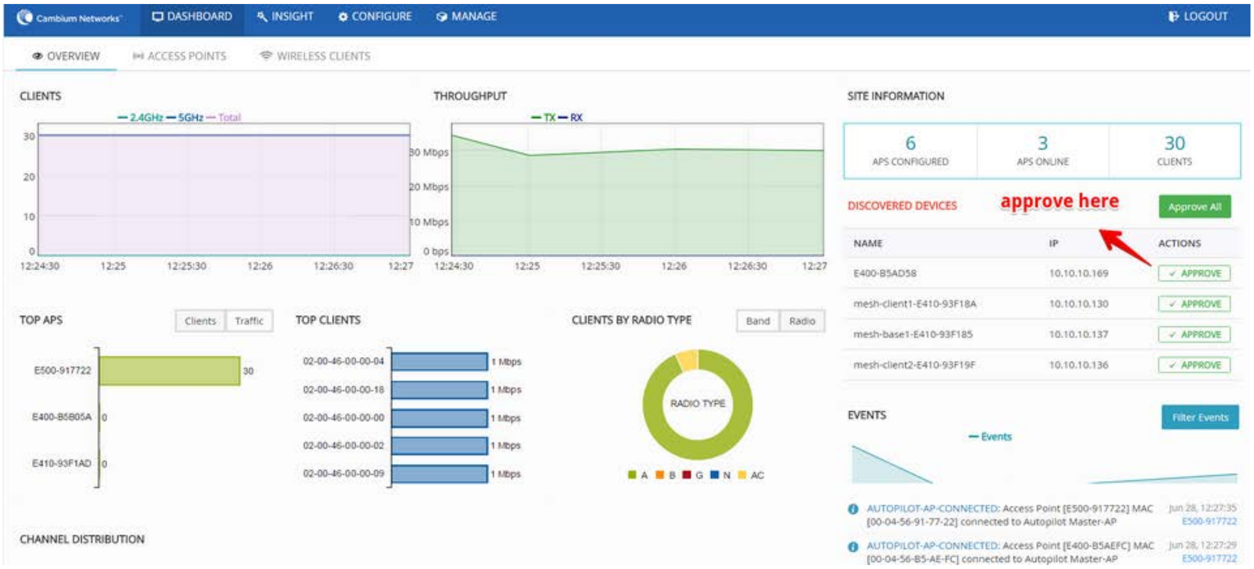
Sign in

© 2017 Cambium Networks • Version - 1.0

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 APs need 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.



SITE INFORMATION

6	3	30
APS CONFIGURED	APS ONLINE	CLIENTS

DISCOVERED DEVICES — Approve All

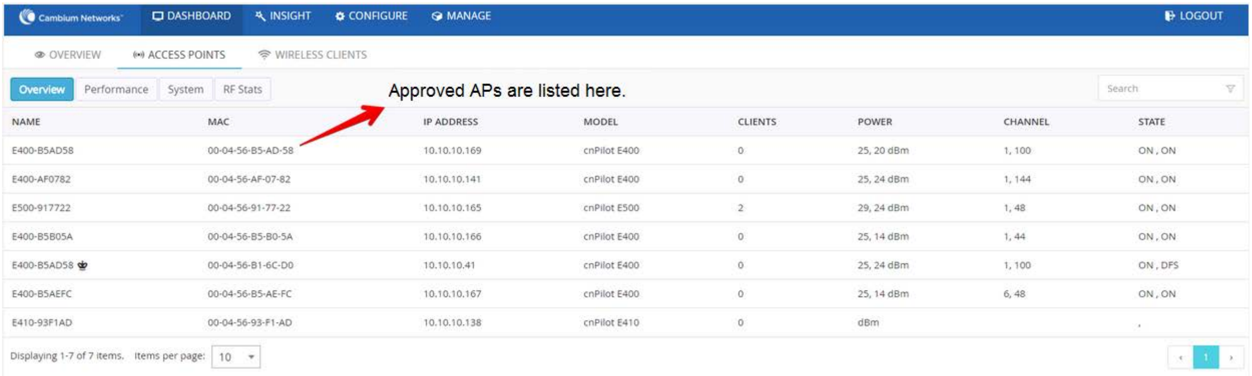
NAME	IP	ACTIONS
E400-B5AD58	10.10.10.169	✓ APPROVE
mesh-client1-E410-93F18A	10.10.10.130	✓ APPROVE
mesh-base1-E410-93F185	10.10.10.137	✓ APPROVE
mesh-client2-E410-93F19F	10.10.10.136	✓ APPROVE

EVENTS

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** tab -> **ACCESS POINTS** tab.



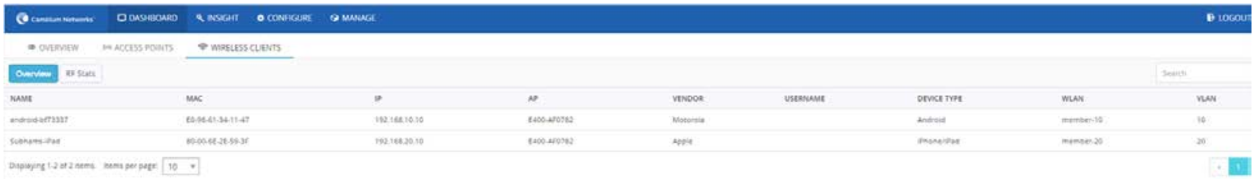
Approved APs are listed here.

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** tab -> **WIRELESS CLIENTS**.
2. Connect the listed clients to the configured WLANS and check statistics

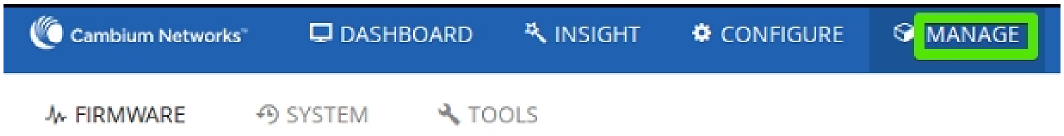


NAME	MAC	IP	AP	VENDOR	USERNAME	DEVICE TYPE	WLAN	VLAN
android-bf73337	E0-98-61-34-11-47	192.168.10.10	E400-AF0782	Motorola		Android	member-10	10
Subhams-iPad	80-00-6E-2E-59-3F	192.168.20.10	E400-AF0782	Apple		iPhone/iPad	member-20	20

Displaying 1-2 of 2 items. Items per page: 10

Manage Autopilot

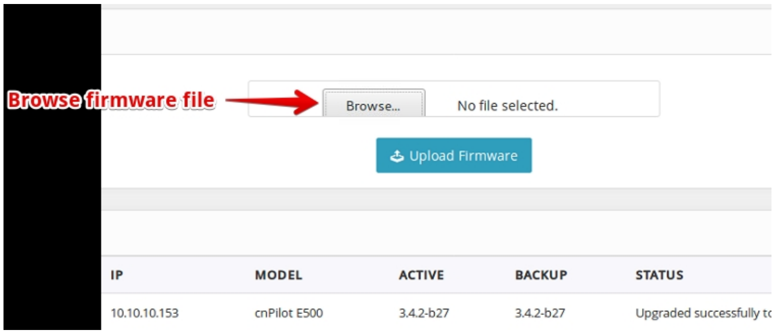
The Manage tab of Autopilot GUI manages firmware upgrades, configuration file updates, and technical assistance of the master and member APs. Data is distributed in sub-sections of Firmware, System, and Tools.



Firmware

Thi ss ection supports uploading required firmware to master AP, and from master AP to the member APs.

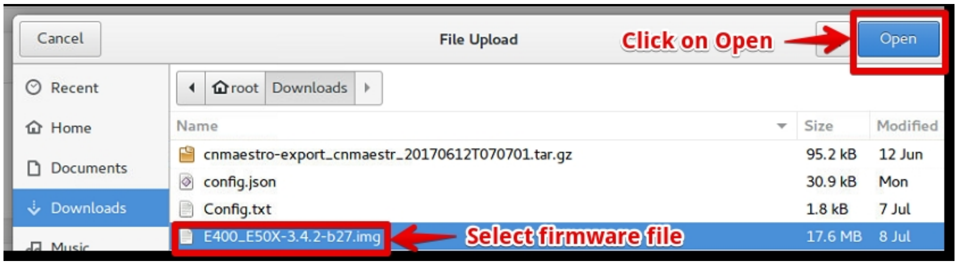
1. Go to **Manage** -> **Firmware** tab.
2. Click the **Browse** button to browse the firmware file.



Browse firmware file

IP	MODEL	ACTIVE	BACKUP	STATUS
10.10.10.153	cnPilot E500	3.4.2-b27	3.4.2-b27	Upgraded successfully to

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

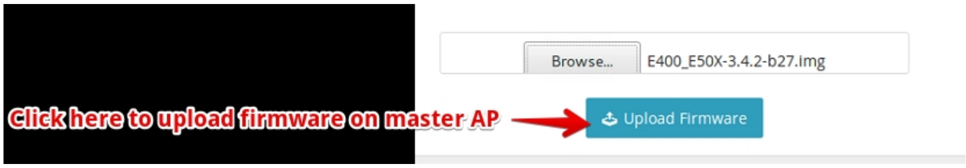


Click on Open

Select firmware file

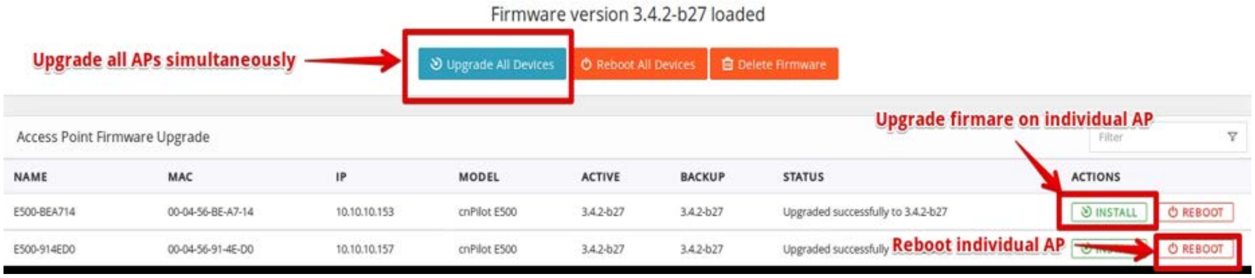
Name	Size	Modified
cnmaestro-export_cnmaestr_20170612T070701.tar.gz	95.2 kB	12 Jun
config.json	30.9 kB	Mon
Config.txt	1.8 kB	7 Jul
E400_E50X-3.4.2-b27.img	17.6 MB	8 Jul

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



Click here to 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.



Firmware version 3.4.2-b27 loaded

Upgrade all APs simultaneously

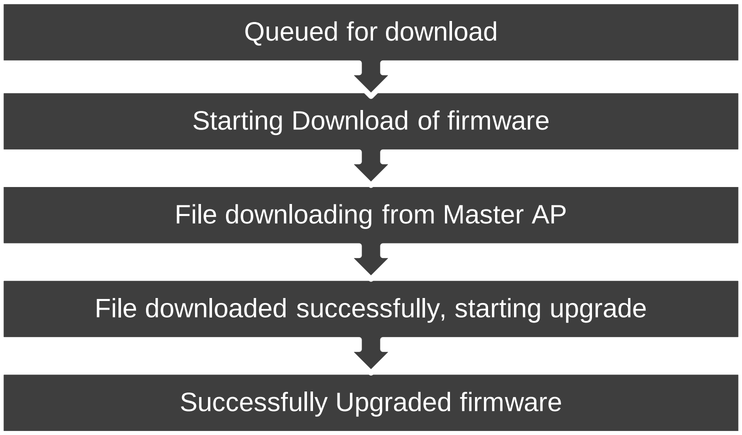
Upgrade firmare on individual AP

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 4 is done, the following statuses during the Firmware upgrade can be seen in sequence:



Queued for download

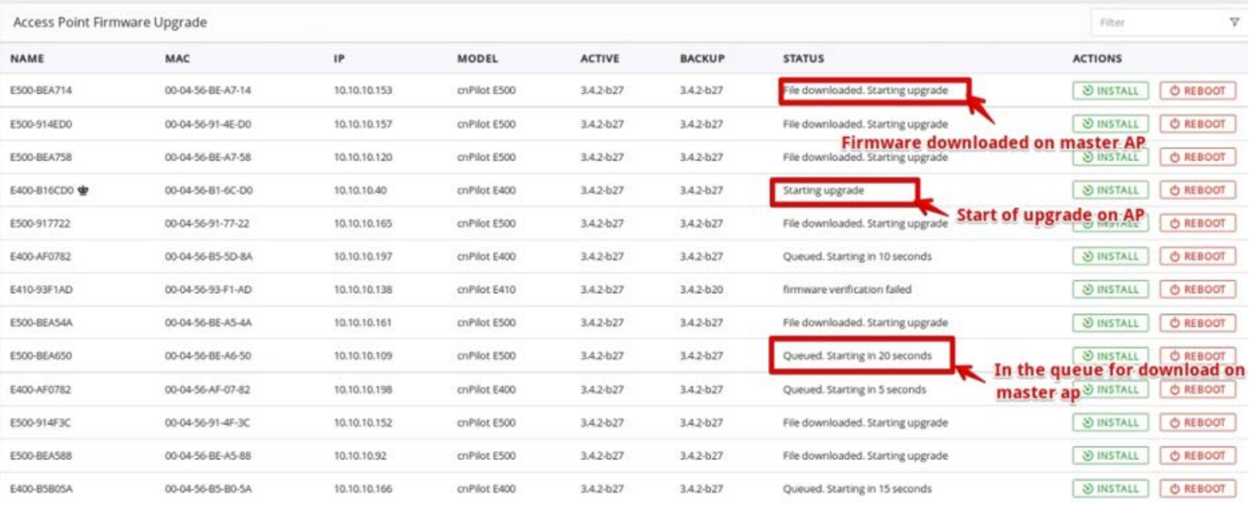
Starting Download of firmware

File downloading from Master AP

File downloaded successfully, starting upgrade

Successfully Upgraded firmware

6. Different statuses of the firmware upgrade can be seen as shown in the following figure



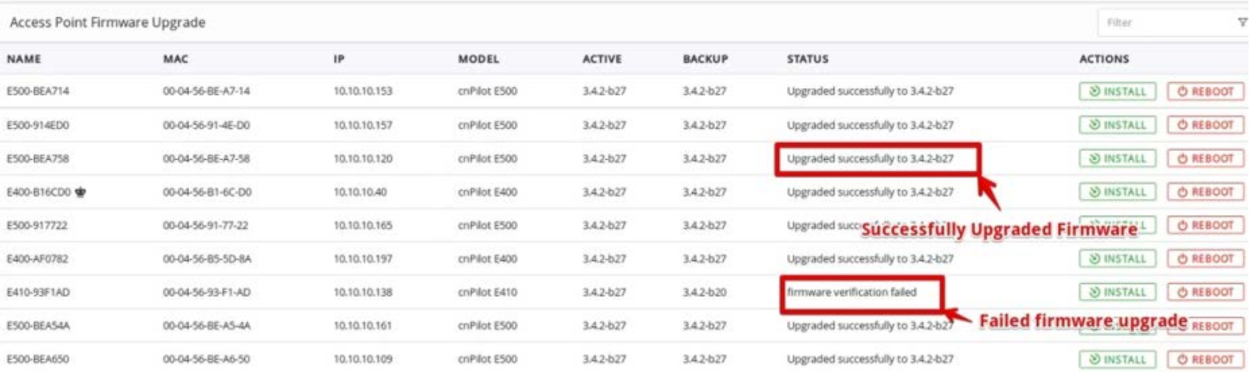
Access Point Firmware Upgrade

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	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

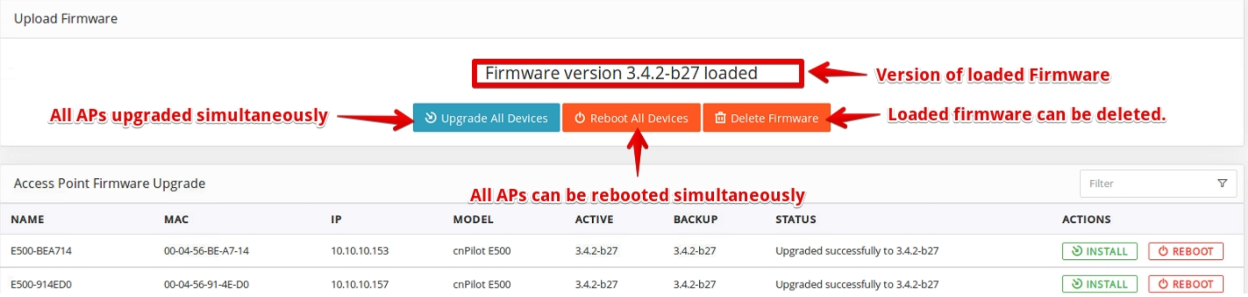
Successfully Upgraded Firmware

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 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


Upload Firmware
Firmware version 3.4.2-b27 loaded
Version of loaded Firmware
All APs upgraded simultaneously
Upgrade All Devices
Reboot All Devices
Delete Firmware
Loaded firmware can be deleted.
All APs can be rebooted simultaneously
Filter

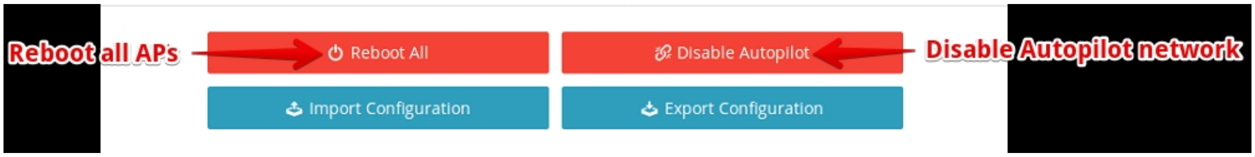
Access Point Firmware Upgrade

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

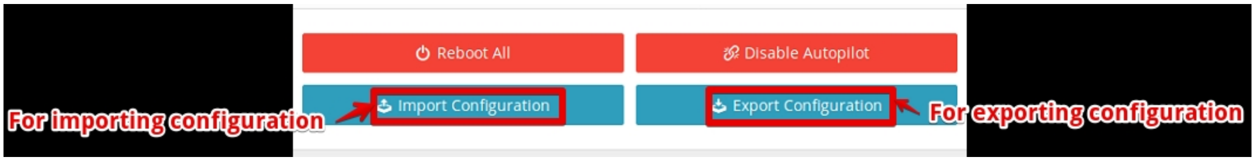
System

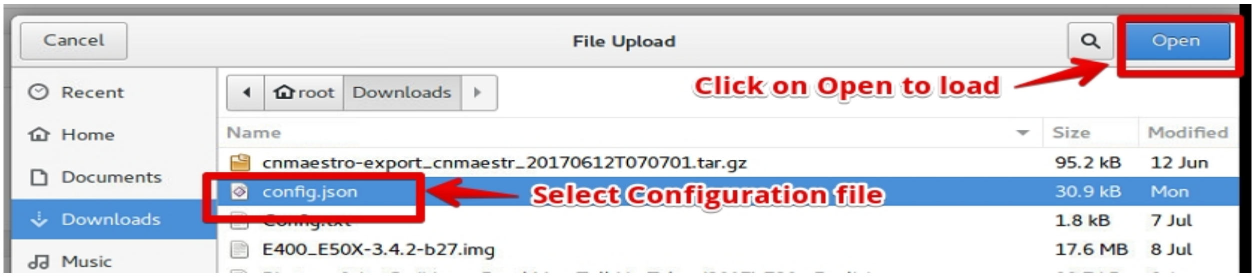
This tab supports following options:

- 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.



- 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.



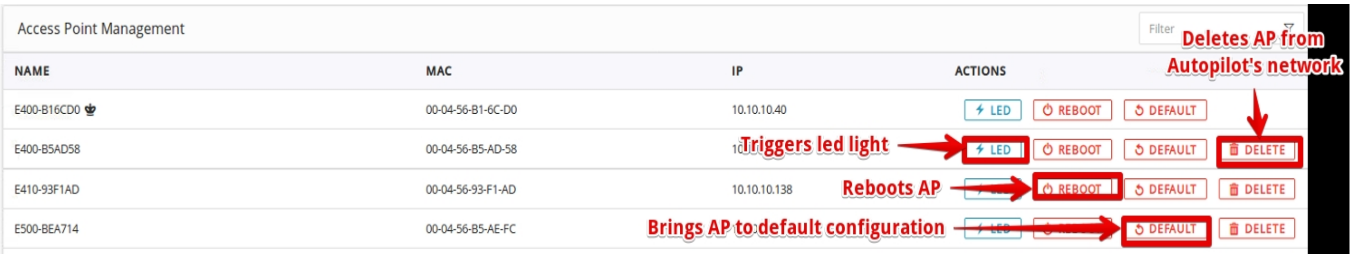


Name	Size	Modified
cnmaestro-export_cnmaestr_20170612T070701.tar.gz	95.2 kB	12 Jun
config.json	30.9 kB	Mon
config.txt	1.8 kB	7 Jul
E400_E50X-3.4.2-b27.img	17.6 MB	8 Jul

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.



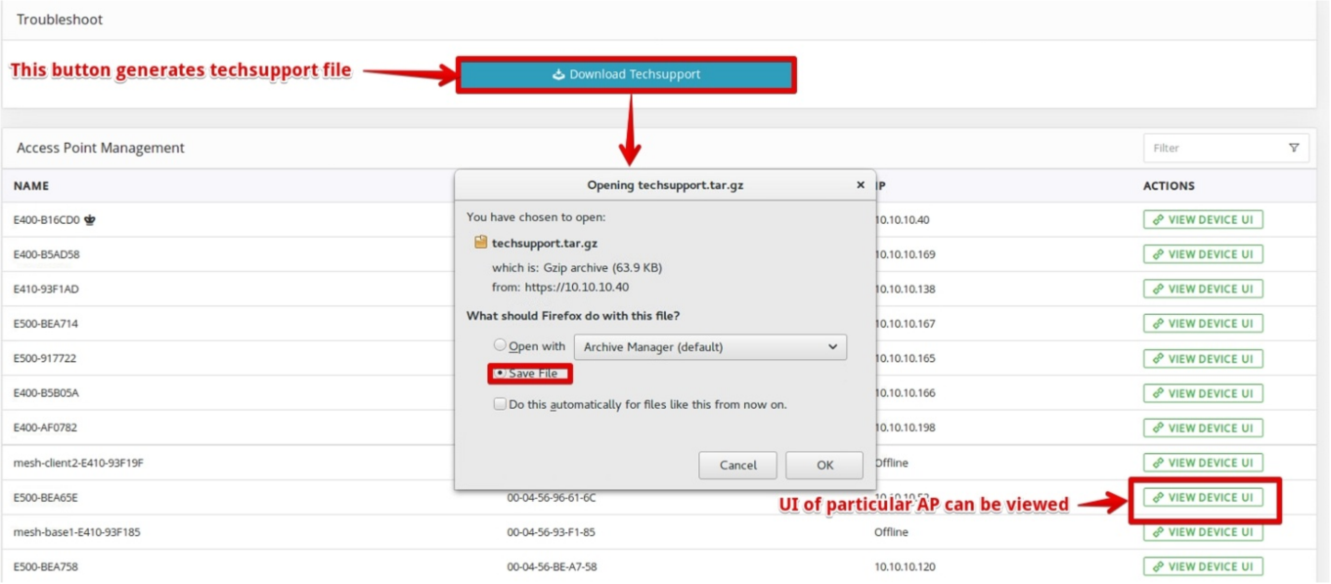
Access Point Management

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	REBOOT DEFAULT DELETE
E500-BEA714	00-04-56-B5-AE-FC		DEFAULT DELETE

Filter
Deletes AP from Autopilot's network
Triggers led light
Reboots AP
Brings AP to default configuration

Troubleshoot

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



Troubleshoot

Access Point Management

NAME	MAC	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

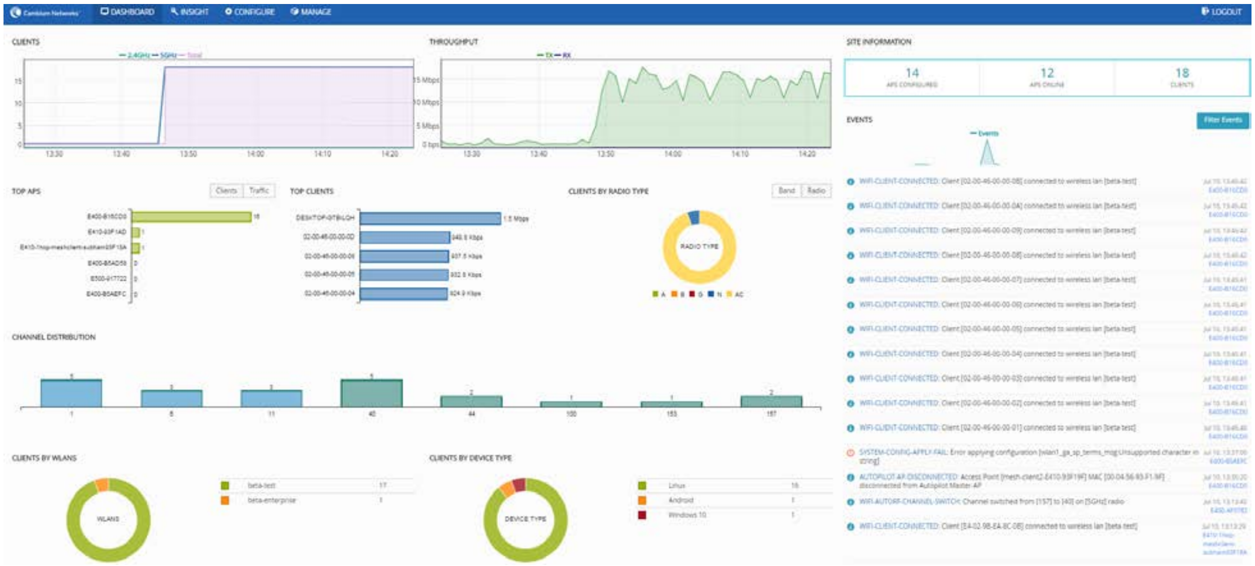
□ Do this automatically for files like this from now on.

This button generates techsupport file
Download Techsupport
Filter
×
Cancel
OK
UI of particular AP can be viewed

Dashboard

The Dashboard of Autopilot GUI 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.



SITE INFORMATION

14 APS CONFIGURED | 12 APS ONLINE | 18 CLIENTS

```
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-08] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-0A] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-09] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-08] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-07] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-06] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-05] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-04] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-03] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-02] connected to wireless lan [beta-test]
WIFI-CLIENT-CONNECTED: Client [02-00-46-00-00-01] connected to wireless lan [beta-test]
SYSTEM-CONFIG-APPLY-FAIL: Error applying configuration [wlan1_ga_sp_terms_msg:Unsupported character in string]
AUTOPILOT-AP-DISCONNECTED: Access Point [mesh-client2-E410-93F19F] MAC [00-04-56-93-F1-9F] disconnected from Autopilot Master AP
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [157] to [40] on [5GHz] radio
WIFI-CLIENT-CONNECTED: Client [E4-02-9B-EA-8C-08] connected to wireless lan [beta-test]
```

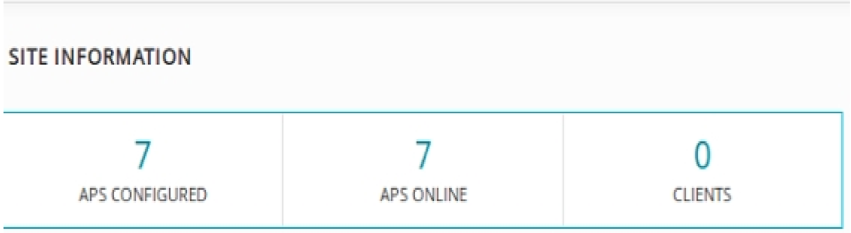
Overview

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

- Site Information
- Discovered Devices
- Events
- Clients
- Throughput
- Top AP
- Top Clients
- Clients by Radio/Band Type
- Channel Distribution
- Clients by WLANS
- Clients by Device Type

SITE INFORMATION

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

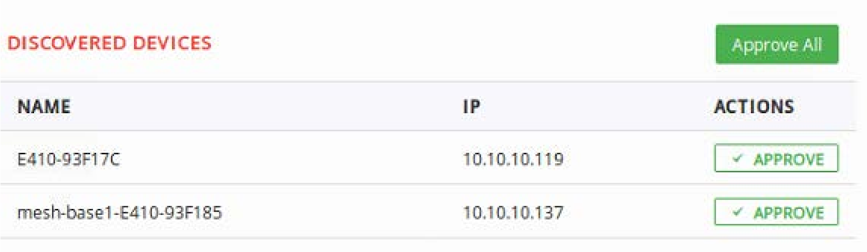


SITE INFORMATION

7 APS CONFIGURED | 7 APS ONLINE | 0 CLIENTS

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.

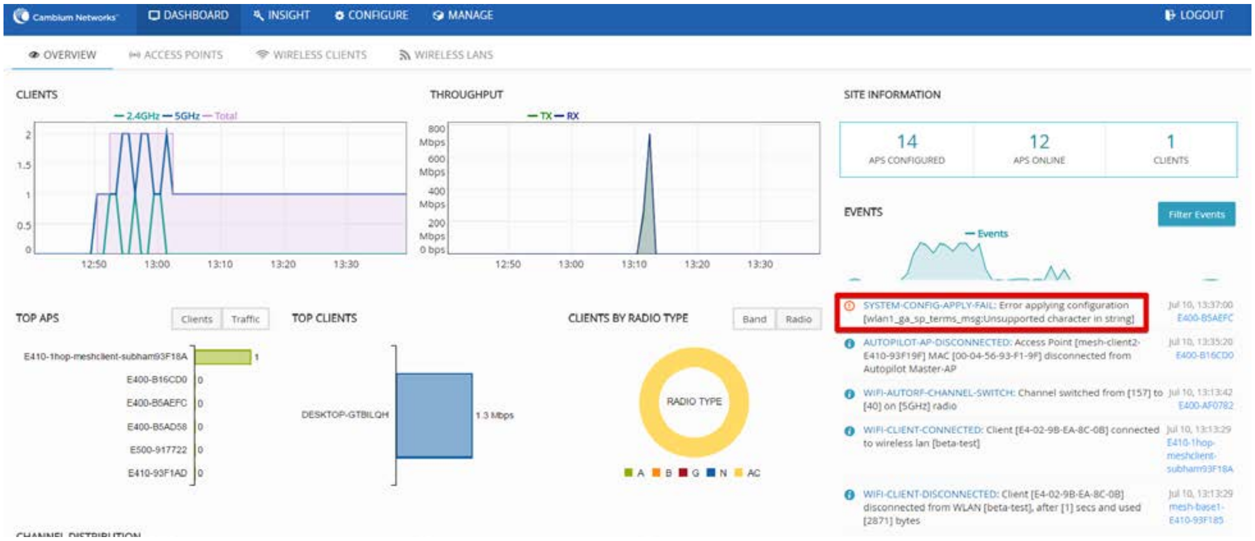


DISCOVERED DEVICES

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.



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

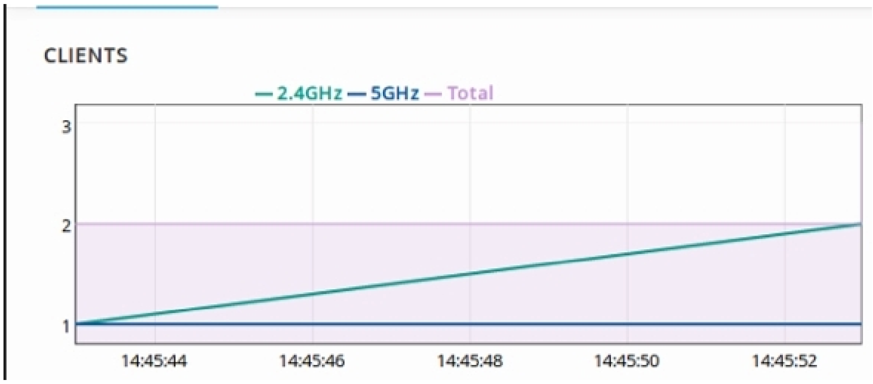
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [157] to [40] on [5GHz] radio — Jul 10, 13:13:42 E400-AF0782

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

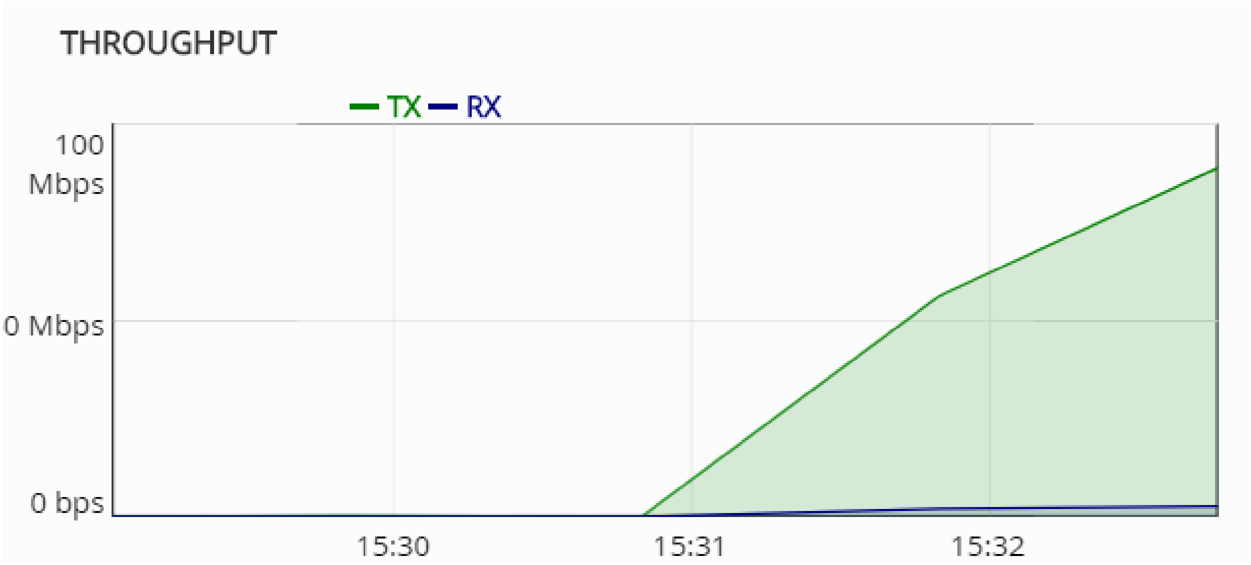
CLIENTS

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.



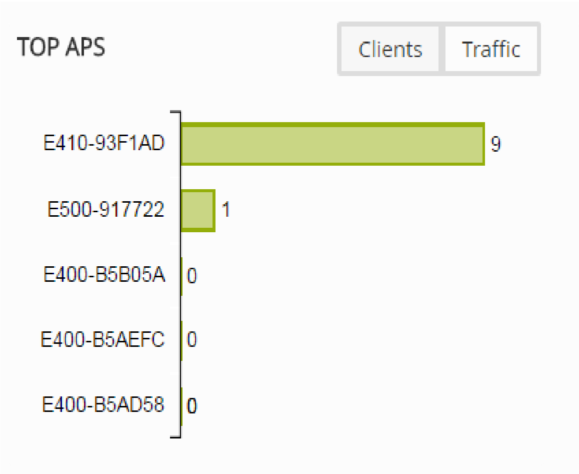
THROUGHPUT

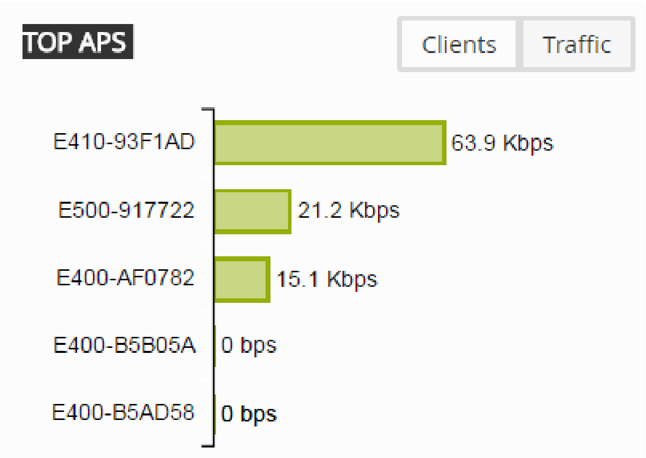
This section graphically represents the TX, RX of each client and total Throughput of all clients against each channel. User can hover over the graph and get more granular details.



TOP APS

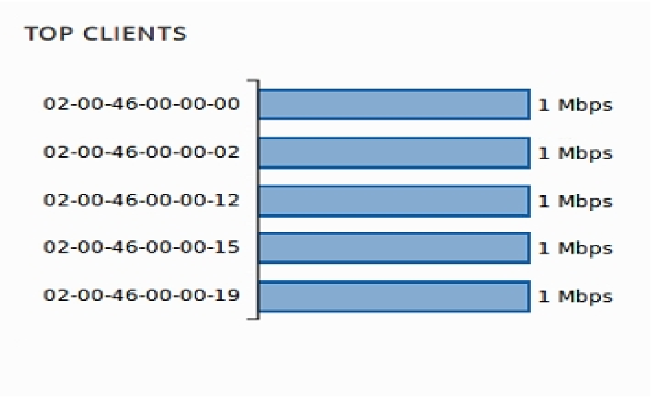
This section graphically displays the top five APs connected to Autopilot's network along with numbers of clients and traffic in respective frequencies (2.4hz or 5hz).


TOP APS
Clients
Traffic
E410-93F1AD
9
E500-917722
1
E400-B5B05A
0
E400-B5AEFC
0
E400-B5AD58
0


TOP APS
Clients
Traffic
E410-93F1AD
63.9 Kbps
E500-917722
21.2 Kbps
E400-AF0782
15.1 Kbps
E400-B5B05A
0 bps
E400-B5AD58
0 bps

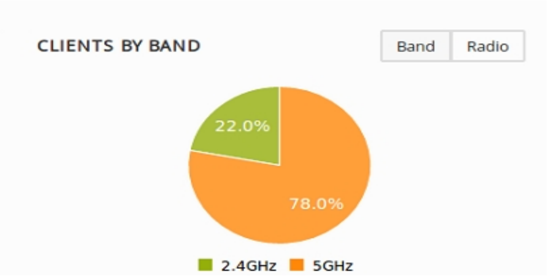
TOP CLIENTS

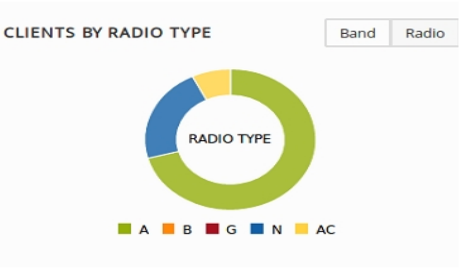
This section graphically represents the top five clients connected to APs with highest traffic flow.



CLIENTS BY RADIO/BAND TYPE

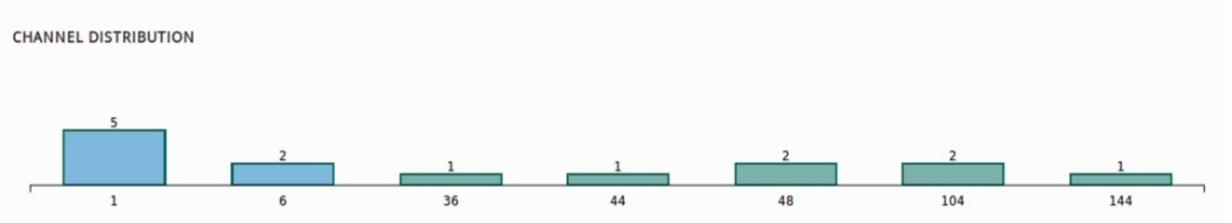
This section provides pie chart representation of the radio types of Clients. This shows pie chart based on the percentage of 2.4 GHz and 5 GHz clients connected to Autopilot network. Another pie chart is plotted based on types of clients such as 802.11a, 802.11b/g/n, 802.11ac.





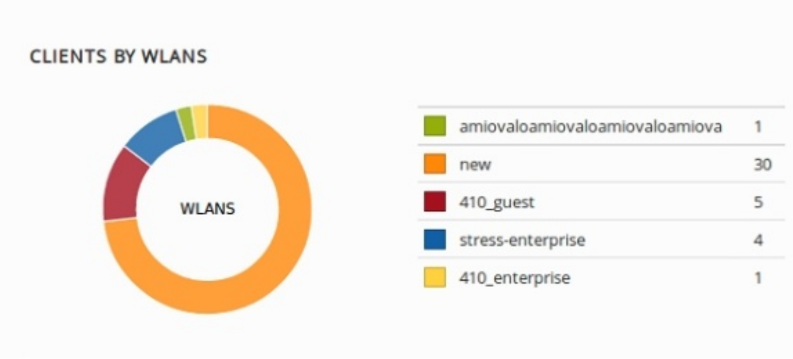
CHANNEL DISTRIBUTION

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



CLIENTS BY WLANS

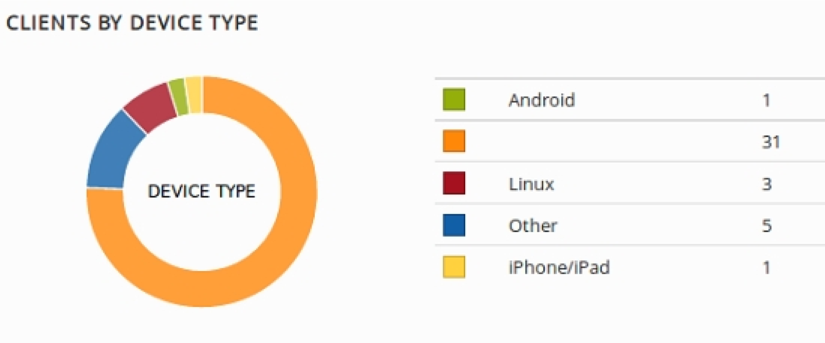
This section provides a pie chart representation of all the Clients and WLANs. This helps to instantly know the load on the WLANs.



🟩	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.



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

Access Points

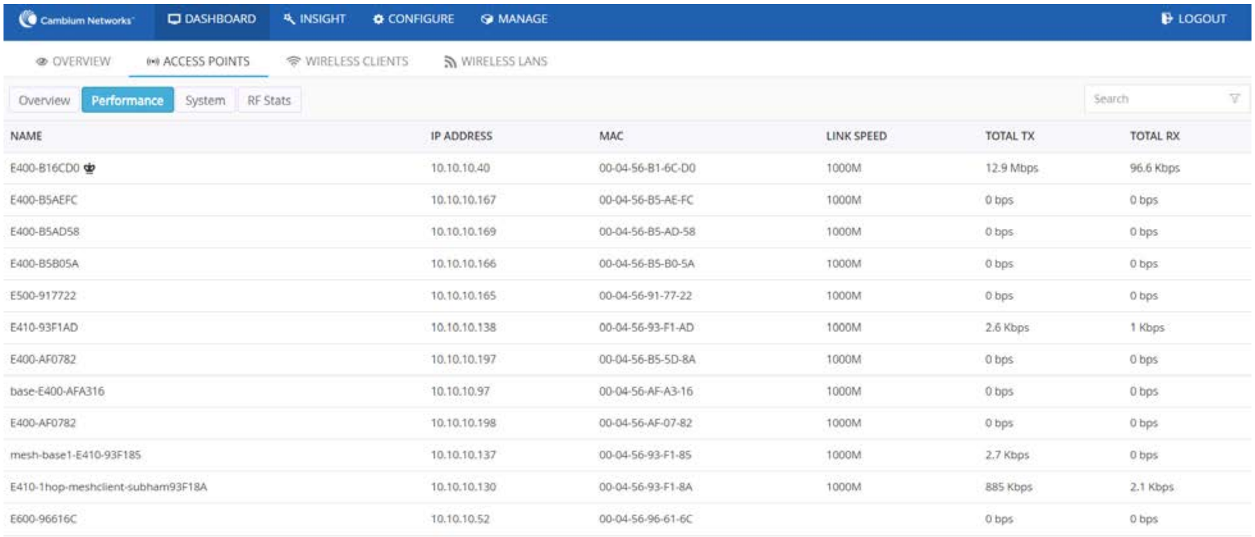
This tab contains details such as Performance, System details, Client details, and so on of all the APs connected to Autopilot. Under Access Point tab, there are four tabs which are as follows:

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

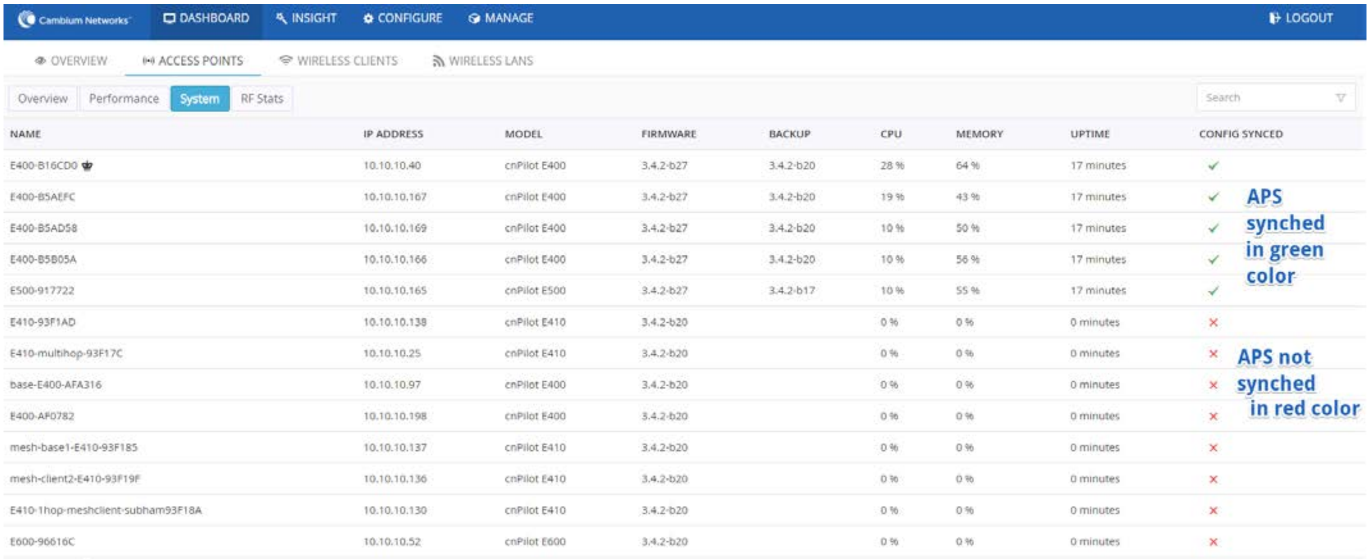
This tab displays MAC, IP, Link speed, Total TX (Transmit from APS), and Total RX (Received to APS).
For example, if AP transmits data at the speed of 10mbps, then its TX is equal to 10mbps.



NAME	IP ADDRESS	MAC	LINK SPEED	TOTAL TX	TOTAL RX
E400-B16CD0 ♛	10.10.10.40	00-04-56-B1-6C-D0	1000M	12.9 Mbps	96.6 Kbps
E400-B5AEFC	10.10.10.167	00-04-56-B5-AE-FC	1000M	0 bps	0 bps
E400-B5AD58	10.10.10.169	00-04-56-B5-AD-58	1000M	0 bps	0 bps
E400-B5B05A	10.10.10.166	00-04-56-B5-B0-5A	1000M	0 bps	0 bps
E500-917722	10.10.10.165	00-04-56-91-77-22	1000M	0 bps	0 bps
E410-93F1AD	10.10.10.138	00-04-56-93-F1-AD	1000M	2.6 Kbps	1 Kbps
E400-AF0782	10.10.10.197	00-04-56-B5-5D-8A	1000M	0 bps	0 bps
base-E400-AFA316	10.10.10.97	00-04-56-AF-A3-16	1000M	0 bps	0 bps
E400-AF0782	10.10.10.198	00-04-56-AF-07-82	1000M	0 bps	0 bps
mesh-base1-E410-93F185	10.10.10.137	00-04-56-93-F1-85	1000M	2.7 Kbps	0 bps
E410-1hop-meshclient-subham93F18A	10.10.10.130	00-04-56-93-F1-8A	1000M	885 Kbps	2.1 Kbps
E600-96616C	10.10.10.52	00-04-56-96-61-6C		0 bps	0 bps

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 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 the following figure.



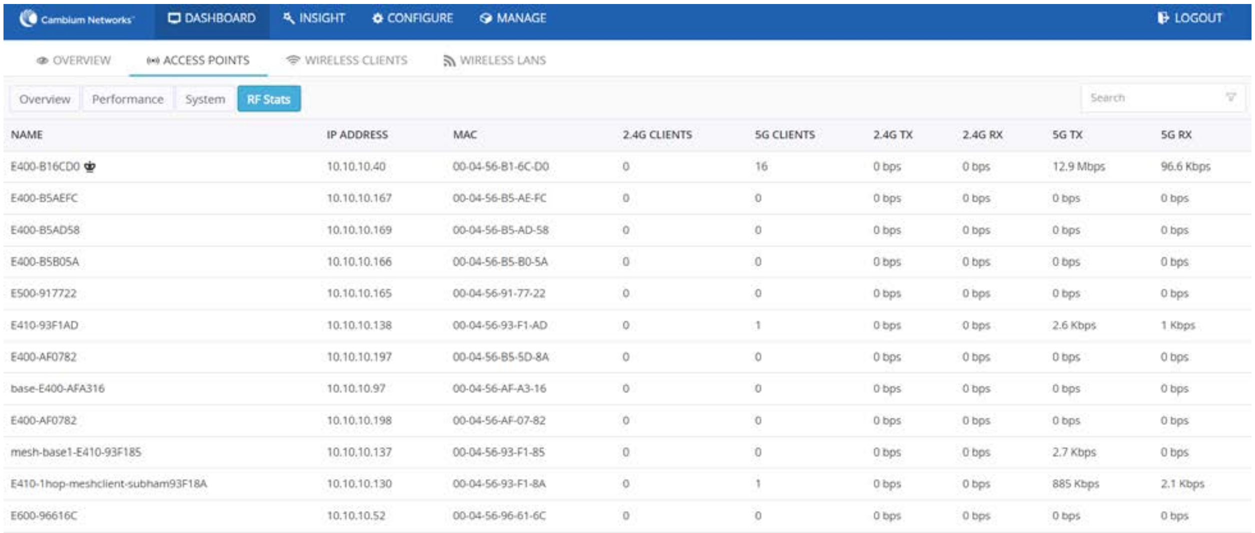
NAME	IP ADDRESS	MODEL	FIRMWARE	BACKUP	CPU	MEMORY	UPTIME	CONFIG SYNCED
E400-B16CD0 ♛	10.10.10.40	cnPilot E400	3.4.2-b27	3.4.2-b20	28 %	64 %	17 minutes	✓
E400-B5AEFC	10.10.10.167	cnPilot E400	3.4.2-b27	3.4.2-b20	19 %	43 %	17 minutes	✓
E400-B5AD58	10.10.10.169	cnPilot E400	3.4.2-b27	3.4.2-b20	10 %	50 %	17 minutes	✓
E400-B5B05A	10.10.10.166	cnPilot E400	3.4.2-b27	3.4.2-b20	10 %	56 %	17 minutes	✓
E500-917722	10.10.10.165	cnPilot E500	3.4.2-b27	3.4.2-b17	10 %	55 %	17 minutes	✓
E410-93F1AD	10.10.10.138	cnPilot E410	3.4.2-b20		0 %	0 %	0 minutes	✗
E410-multihop-93F17C	10.10.10.25	cnPilot E410	3.4.2-b20		0 %	0 %	0 minutes	✗
base-E400-AFA316	10.10.10.97	cnPilot E400	3.4.2-b20		0 %	0 %	0 minutes	✗
E400-AF0782	10.10.10.198	cnPilot E400	3.4.2-b20		0 %	0 %	0 minutes	✗
mesh-base1-E410-93F185	10.10.10.137	cnPilot E410	3.4.2-b20		0 %	0 %	0 minutes	✗
mesh-client2-E410-93F19F	10.10.10.136	cnPilot E410	3.4.2-b20		0 %	0 %	0 minutes	✗
E410-1hop-meshclient-subham93F18A	10.10.10.130	cnPilot E410	3.4.2-b20		0 %	0 %	0 minutes	✗
E600-96616C	10.10.10.52	cnPilot E600	3.4.2-b20		0 %	0 %	0 minutes	✗

APS synched in green color

APS not synched in red color

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.



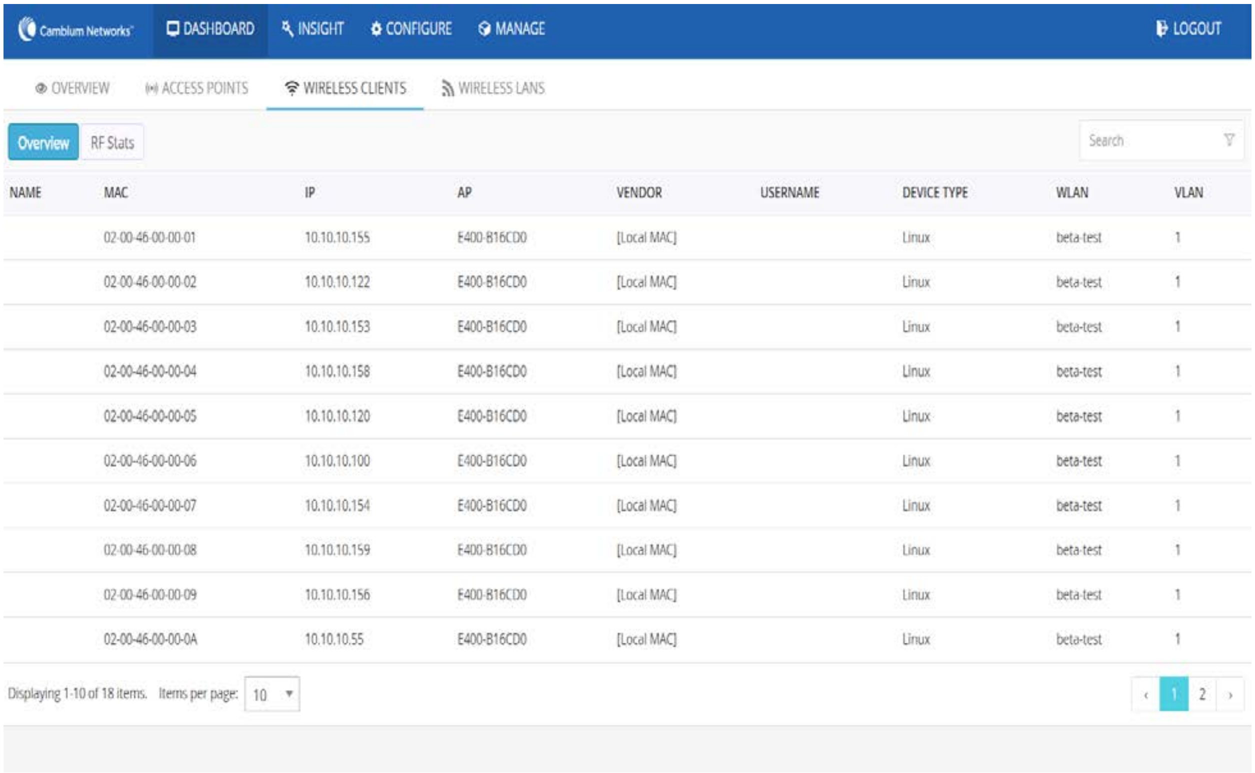
NAME	IP ADDRESS	MAC	2.4G CLIENTS	5G CLIENTS	2.4G TX	2.4G RX	5G TX	5G RX
E400-B16CD0 ♚	10.10.10.40	00-04-56-B1-6C-D0	0	16	0 bps	0 bps	12.9 Mbps	96.6 Kbps
E400-B5AEFC	10.10.10.167	00-04-56-B5-AE-FC	0	0	0 bps	0 bps	0 bps	0 bps
E400-B5AD58	10.10.10.169	00-04-56-B5-AD-58	0	0	0 bps	0 bps	0 bps	0 bps
E400-B5B05A	10.10.10.166	00-04-56-B5-B0-5A	0	0	0 bps	0 bps	0 bps	0 bps
E500-917722	10.10.10.165	00-04-56-91-77-22	0	0	0 bps	0 bps	0 bps	0 bps
E410-93F1AD	10.10.10.138	00-04-56-93-F1-AD	0	1	0 bps	0 bps	2.6 Kbps	1 Kbps
E400-AF0782	10.10.10.197	00-04-56-B5-5D-8A	0	0	0 bps	0 bps	0 bps	0 bps
base-E400-AFA316	10.10.10.97	00-04-56-AF-A3-16	0	0	0 bps	0 bps	0 bps	0 bps
E400-AF0782	10.10.10.198	00-04-56-AF-07-82	0	0	0 bps	0 bps	0 bps	0 bps
mesh-base1-E410-93F185	10.10.10.137	00-04-56-93-F1-85	0	0	0 bps	0 bps	2.7 Kbps	0 bps
E410-1hop-meshclient-subham93F18A	10.10.10.130	00-04-56-93-F1-8A	0	1	0 bps	0 bps	885 Kbps	2.1 Kbps
E600-96616C	10.10.10.52	00-04-56-96-61-6C	0	0	0 bps	0 bps	0 bps	0 bps

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.



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

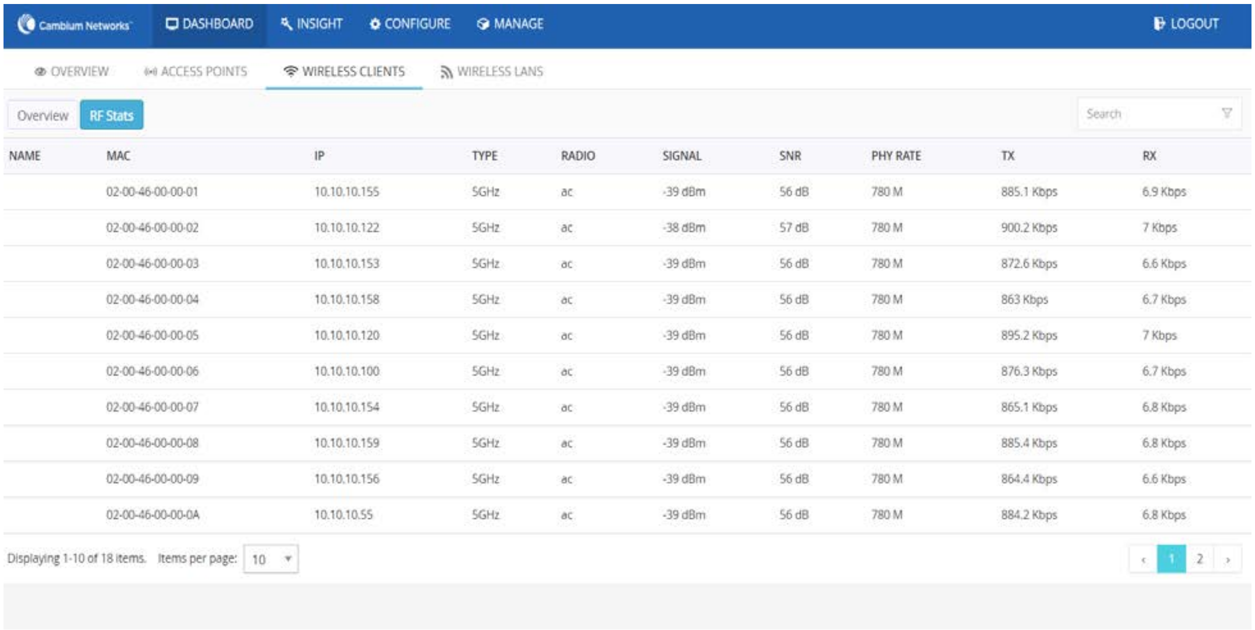
‹ 1 2 ›

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.



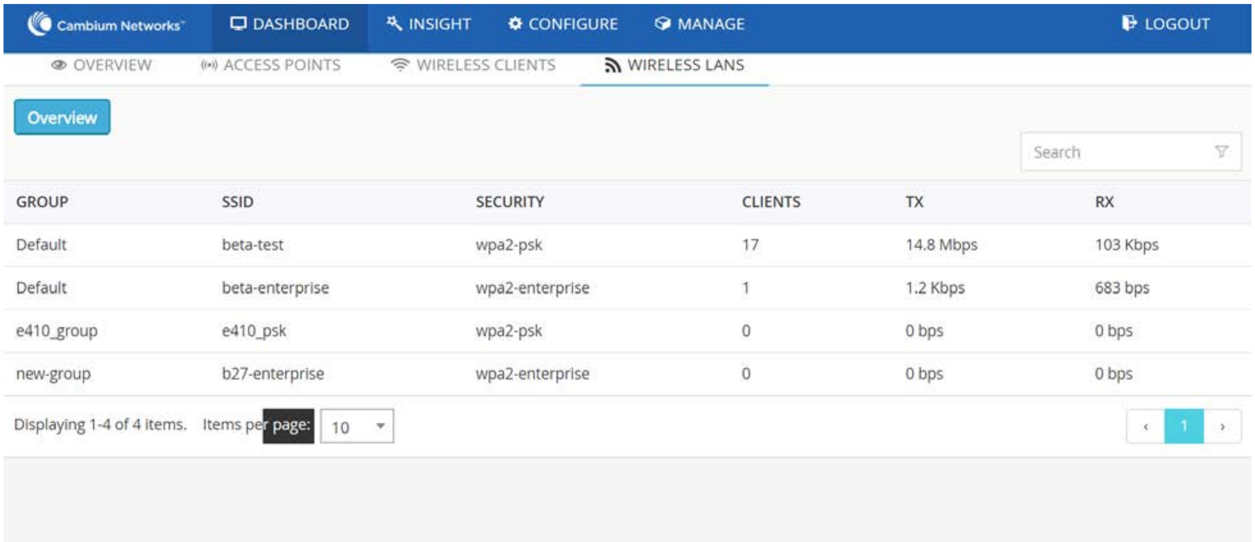
NAME	MAC	IP	TYPE	RADIO	SIGNAL	SNR	PHY RATE	TX	RX
	02-00-46-00-00-01	10.10.10.155	5GHz	ac	-39 dBm	56 dB	780 M	885.1 Kbps	6.9 Kbps
	02-00-46-00-00-02	10.10.10.122	5GHz	ac	-38 dBm	57 dB	780 M	900.2 Kbps	7 Kbps
	02-00-46-00-00-03	10.10.10.153	5GHz	ac	-39 dBm	56 dB	780 M	872.6 Kbps	6.6 Kbps
	02-00-46-00-00-04	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.



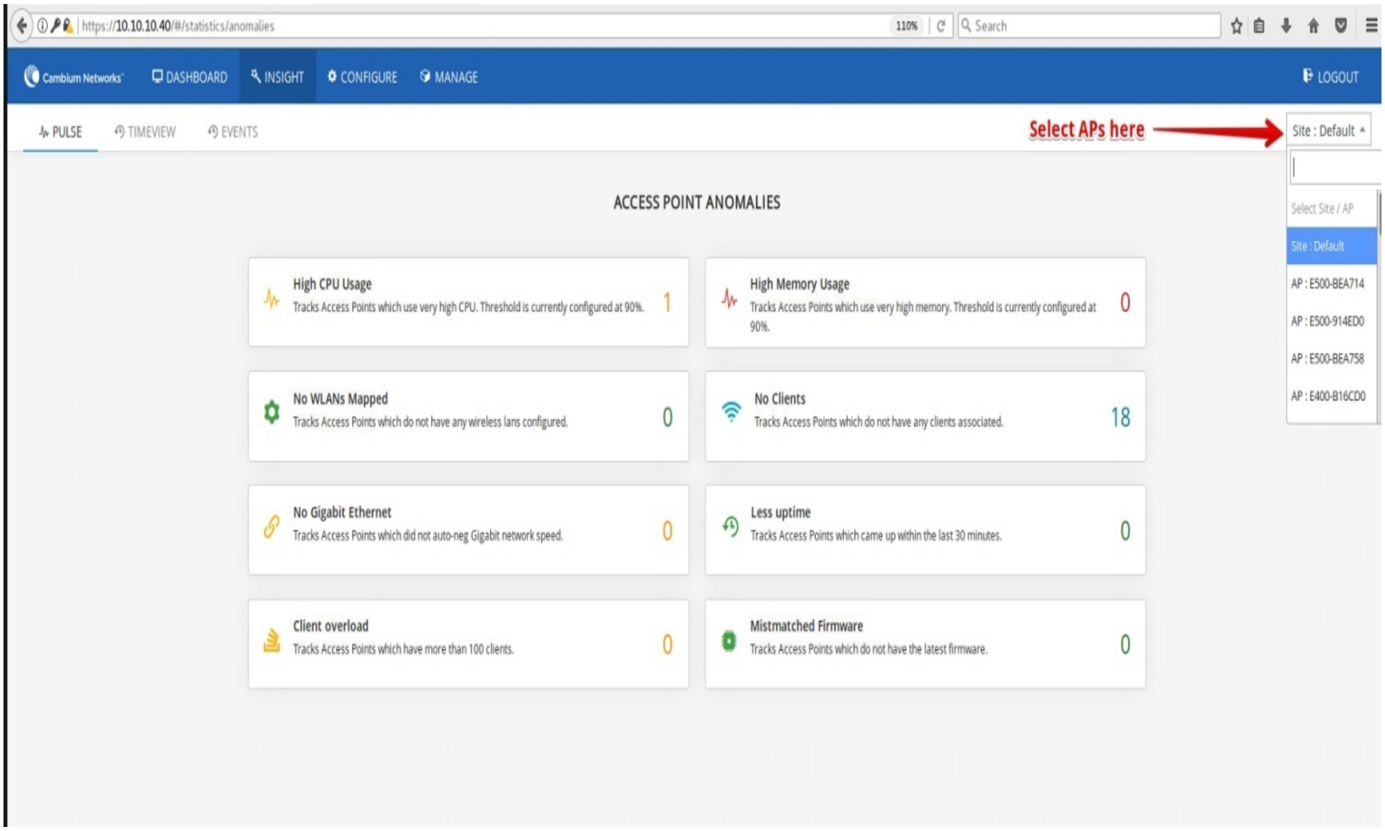
GROUP	SSID	SECURITY	CLIENTS	TX	RX
Default	beta-test	wpa2-psk	17	14.8 Mbps	103 Kbps
Default	beta-enterprise	wpa2-enterprise	1	1.2 Kbps	683 bps
e410_group	e410_psk	wpa2-psk	0	0 bps	0 bps
new-group	b27-enterprise	wpa2-enterprise	0	0 bps	0 bps

Displaying 1-4 of 4 items. Items per page: 10

Insight

Insight option of Autopilot UI provides accurate insights on an AP anomalies which are distributed on the sub tabs namely Pulse, TimeView and Events.

On the top left corner of the page the master and the member APs can be selected from the dropdown menu. Site default gives overall details.



ACCESS POINT ANOMALIES

High CPU Usage
Tracks Access Points which use very high CPU. Threshold is currently configured at 90%. 1

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. 18

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:

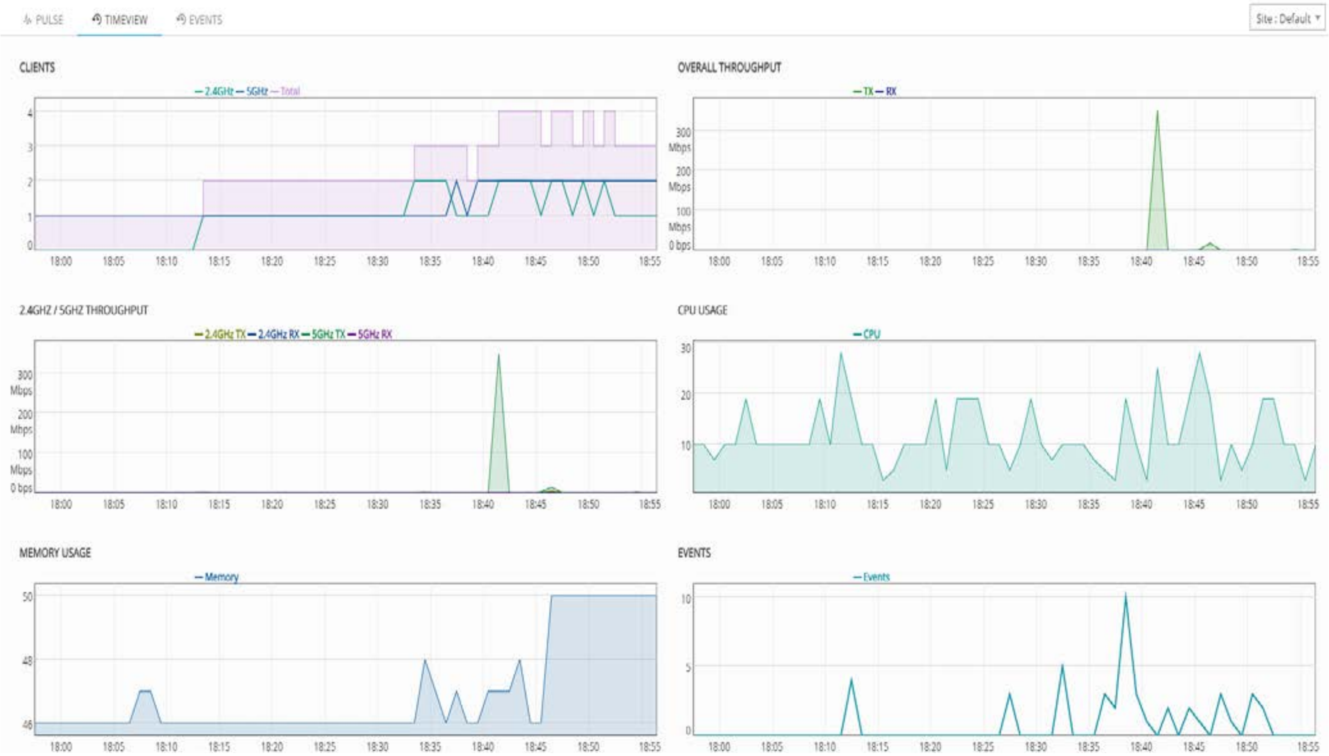
- **High CPU Usage**: On clicking, this option leads to Time View page of Insight tab and tracks the CPU usage of all APs graphically.
- **No WLANs Mapped**: This option leads to AccessPoints page of Dashboard tab and tracks number of APs without wireless LANs configured.
- **No Gigabit Ethernet**: This option leads to AccessPoints page of Dashboard tab and tracks APs which do not auto negotiate gigabit network speed.
- **Client Overload**: This option leads to AccessPoint 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 AccessPoints 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:**

Note

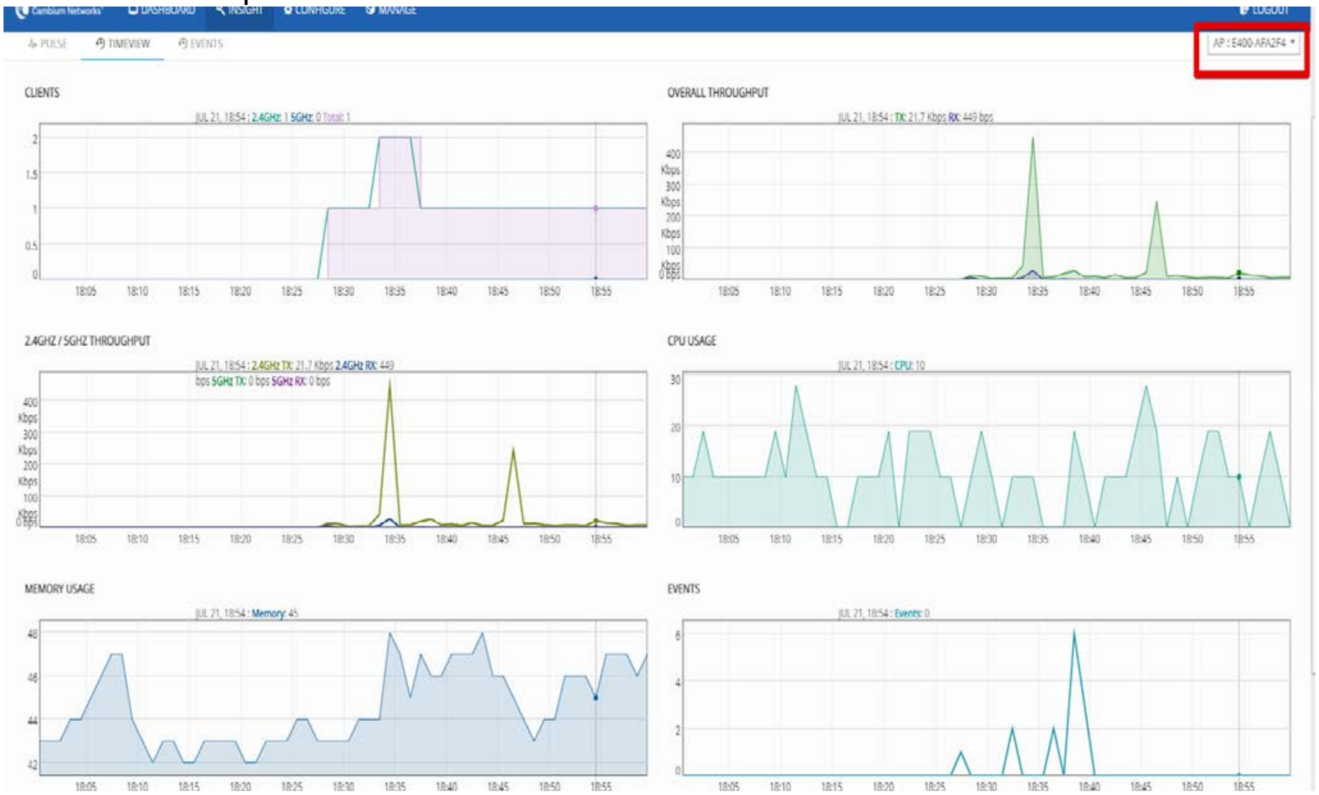
In current version not all of these options are supported.

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.

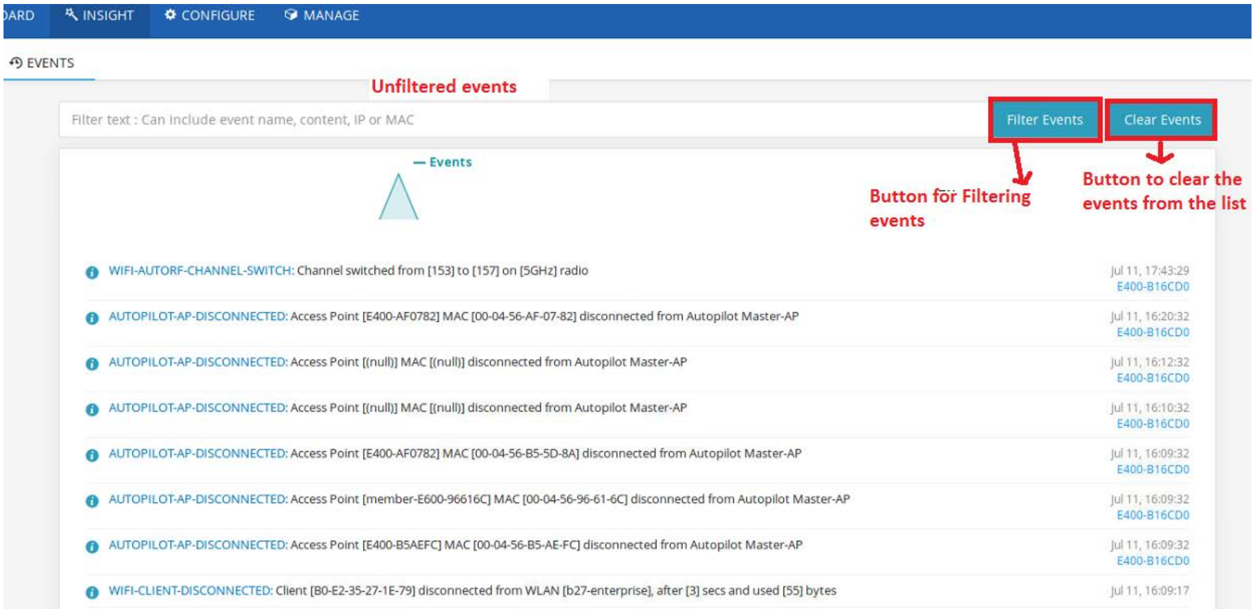


Also, Individual APs can be selected from the dropdown menu and all the above mentioned components of the selected AP can be tracked.

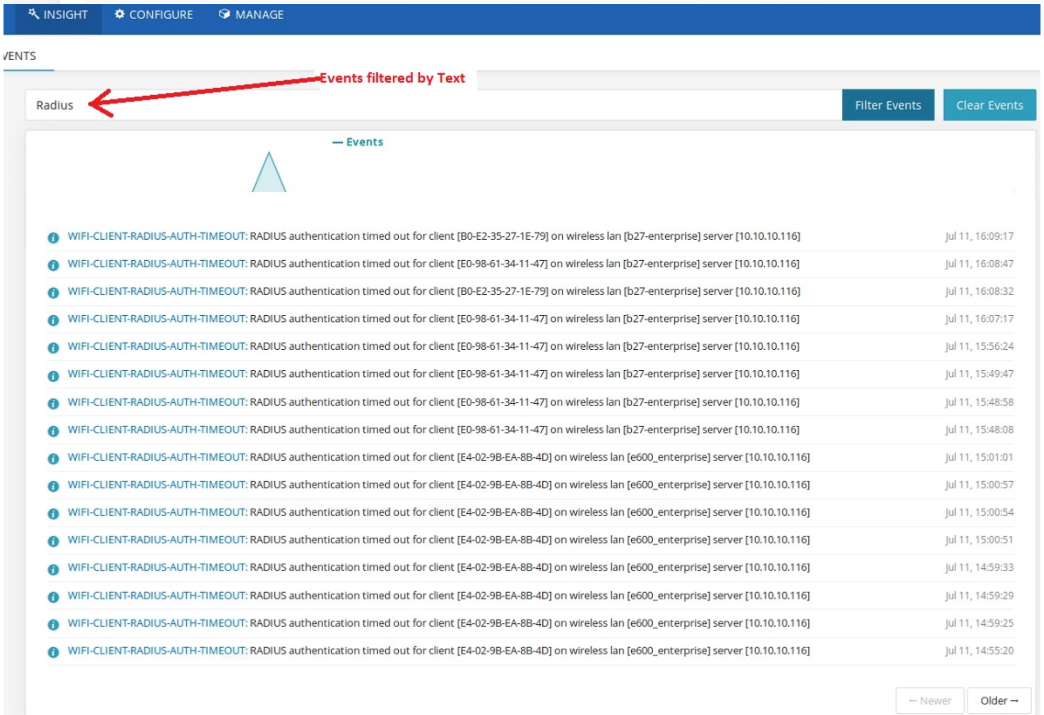


EVENTS

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.


ARD
INSIGHT
CONFIGURE
MANAGE
EVENTS
Unfiltered events
Filter text : Can include event name, content, IP or MAC
Filter Events
Clear Events
— Events
Button for Filtering events
Button to clear the events from the list

```
WIFI-AUTORF-CHANNEL-SWITCH: Channel switched from [153] to [157] on [5GHz] radio    Jul 11, 17:43:29
                                                                                    E400-B16CD0
AUTOPILOT-AP-DISCONNECTED: Access Point [E400-AF0782] MAC [00-04-56-AF-07-82] disconnected from Autopilot Master-AP    Jul 11, 16:20:32
                                                                                    E400-B16CD0
AUTOPILOT-AP-DISCONNECTED: Access Point [(null)] MAC [(null)] disconnected from Autopilot Master-AP    Jul 11, 16:12:32
                                                                                    E400-B16CD0
AUTOPILOT-AP-DISCONNECTED: Access Point [(null)] MAC [(null)] disconnected from Autopilot Master-AP    Jul 11, 16:10:32
                                                                                    E400-B16CD0
AUTOPILOT-AP-DISCONNECTED: Access Point [E400-AF0782] MAC [00-04-56-B5-5D-8A] disconnected from Autopilot Master-AP    Jul 11, 16:09:32
                                                                                    E400-B16CD0
AUTOPILOT-AP-DISCONNECTED: Access Point [member-E600-96616C] MAC [00-04-56-96-61-6C] disconnected from Autopilot Master-AP    Jul 11, 16:09:32
                                                                                    E400-B16CD0
AUTOPILOT-AP-DISCONNECTED: Access Point [E400-B5AEFC] MAC [00-04-56-B5-AE-FC] disconnected from Autopilot Master-AP    Jul 11, 16:09:32
                                                                                    E400-B16CD0
WIFI-CLIENT-DISCONNECTED: Client [B0-E2-35-27-1E-79] disconnected from WLAN [b27-enterprise], after [3] secs and used [55] bytes    Jul 11, 16:09:17
```



```
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [B0-E2-35-27-1E-79] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 16:09:17
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E0-98-61-34-11-47] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 16:08:47
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [B0-E2-35-27-1E-79] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 16:08:32
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E0-98-61-34-11-47] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 16:07:17
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E0-98-61-34-11-47] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 15:56:24
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E0-98-61-34-11-47] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 15:49:47
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E0-98-61-34-11-47] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 15:48:58
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E0-98-61-34-11-47] on wireless lan [b27-enterprise] server [10.10.10.116]    Jul 11, 15:48:08
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 15:01:01
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 15:00:57
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 15:00:54
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 15:00:51
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 14:59:33
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 14:59:29
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 14:59:25
WIFI-CLIENT-RADIUS-AUTH-TIMEOUT: RADIUS authentication timed out for client [E4-02-9B-EA-8B-4D] on wireless lan [e600_enterprise] server [10.10.10.116]    Jul 11, 14:55:20
```

Firmware Management

The running software on the cnPilot Enterprise AP can be upgraded to newer firmware from either the CLI or the UI. When upgrading from the CLI the user must specify a TFTP or FTP server from where the firmware file would be downloaded by the Access Point. When upgrading from the UI the user can upload the firmware file from the browser. The same process can be followed to downgrade the Access Point to a previous firmware version if required. Configuration is maintained across the firmware upgrade process.

Note

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

You can configure the parameters through the UI or CLI.

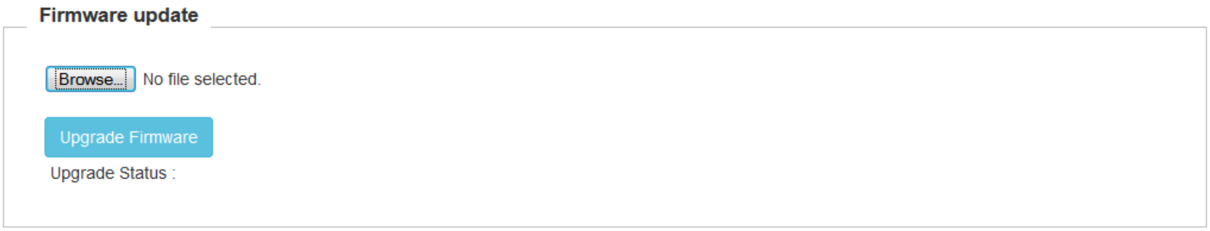
In the UI

1. Navigate to the **Operations > Firmware Upgrade** tab. The following fields are displayed:
2. To upgrade the firmware manually:

   Click **Browse** and select the downloaded image file.
3. To upgrade the firmware automatically:

   Click **Upgrade Firmware**.
4. You can view the status of upgrade in the **Upgrade Status** field.
5. Click **Save**.

Figure 27: Operations: Firmware Upgrade page



In the CLI

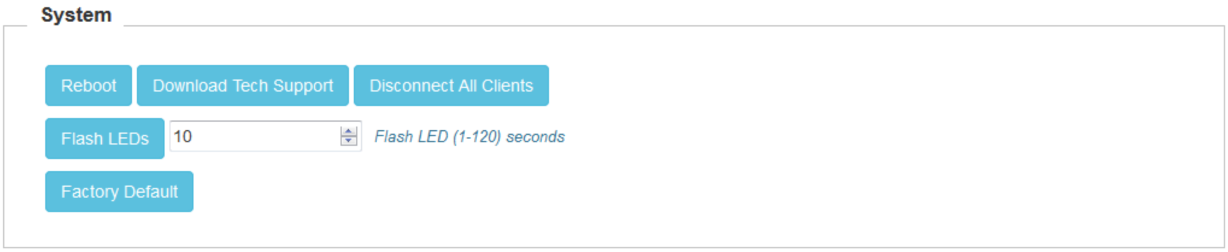
To upgrade firmware:

```
(cnPilot Enterprise AP) (configure)# upgrade
```

System

You can reboot the device, download tech support from the device, and disconnect all the wireless clients under the **Operations > System** page of the UI.

Figure 28: Configure: **Operations> Systems** page



System

Reboot Download Tech Support Disconnect All Clients

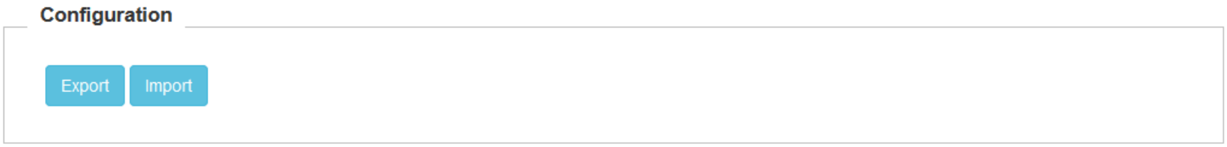
Flash LEDs 10 *Flash LED (1-120) seconds*

Factory Default

Configuration

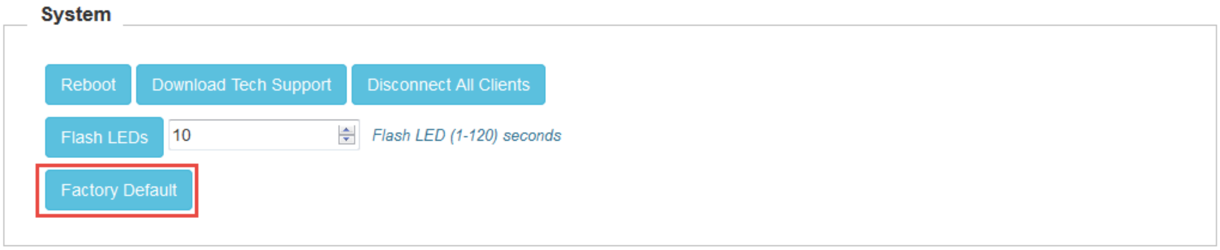
1. **Configuration Import, Export, Delete**: The device configuration can either be exported from the device as a text file of CLI commands, or imported into the device from a previous backup. The delete configuration option will factory-reset the device. All configuration, configured onboarding parameters are reset to default when the configuration is deleted and the device rebooted. Note that when a configuration file is imported onto the device, a reboot is necessary to activate that new configuration.

Figure 29: Import/Export Configuration



2. **Factory Default**: There are two ways a device can be reset back to factory default:
    1. Using the 'Factory Default' option in the Operations panel of the GUI or by using the 'delete config' CLI command.

Figure 30: Factory Default



    2. By pressing down the reset tab on the Access Point for about 10 seconds until the AP reboots (indicated by the power LED changing color from Green to Orange).

Services

This section provides information on how to configure the following services on an AP:

- LDAP
- NAT-Logging
- Location-API

LDAP

The following table lists the fields that are displayed in the **Configuration > Services > LDAP** page:

Table 24: Configuration: **LDAP** parameters

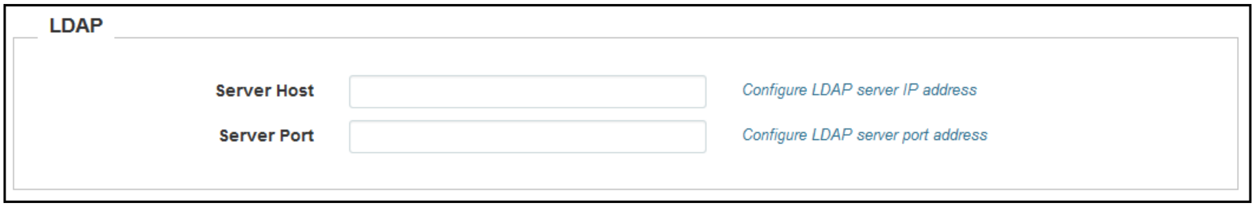
Parameter	Description	Default Value
Server Host	IP address of the LDAP server.	–
Server Port	Port address of the LDAP server.	–

You can configure the parameters through the UI or CLI.

In the UI

6. Navigate to the **Configuration > Services> LDAP** tab. The following fields are displayed:
7. Enter the IP address of the LDAP server in the **Server Host** text box.
8. Enter the Port address of the LDAP server in the **Server Port** text box.
9. Click **Save**.

Figure 31: Configurations: **Services > LDAP** page


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

NAT Logging

The NAT-log is same as the Internet access log that is generated when NAT is enabled on the 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 below:

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:

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.

The following table lists the fields that are displayed in the **Configuration > Services > NAT-Logging** page:

Table 26: Configuration: **NAT-Logging** parameters

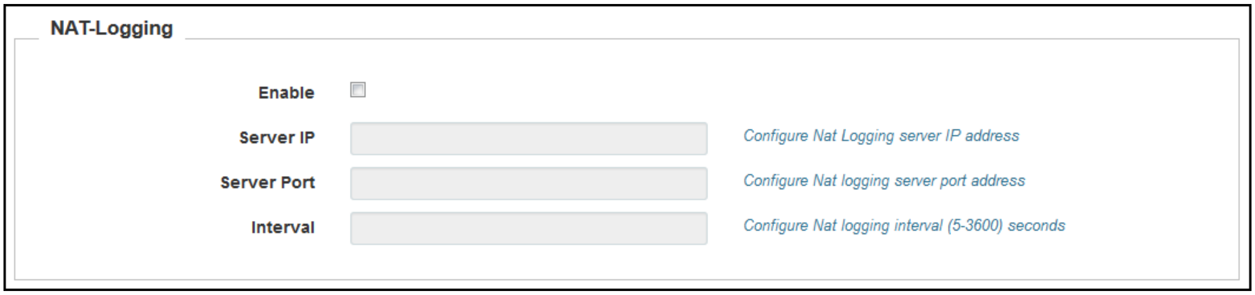
Parameter	Description	Default Value
Enable	To enable the NAT-Log functionality.	–
Server IP	The server IP address for NAT Logging.	–
Server Port	The server port address for NAT Logging.	–
Interval	The NAT logging interval in seconds.	–

You can configure the parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > Services> Nat-Logging** tab. The following fields are displayed:
2. Select the **Enable** checkbox to enable NAT- Logging.
3. Enter the IP address of the server for NAT Logging in the **Server IP** text box.
4. Enter the IP address of the server port for NAT Logging in the **Server Port** text box.
5. Enter the interval for NAT logging in the **Interval** text box.
6. Click **Save**.

Figure 32: Configurations: Services > NAT-Logging page



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) seconds

In the CLI

To configure NAT-Logging:

```
(cnPilot Enterprise AP) (configure)# nat-log
Interval < 5-3600s>
server-ip
server-port
```

Location API

Overview

Location API feature is a method to send the discovered (probed) clients list to the specified server address. The reports are send as a http post to the http server every interval. The http server address, port, and the interval can be configured from the AP CLI.

Discovered client list

The AP listens to the probe requests on the native (configured) channel and populates the discovered client list. The maximum list entries are set to 100. At first, 100 probed clients are added to the report and send to server. The list contains both 2.4Hz and 5GHz clients in case of dual radio APs. User can look at the opmode to identify the operation mode of the client.

Sending report

The discovered/probed client list is send to the configured http server periodically. The server, port, and period/interval can be configured by using the CLI command.

Aging out stale entries

The discovered client entries are deleted from the list if the entry is aged out. The age out time is five minutes, if there are no new probe requests from the client within 5 minutes the entry is deleted.

The following table lists the fields that are displayed in the **Configuration > Services > Location - API** page:

Table 27: Configuration: **Services > Location-API** parameters

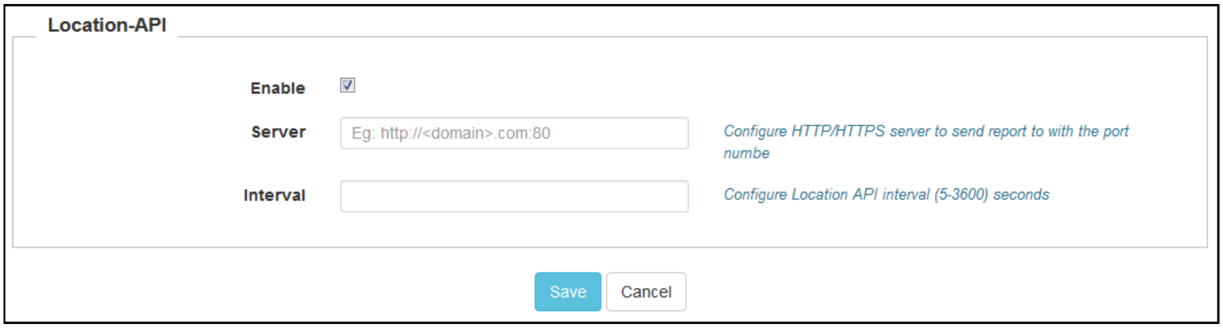
Parameter	Description	Default Value
Enable	To enable the Location-API functionality.	–
Server	The HTTP/HTTPS server to send report with the port number. (Example: http://192.168.0.100:8000)	–
Interval	The Location-API interval in seconds. Range: 5-3600	–

You can configure the parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > Services> Location-API** tab. The following fields are displayed:
2. Select the **Enable** checkbox to enable Location-API.
3. Enter the HTTP/HTTPs server and port number in the **Server** text box.
4. Enter the interval for location-API in the **Interval** text box.
5. Click **Save**.

Figure 33: Configurations: Services > Location-API page



Location-API

Enable ☑

Server Eg: http://<domain>.com:80 *Configure HTTP/HTTPS server to send report to with the port numbe*

Interval *Configure Location API interval (5-3600) seconds*

In the CLI

To configure Location-API:

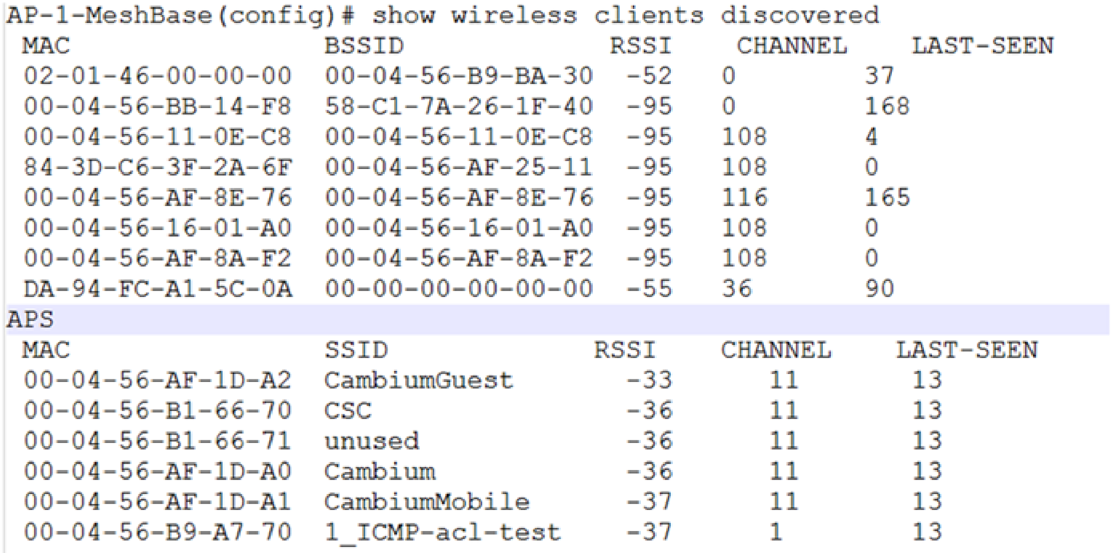
```
(cnPilot Enterprise AP) (configure)# location-api
Interval<5-3600>
Server
```

To disable the Location-API:

```
(cnPilot Enterprise AP) (configure)# no location-api
```

To view the list of discovered stations for the Location-API:

```
(cnPilot Enterprise AP) (configure) # show wireless clients discovered
```



```
AP-1-MeshBase(config)# show wireless clients discovered
 MAC                BSSID              RSSI   CHANNEL    LAST-SEEN
 02-01-46-00-00-00  00-04-56-B9-BA-30  -52   0          37
 00-04-56-BB-14-F8  58-C1-7A-26-1F-40  -95   0          168
 00-04-56-11-0E-C8  00-04-56-11-0E-C8  -95   108        4
 84-3D-C6-3F-2A-6F  00-04-56-AF-25-11  -95   108        0
 00-04-56-AF-8E-76  00-04-56-AF-8E-76  -95   116        165
 00-04-56-16-01-A0  00-04-56-16-01-A0  -95   108        0
 00-04-56-AF-8A-F2  00-04-56-AF-8A-F2  -95   108        0
 DA-94-FC-A1-5C-0A  00-00-00-00-00-00  -55   36         90
APS
 MAC                SSID              RSSI    CHANNEL     LAST-SEEN
 00-04-56-AF-1D-A2  CambiumGuest        -33      11         13
 00-04-56-B1-66-70  CSC                 -36      11         13
 00-04-56-B1-66-71  unused              -36      11         13
 00-04-56-AF-1D-A0  Cambium             -36      11         13
 00-04-56-AF-1D-A1  CambiumMobile       -37      11         13
 00-04-56-B9-A7-70  1_ICMP-acl-test     -37      1          13
```

Note

OCS should be enabled to view list of Wireless Clients and APs across channels.

HTTP post message format

The reports are send in JSON format as mentioned in the below sample:

```
{
   u'beaconed_aps':[
      {
         u'rssi':-92,
         u'mac':u'00-04-56-04-26-D0',
         u'chan':11,
         u'ssid':u'Default_2.4GHz',
         u'last_seen':70
      },
      {
         u'rssi':-89,
         u'mac':u'00-04-56-10-AB-E0',
         u'chan':11,
         u'ssid':u'cnPilot',
         u'last_seen':70
      },
      {
         u'rssi':-90,
         u'mac':u'00-04-56-95-BB-88',
         u'chan':52,
         u'ssid':u'auto-TEST_SMOKE_3',
         u'last_seen':242
      }
```

```
    ],
        u'associated_clients':[
           {
              u'ch':52,
              u'rssi':-36,
              u'mac':u'8C-85-90-B0-89-AC',
              u'last_seen':48100,
              u'bss':u'00-04-56-AF-8F-80'
           }
        ],
        u'probe_requests_clients':[
           {
              u'ch':11,
              u'rssi':-49,
              u'mac':u'3C-A9-F4-9F-3E-D8,
              u'last_seen':37,
              u'bss':u'00-04-56-9A-F7-40
           },
           {
              u'ch':11,
              u'rssi':-81,
              u'mac':u'00-04-56-93-F4-B0',
              u'last_seen':13,
              u'bss':u'00-00-00-00-00-00'
           },
           {
              u'ch':52,
              u'rssi':-79,
              u'mac':u'A4-4E-31-5F-6D-2C',
              u'last_seen':62,
              u'bss':u'00-04-56-BD-85-70
           }
        ],
           u'ap_mac':u'00-04-56-AF-89-BA',
           u'version':u'2.1',
           u'ap_name':u'E510-AF89BA'
        }
```

The JSON object contains the MAC of the AP followed by an array or records. The user/server can look at the MAC of the AP to find out from which device the reports are being sent.

The JSON object contains the MAC of the AP followed by an array or records. The user/server can look at the MAC of the AP to find out from which device the reports are being sent.

Parameter	Description
ap-mac	The MAC address of the AP which is same as the ESN number printed on the device.
ap-name	The hostname of the AP.

version	The version number of the protocol. if there is any change in the message format the version number will be changed and the server can look at the version number and parse the message accordingly. Currently the version is set to 2.1.
beaconed_aps	A JSON object with an array of discovered Neighbour BSS's records. The details about the neighbour BSS's are sent in beaconed_aps JSON array. Each Neighbour BSS record has the following details: **ch**: Channel on which BSS discovered. **mac**: The MAC address of the BSS. **rssi**: The SNR of the client in dB. **last_seen**: Time in milliseconds when the last probe request was received from the client. **ssid**: SSID of the BSS.
associated_clients	A JSON object with an array of associated client's records. The details about the associated clients are sent in associated_clients JSON array. Each client record has the following details: • **ch**: Channel on which client discovered. • **mac**: The MAC address of the client. • **bss:** The BSSID/MAC address of the WLAN on which the client has probed. **rssi:** The SNR of the client in dB. **last_seen:** Time in milliseconds when the last probe request was received from the client.
probe-requests	A JSON object with an array of probed client's records. The details about the probed client are sent in probe requests JSON array. Each client record has the following details: • **ch**: Channel on which client sends the probe request. • **mac**: The MAC address of the client. • **bss**: The BSSID/MAC address of the WLAN on which the client has probed. • **rssi**: The SNR of the client in dB. • **last_seen**: Time in milliseconds when the last probe request was received from the client.

WiFiperf

Wifiperf is a speed test service available on cnPilot APs.

Speed test between cnPilot AP and cnMeastro On-Premises

For the devices onboarded to cnMaestro On-Premises, speed test can be triggered from the controller.

Speed test between cnPilot AP and other devices

Wifiperf has interoperability support 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 the above URL 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 or CLI as shown below.

The following table lists the fields that are displayed in the **Configuration > Services > WiFiperf** page:

Table 26: Configuration: **WiFiperf** parameters

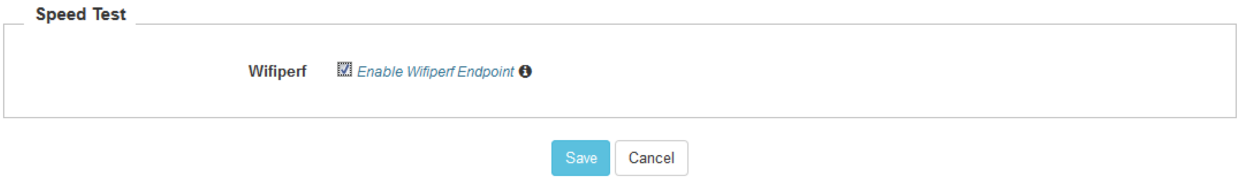
Parameter	Description	Default Value
wifiperf	To enable wifiperf functionality.	disable

You can configure the parameters through the UI or CLI.

In the UI

1. Navigate to the **Configuration > Services> wifiperf** tab. The following fields are displayed:

Figure 32: Configurations: Services > wifiperf page



Speed Test

Wifiperf ☑ Enable Wifiperf Endpoint

In the CLI

To configure NAT-Logging:

```
(cnPilot Enterprise AP) (configure)# wifiperf
```

Device Access

cnPilot E-series APs can learn the type of a device from the DHCP options. The device-access feature is used to limit the access on an SSID to a device type.

By default, access is allowed to all the devices. To block any device category, use the **NO device-access <device-name>** command.

Configuring Device Access:

Currently, you can configure this functionality by using CLI and configuring by using UI will be supported in the future release.

Syntax:

```
(Cambium AP) (config-wlan-<wlan-index># no device access {gaming, Linux, Macintosh,
multimedia, others, phone-tablet, printer, VoIP-phone, Wi-Fi-router, windows}
```

Example

```
(Cambium AP) (config-wlan-<wlan-index># no device access phone-tablet
```

Note

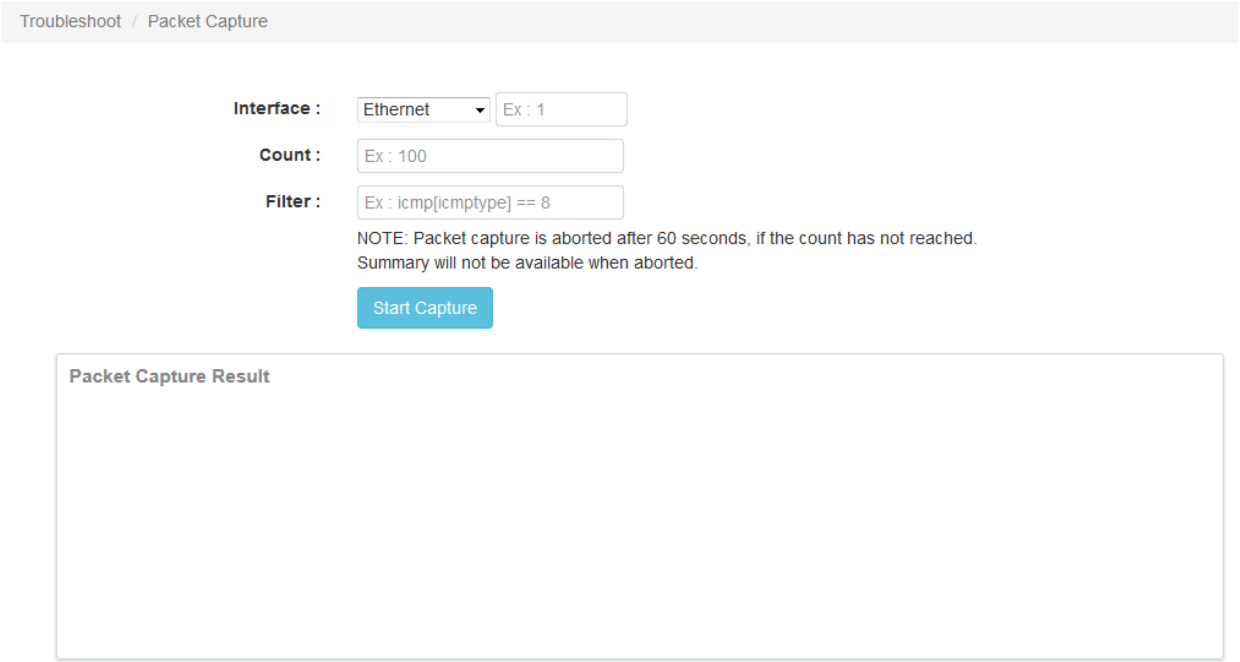
The **Show Configuration** command displays only non-default parameters, so by default nothing is shown, and if you disable access to a device-type, only that config line will be shown. Also this is a crude blocking that association will go through and the device will also attempt to get an IP address. It is the DHCP discover which we see from the device which allows us to learn what its type is and based on that act (disconnect it if it is a disallowed device).

Troubleshooting

The following types of troubleshooting tools are supported:

- **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. Packets captures on the WLAN interfaces are data packets on a particular WLAN as they are bridged on the radio interface of the device.

Figure 34: Troubleshooting > Packet Capture page



Troubleshoot / Packet Capture

Interface : Ethernet Ex : 1

Count : Ex : 100

Filter : Ex : icmp[icmptype] == 8

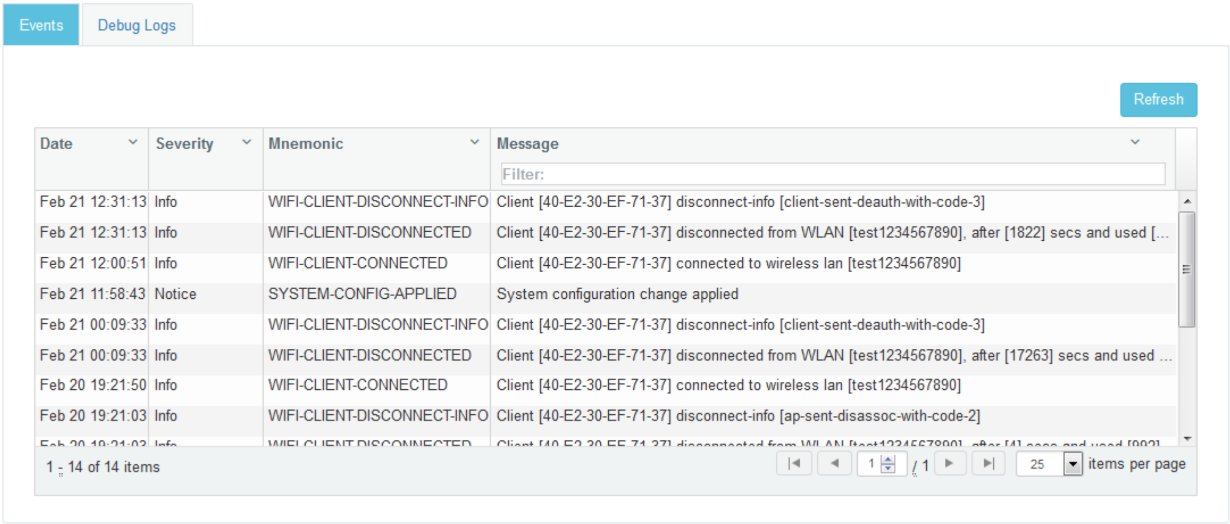
NOTE: Packet capture is aborted after 60 seconds, if the count has not reached.
Summary will not be available when aborted.

Packet Capture Result

- **Logs and Events**: The system generates event-messages for any notable activity on the device from client associations and authentications to system configuration changes. These logs are:

3. Forwarded to cnMaestro for later viewing and filtering
4. Buffered on the device and can be viewed using ‘show logging’ in the CLI
5. Transmitted to any configured syslog servers.

Figure 35: Logs page



Date	Severity	Mnemonic	Message
Feb 21 12:31:13	Info	WIFI-CLIENT-DISCONNECT-INFO	Client [40-E2-30-EF-71-37] disconnect-info [client-sent-deauth-with-code-3]
Feb 21 12:31:13	Info	WIFI-CLIENT-DISCONNECTED	Client [40-E2-30-EF-71-37] disconnected from WLAN [test1234567890], after [1822] secs and used [...
Feb 21 12:00:51	Info	WIFI-CLIENT-CONNECTED	Client [40-E2-30-EF-71-37] connected to wireless lan [test1234567890]
Feb 21 11:58:43	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Feb 21 00:09:33	Info	WIFI-CLIENT-DISCONNECT-INFO	Client [40-E2-30-EF-71-37] disconnect-info [client-sent-deauth-with-code-3]
Feb 21 00:09:33	Info	WIFI-CLIENT-DISCONNECTED	Client [40-E2-30-EF-71-37] disconnected from WLAN [test1234567890], after [17263] secs and used ...
Feb 20 19:21:50	Info	WIFI-CLIENT-CONNECTED	Client [40-E2-30-EF-71-37] connected to wireless lan [test1234567890]
Feb 20 19:21:03	Info	WIFI-CLIENT-DISCONNECT-INFO	Client [40-E2-30-EF-71-37] disconnect-info [ap-sent-disassoc-with-code-2]
Feb 20 19:21:03	Info	WIFI-CLIENT-DISCONNECTED	Client [40-E2-30-EF-71-37] disconnected from WLAN [test1234567890], after [4] secs and used [992]

1 - 14 of 14 items   1 / 1   25 items per page

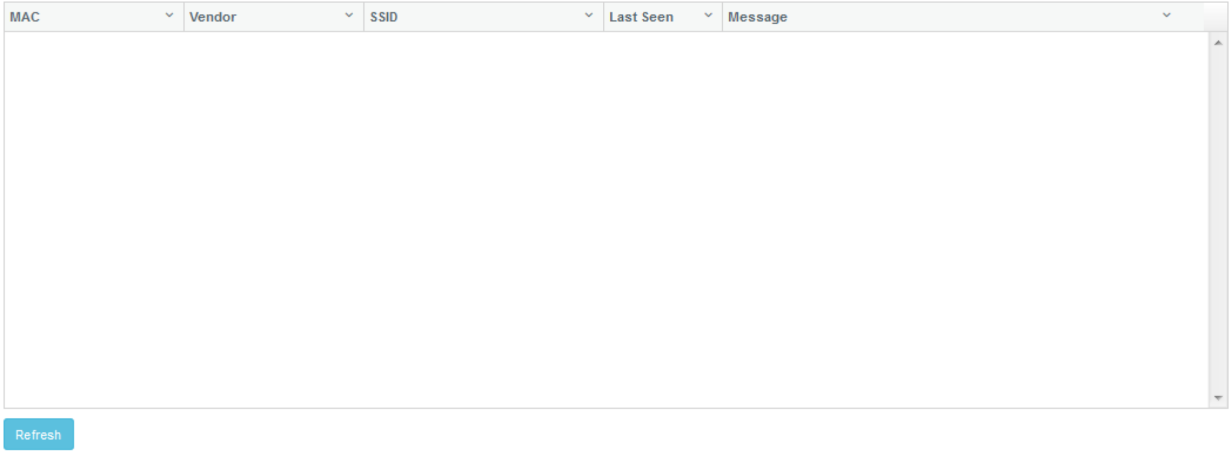
3. **Unconnected Clients**: Unconnected clients provides a list of clients that could not connect properly due to various reasons, with the access points. Currently the following failures are tracked:

   - Invalid pre-shared key
   - EAP authentication failure
   - Denied due to MAC ACL
   - Radius server not reachable
   - No radius server found
   - Client disconnected by enhanced-roaming
   - Denied association by enhanced-roaming

Use the following CLI to display the list of wireless clients unconnected:

```
(cnPilot Enterprise AP) (config)# show wireless unconnected clients
```

Figure 36: Unconnected Clients



MAC	Vendor	SSID	Last Seen	Message

Legal and Reference Information

This chapter provides legal notices including software license agreements.

⚠Caution

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

Cambium Networks End User License Agreement

ACCEPTANCE OF THIS AGREEMENT

In connection with Cambium Networks' delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both, Cambium Networks is willing to license this certain proprietary software and the accompanying documentation to you only on the condition that you accept all the terms in this End User License Agreement ("Agreement").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT OR INSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE PRODUCT, WILL CONSTITUTE YOUR ACCEPTANCE TO THE TERMS OF THIS AGREEMENT.

DEFINITIONS

In this Agreement, the word "Software" refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word "Documentation" refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word "Product" refers to Cambium Networks' fixed wireless broadband devices for which the Software and Documentation is licensed for use.

GRANT OF LICENSE

Cambium Networks Limited ("Cambium") grants you ("Licensee" or "you") a personal, nonexclusive, non-transferable license to use the Software and Documentation subject to the Conditions of Use set forth in "**Conditions of use**" and the terms and conditions of this Agreement. Any terms or conditions relating to the Software and Documentation appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

CONDITIONS OF USE

Any use of the Software and Documentation outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.

3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.

4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium Networks copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

TITLE AND RESTRICTIONS

If you transfer possession of any copy of the Software and Documentation to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Software and Documentation and any copies made by you remain with Cambium Networks and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Cambium's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Software and Documentation be equipped with such a protection device. If the Software and Documentation is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Cambium's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

CONFIDENTIALITY

You acknowledge that all Software and Documentation contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Software and Documentation will result in irreparable harm to Cambium Networks for which monetary damages would be inadequate and for which Cambium Networks will be entitled to immediate injunctive relief. If applicable, you will limit access to the Software and Documentation to those of your employees and agents who need to use the Software and Documentation for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Software and Documentation, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Cambium Networks prior to such disclosure and provide Cambium Networks with a reasonable opportunity to respond.

RIGHT TO USE CAMBIUM’S NAME

Except as required in “**Conditions of use**”, you will not, during the term of this Agreement or thereafter, use any trademark of Cambium Networks, or any word or symbol likely to be confused with any Cambium Networks trademark, either alone or in any combination with another word or words.

TRANSFER

The Software and Documentation may not be transferred to another party without the express written consent of Cambium Networks, regardless of whether or not such transfer is accomplished by physical or electronic means. Cambium’s consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

UPDATES

During the first 12 months after purchase of a Product, or during the term of any executed Maintenance and Support Agreement for the Product, you are entitled to receive Updates. An “Update” means any code in any form which is a bug fix, patch, error correction, or minor enhancement, but excludes any major feature added to the Software. Updates are available for download at the support website.

Major features may be available from time to time for an additional license fee. If Cambium Networks makes available to you major features and no other end user license agreement is provided, then the terms of this Agreement will apply.

MAINTENANCE

Except as provided above, Cambium Networks is not responsible for maintenance or field service of the Software under this Agreement.

DISCLAIMER

CAMBIUM NETWORKS DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. CAMBIUM NETWORKS SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILTY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS." CAMBIUM NETWORKS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM NETWORKS MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

LIMITATION OF LIABILITY

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

U.S. GOVERNMENT

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Software and Documentation is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

TERM OF LICENSE

Your right to use the Software will continue in perpetuity unless terminated as follows. Your right to use the Software will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Cambium Networks in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Cambium Networks, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

GOVERNING LAW

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

ASSIGNMENT

This agreement may not be assigned by you without Cambium's prior written consent.

SURVIVAL OF PROVISIONS

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

ENTIRE AGREEMENT

This agreement contains the parties' entire agreement regarding your use of the Software and may be amended only in writing signed by both parties, except that Cambium Networks may modify this Agreement as necessary to comply with applicable laws.

THIRD PARTY SOFTWARE

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

Zap	Copyright (c) 2004-2009, Ruckus Wireless, Inc. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

* Neither the name of Ruckus Wireless nor the

names of its contributors may be used to endorse or promote products

derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND

ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED

WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE

DISCLAIMED. IN NO EVENT SHALL COPYRIGHT HOLDER OR CONTRIBUTERS BE LIABLE FOR ANY

DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES

(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;

LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND

ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS

SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Aquila

Copyright (c) 2002-2010, Atheros Communications Inc.
Copyright (c) 2002-2005 Sam Leffler, Errno Consulting
Copyright (C) 2011 Denali Software Inc. All rights reserved

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES
WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR
ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES
WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF
OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

==

Redistribution and use in source and binary forms are permitted provided that the following conditions are met:

1. The materials contained herein are unmodified and are used unmodified.
2. Redistributions of source code must retain the above copyright notice, this list of conditions and the following NO ''WARRANTY'' disclaimer below (''Disclaimer''), without modification.
3. Redistributions in binary form must reproduce at minimum a disclaimer similar to the Disclaimer below and any redistribution must be conditioned upon including a substantially similar Disclaimer requirement for further binary redistribution.
4. Neither the names of the above-listed copyright holders nor the names of any contributors may be used to endorse or promote product derived from this software without specific prior written permission.

NO WARRANTY
THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES,

	INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NONINFRINGEMENT,MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
Linux Kernel	Copyright (c) 1989, 1991 Free Software Foundation NOTE! This copyright does *not* cover user programs that use kernel services by normal system calls - this is merely considered normal use of the kernel, and does *not* fall under the heading of "derived work". Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the Linux kernel) is copyrighted by me and others who actually wrote it. Also note that the only valid version of the GPL as far as the kernel is concerned is _this_ particular version of the license (ie v2, not v2.2 or v3.x or whatever), unless explicitly otherwise stated. Linus Torvalds -- GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.

gpio_keys	/* * Driver for keys on GPIO lines capable of generating interrupts. * * Copyright 2005 Phil Blundell * * This program is free software; you can redistribute it and/or modify * it under the terms of the GNU General Public License version 2 as * published by the Free Software Foundation. */
uboot	Copyright (c) 2007 Wolfgan Denk, DENIX Software Engeneering, wd@denix.de # (C) Copyright 2000 - 2005 # Wolfgang Denk, DENX Software Engineering, wd@denx.de. # # See file CREDITS for list of people who contributed to this # project. # # This program is free software; you can redistribute it and/or # modify it under the terms of the GNU General Public License as # published by the Free Software Foundation; either version 2 of # the License, or (at your option) any later version. # # This program is distributed in the hope that it will be useful, # but WITHOUT ANY WARRANTY; without even the implied warranty of # MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the # GNU General Public License for more details. # # You should have received a copy of the GNU General Public License # along with this program; if not, write to the Free Software # Foundation, Inc., 59 Temple Place, Suite 330, Boston, # MA 02111-1307 USA See above for details of the license.

busybox

--- A note on GPL versions

BusyBox is distributed under version 2 of the General Public License (included in its entirety, below). Version 2 is the only version of this license which this version of BusyBox (or modified versions derived from this one) may be distributed under.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> **b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
>
> **c)** Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

	10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally. NO WARRANTY **11.** BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. **12.** IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS
dnsmasq	# This program is free software; you can redistribute it and/or modify # it under the terms of the GNU General Public License as published by # the Free Software Foundation; version 2 dated June, 1991, or # (at your option) version 3 dated 29 June, 2007. See above for details of the license.

dropbear	Dropbear contains a number of components from different sources, hence there are a few licenses and authors involved. All licenses are fairly non-restrictive. The majority of code is written by Matt Johnston, under the license below.

Portions of the client-mode work are (c) 2004 Mihnea Stoenescu, under the same license:

Copyright (c) 2002-2008 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

=====

LibTomCrypt and LibTomMath are written by Tom St Denis, and are Public Domain.

=====

sshpty.c is taken from OpenSSH 3.5p1,
Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
All rights reserved
"As far as I am concerned, the code I have written for this software
can be used freely for any purpose. Any derived versions of this
software must be clearly marked as such, and if the derived work is
incompatible with the protocol description in the RFC file, it must be
called by a name other than "ssh" or "Secure Shell". "

=====

loginrec.c

loginrec.h
atomicio.h
atomicio.c
and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

hostapd	Copyright (c) 2002-2011, Jouni Malinen <j@w1.fi> and contributors All Rights Reserved. These programs are dual-licensed under both the GPL version 2 and BSD license (the one with advertisement clause removed). Either license may be used at your option. This package may include either wpa_supplicant, hostapd, or both. See README file respective subdirectories (wpa_supplicant/README or hostapd/README) for more details. See above for details of the license.
iproute2	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.
iptables	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 675 Mass Ave, Cambridge, MA 02139, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.
Openssl	LICENSE ISSUES ============== The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org. OpenSSL License --------------- Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

	1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)" 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org. 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project. 6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)" THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
c-ares	Copyright 1998 by the Massachusetts Institute of Technology. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

lighttpd	Copyright (c) 2004, Jan Kneschke, incremental All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: - Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. - Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. - Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
libnl	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.] Preamble The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This license, the Lesser General Public License, applies to some

specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

bridge-utils	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.
jansson	Copyright (c) 2009-2013 Petri Lehtinen <petri@digip.org> Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
libnl	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

libwebsockets	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.] See above for details of the license.
mtd	Copyright © 2005 Waldemar Brodkorb <wbx@dass-it.de> Copyright (C) 2005-2009 Felix Fietkau < ndb@openwrt.org> # # Copyright (C) 2006-2009 OpenWrt.org # # This is free software, licensed under the GNU General Public License v2. # See above for details of the license.
netsnmp	Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. ---- Part 1: CMU/UCD copyright notice: (BSD like) ----- Copyright 1989, 1991, 1992 by Carnegie Mellon University Derivative Work - 1996, 1998-2000 Copyright 1996, 1998-2000 The Regents of the University of California All Rights Reserved Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE

OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2012, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and

Telecommunications, nor the names of their contributors may

be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``ASIS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz bernhard.penz@fabasoft.com Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,

this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or

promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULARPURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVENIF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions

are met:

1. Redistributions of source code must retain the above copyright

notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above

copyright notice, this list of conditions and the following

disclaimer in the documentation and/or other materials provided

with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its

contributors may be used to endorse or promote products derived

from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are

met:

* Redistributions of source code must retain the above copyright notice,

this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright

notice, this list of conditions and the following disclaimer in the

documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its

contributors may be used to endorse or promote products derived

from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE

USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

rng-tools	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.
strace	Copyright (c) 1991, 1992 Paul Kranenburg <pk@cs.few.eur.nl> Copyright (c) 1993 Branko Lankester <branko@hacktic.nl> Copyright (c) 1993 Ulrich Pegelow <pegelow@moorea.uni-muenster.de> Copyright (c) 1995, 1996 Michael Elizabeth Chastain <mec@duracef.shout.net> Copyright (c) 1993, 1994, 1995, 1996 Rick Sladkey <jrs@world.std.com> Copyright (C) 1998-2001 Wichert Akkerman <wakkerma@deephackmode.org> All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

stunnel	Copyright (C) 1998-2014 Michal Trojnara This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. You should have received a copy of the GNU General Public License along with this program; if not, see <http://www.gnu.org/licenses>. Linking stunnel statically or dynamically with other modules is making a combined work based on stunnel. Thus, the terms and conditions of the GNU General Public License cover the whole combination. In addition, as a special exception, the copyright holder of stunnel gives you permission to combine stunnel with free software programs or libraries that are released under the GNU LGPL and with code included in the standard release of OpenSSL under the OpenSSL License (or modified versions of such code, with unchanged license). You may copy and distribute such a system following the terms of the GNU GPL for stunnel and the licenses of the other code concerned. Note that people who make modified versions of stunnel are not obligated to grant this special exception for their modified versions; it is their choice whether to do so. The GNU General Public License gives permission to release a modified version without this exception; this exception also makes it possible to release a modified version which carries forward this exception.

tcpdump	Copyright (c) 1991, 1992 Paul Kranenburg <pk@cs.few.eur.nl> Copyright (c) 1993 Branko Lankester <branko@hacktic.nl> Copyright (c) 1993 Ulrich Pegelow <pegelow@moorea.uni-muenster.de> Copyright (c) 1995, 1996 Michael Elizabeth Chastain <mec@duracef.shout.net> Copyright (c) 1993, 1994, 1995, 1996 Rick Sladkey <jrs@world.std.com> Copyright (C) 1998-2001 Wichert Akkerman <wakkerma@deephackmode.org> All rights reserved. See above for details of the license.
uboot-tools	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.
wireless_tools	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.

linux	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.
libcli	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.] See above for details of the license.
libscmd	GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999 Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.] See above for details of the license.
angular	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

	The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
angular-ui	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org See above for details of the license.
angular-ui-bootstrap	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org See above for details of the license.
angular-ui-grid	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org See above for details of the license.
bootstrap	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org See above for details of the license.
c3	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org See above for details of the license.

jquery	The MIT License Copyright (c) 2010-2015 Google, Inc. http://angularjs.org See above for details of the license.
cambium_iprst	GNU GENERAL PUBLIC LICENSE Version 2, June 1991 Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. See above for details of the license.