Cambium Networks™

USER GUIDE

Enterprise Wi-Fi Access Points

System Release **6.2**

Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

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

Contents

Chapter 1: About This User Guide

This chapter describes the following topics:

- Overview of Enterprise Wi-Fi AP products
- Intended audience
- Purpose
- Related documents
- Hardware platforms

Overview of Enterprise Wi-Fi AP products

This User Guide describes the features supported by Enterprise Wi-Fi Access Point (AP) and provides detailed instructions for setting Up and configuring Enterprise Wi-Fi AP.

Intended audience

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

Purpose

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

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

Related documents

Table 1 provides details on Enterprise Wi-Fi AP's support information.

Table 1 :Related documents

Enterprise Wi-Fi AP product details	https://www.cambiumnetworks.com/products/wifi/
Enterprise Wi-Fi AP User Guide (This document)	https://support.cambiumnetworks.com/files
Enterprise Wi-Fi AP Release Notes	https://support.cambiumnetworks.com/files
Software Resources	https://support.cambiumnetworks.com/files
Community	http://community.cambiumnetworks.com/
Support	https://www.cambiumnetworks.com/support/contact-support/

Warranty	https://www.cambiumnetworks.com/support/warranty/
Feedback	For feedback, e-mail to support@cambiumnetworks.com/

Hardware platforms

Table 2 :Existing platforms

Hardware	Description
XV3-8	8x8:8, 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Radio indoor Access Point
XV2-2	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio indoor Access Point

Chapter 2: Quick Start – Device Access

This chapter describes the following topics:

- Powering up the device
- DC power supply
- LED status

Powering up the device

This section includes the following topics:

- PoE switches (802.3af/802.3at/802.3bt)
- PoE adapter
- DC power supply

Enterprise Wi-Fi AP product family can be powered using PoE adapter provided in the package or DC power supply or it can be powered using 802.3af/at/bt capable switches. When powered using 802.3af/at/bt switches based on the negotiated power the modules are enabled.

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

Enterprise Wi-Fi APs negotiate the power via LLDP mechanism. Figure 1 displays the snippet of AP connection to PoE switches.

Figure 1 : *Installation of Enterprise Wi-Fi AP to PoE capable switch*

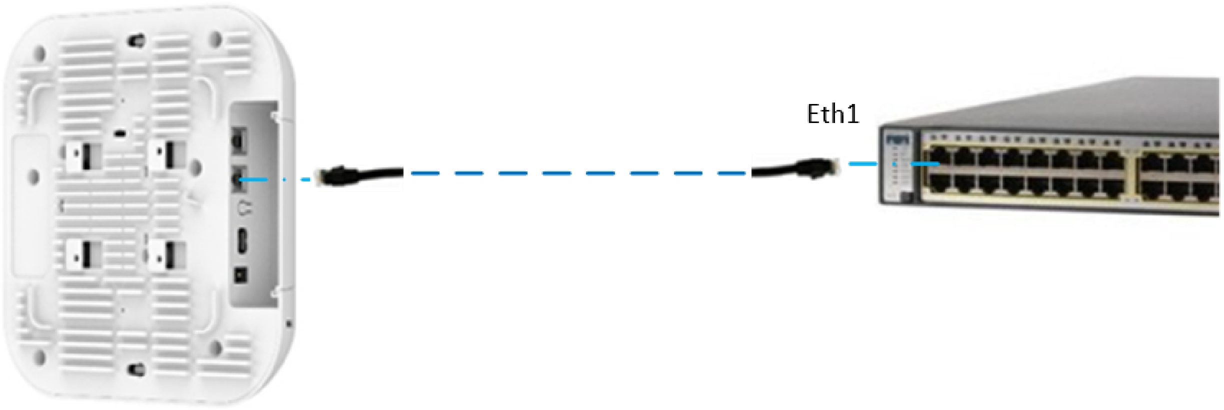


Table 3 provides detailed information on the modules that are enabled based on power negotiated via LLDP.

Table 3 :LLDP Power negotiation

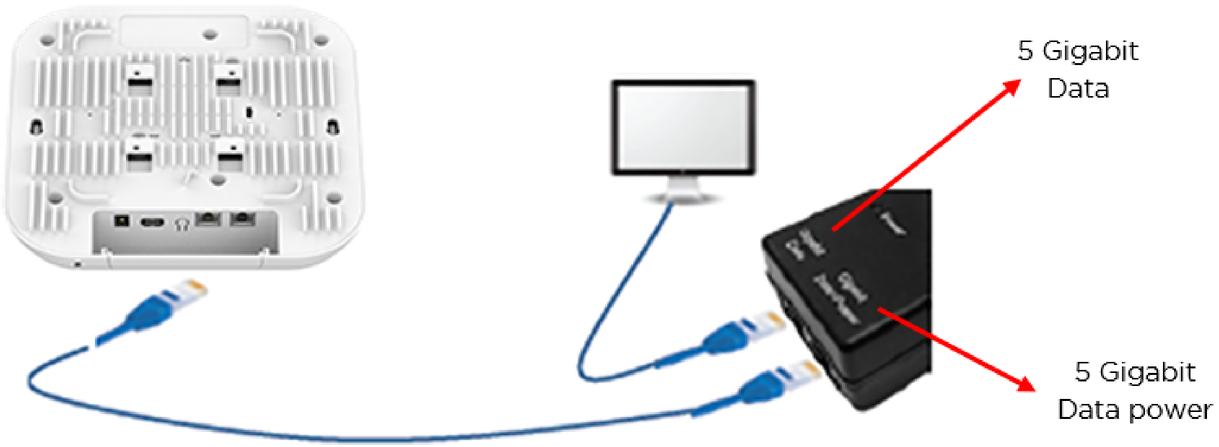
Serial Number	PSE detection mode	Power Available for AP	LLDP Power Negotiation	Modules
1	802.3af	Critical	Yes	• Wireless modules: Enabled • USB port: Disabled • BT module: Disabled
2	802.3at	Limited	Yes	• Wireless modules: Enabled • USB port: Disabled • BT module: Disabled
3	802.3bt Class-0/1/2/3	Critical	Yes	• Wireless modules: Enabled • USB port: Disabled • BT module: Disabled
4	802.3bt Class-4	Limited	Yes	• Wireless modules: Enabled • USB port: Disabled • BT module: Disabled
5	802.3bt Class-5	Sufficient	No	• Wireless modules: Enabled • USB port: Enabled • BT module: Enabled

PoE adapter

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

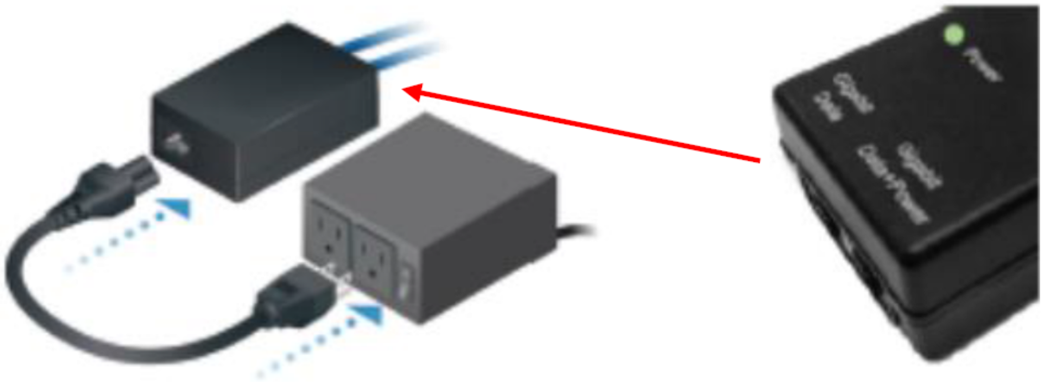
1. Connect the Ethernet cable from Eth1/PoE-IN of the device to the PoE port of 5 Gigabit Data + Power.
2. Connect an Ethernet cable from your LAN or Computer to the 5 Gigabit Data port of the PoE adapter.

Figure 2 : *Installation of Enterprise Wi-Fi AP to PoE adapter*



3. Connect the power cord to the adapter, and then plug the power cord into a power outlet as shown in below figure. Once powered ON, the Power LED should illuminate continuously on the PoE Adapter.

Figure 3 : *Installation of adapter to power outlet*



DC power supply

The Enterprise Wi-Fi AP has an option to power via a DC power adapter through the barrel connector. If both the dc power adapter and POE are connected, the dc power adapter takes precedence.

Accessing the device

This section includes the following topics:

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

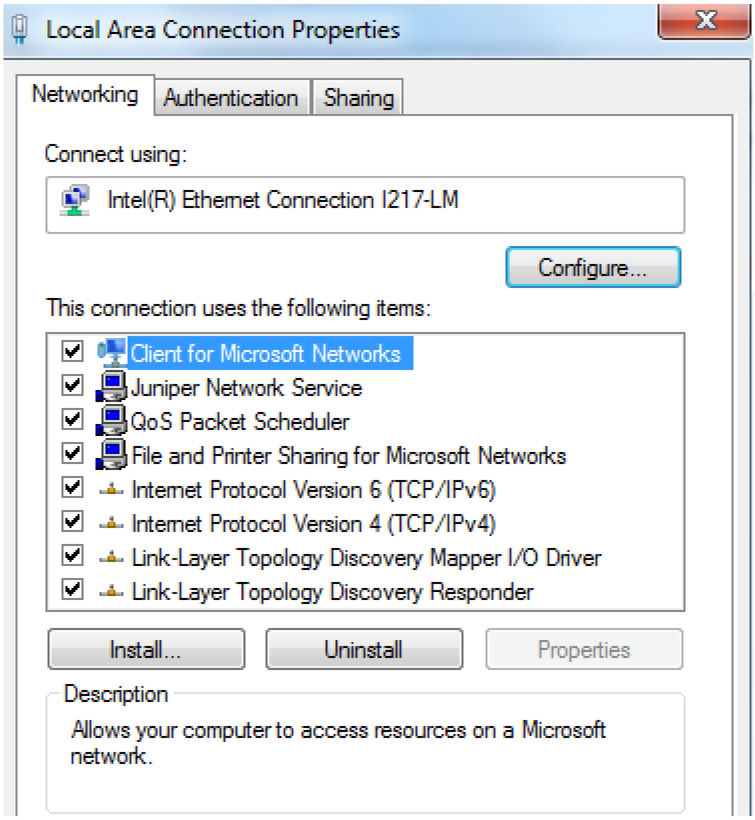
Once the device is powered up ensure the device is up and running before you try to access it based on LED status. Power LED on the Enterprise Wi-Fi AP device should turn Green which indicates that the device is ready for access.

Device access using default/fallback IP

1. Select Properties for the Ethernet port:

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

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



Connect using:

Intel(R) Ethernet Connection I217-LM

This connection uses the following items:

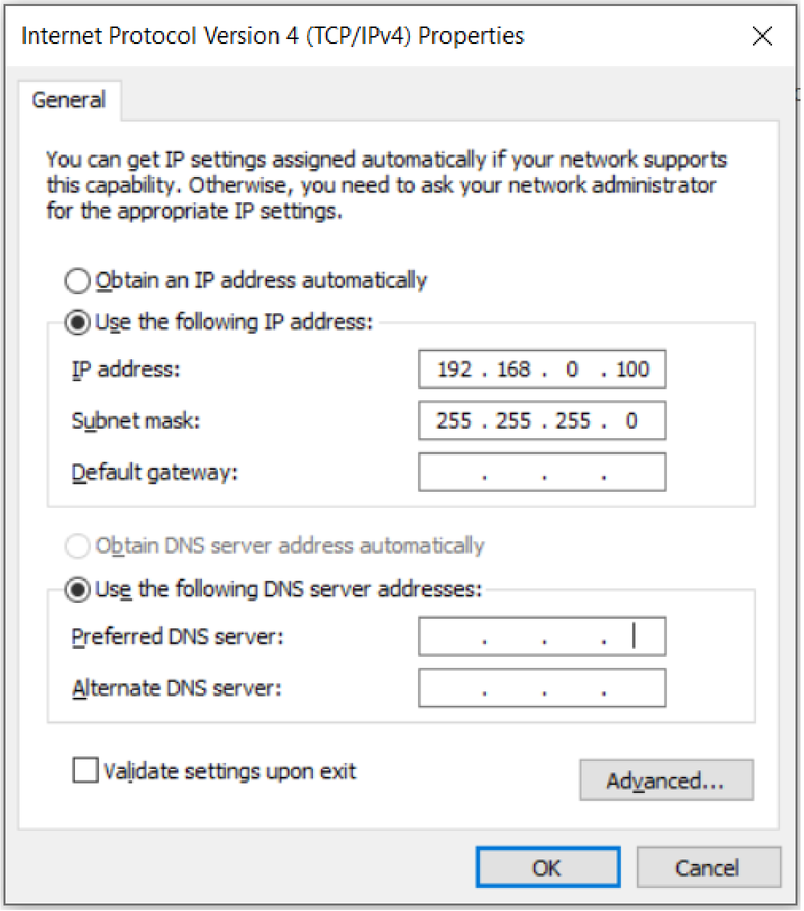
- ☑ Client for Microsoft Networks
- ☑ Juniper Network Service
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology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

Description

Allows your computer to access resources on a Microsoft network.

2. IP Address Configuration:

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


Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

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

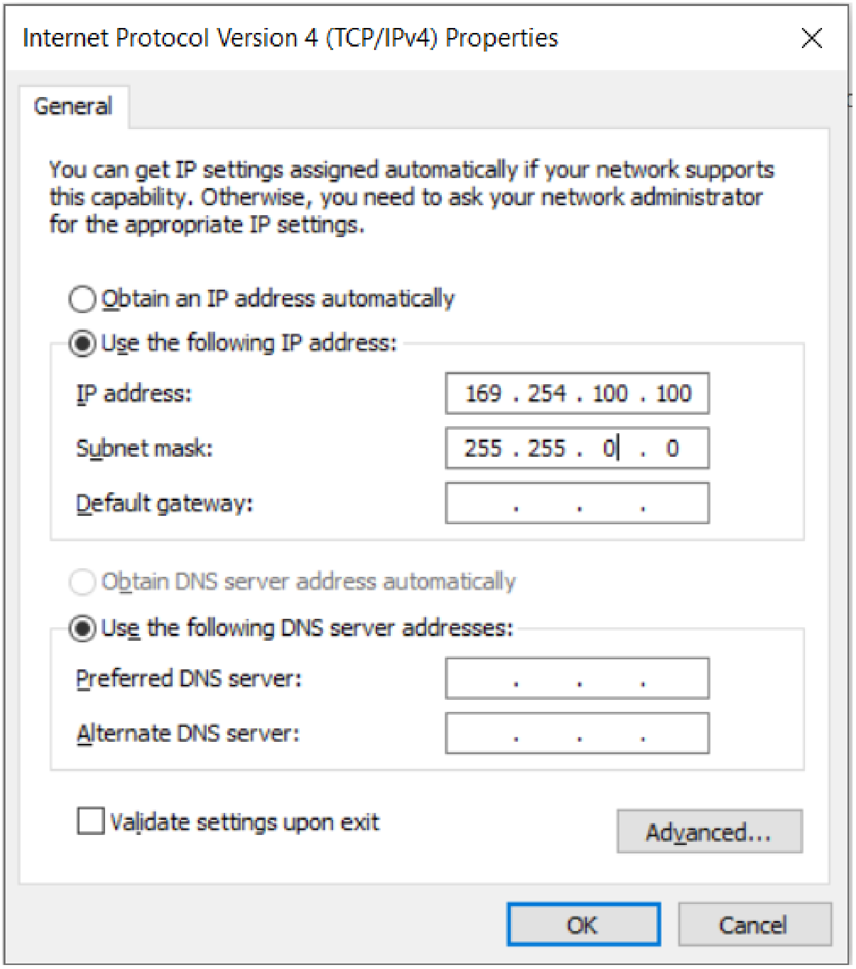
- Username: admin
- Password: admin

Device access using zeroconf IP

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

For example:

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


Internet Protocol Version 4 (TCP/IPv4) Properties

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 169 . 254 . 100 . 100

Subnet mask: 255 . 255 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

4. Access the device UI using http://169.254.170.187 with default credentials as below:

- Username: admin
- Password: admin

Device access using DHCP IP address

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

- Username: admin
- Password: admin

LED status

The XV3-8/XV2-2 AP has single color LED. The power LED will glow Amber as the AP boots up and turn Green once it has booted up successfully. The network/status LED will glow Amber if the connection to

XMS/cnMaestro controller/manager is down and turns Blue once the AP is connected successfully to XMS/cnMaestro.

Table 4 :XV3-8/XV2-2 LED status

LED Color	Status Indication
🟧	• Device is booting up. **Note** If these LEDs remain 'Amber' for more than 5 minutes, indicates that the device failed to boot.
🟩	• Device is successfully up and accessible. • Wi-Fi services are up if configured.
🟦	• XMS/cnMaestro connection is successful.

Chapter 3: Onboarding the Device

This chapter describes the following topics:

- Overview
- Device Onboarding and Provisioning
  - cnMaestro
  - XMS-Cloud

Overview

By default, all devices contact https://cloud.cambiumnetworks.com, no user action is required to direct devices to contact either cnMaestro Cloud or XMS-Cloud. You can onboard and provision devices without any additional setup.

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

https://support.cambiumnetworks.com/files/cnmaestro/ and download cnMaestro On-Premises 2.4.1 User Guide.

Device Onboarding and Provisioning

cnMaestro Cloud

For onboarding devices to cnMaestro Cloud, please refer https://docs.cloud.cambiumnetworks.com/help/2.4.0/index.htm#UG_files/Onboarding Devices/Onboarding.htm%3FTocPath%3DDevice%2520Onboarding%7C_____0.

XMS-Cloud

This section describes the following topics:

- Overview
- Device Onboarding

Overview

XMS-Cloud makes it easy to manage your networks from a single, powerful dashboard. Zero-touch provisioning and centralized, multi-tenant network orchestration simplify network management functions. XMS-Cloud manages Cambium Enterprise Wi-Fi devices.

Device Onboarding

For onboarding devices to XMS-Cloud, please see https://www.youtube.com/watch?v=qD-nPsdRc4Y

Chapter 4: UI Navigation

You can manage Enterprise Wi-Fi AP device using the on-device User Interface (UI) which is accessible from any network devices such as computer, mobile, tabs, etc. Enterprise Wi-Fi AP device accessibility is explained in Chapter 3.

This chapter describes the following topics:

- Login screen
- Home page (Dashboard)

Login screen

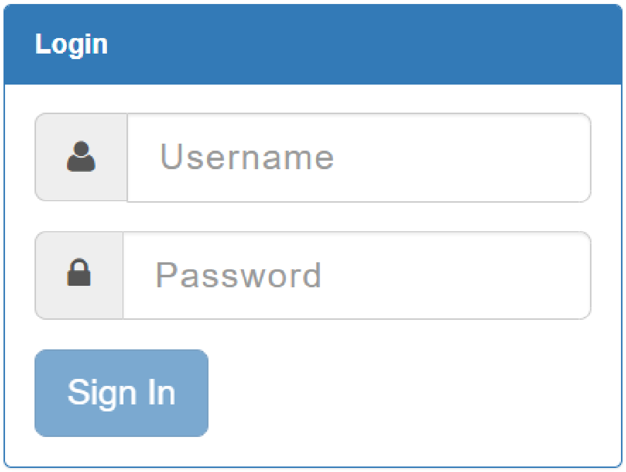
To log to the UI, enter the following credentials:

- Username: admin
- Password: admin

Note

Users are advised to change the Username and Password immediately after the first login as a security best practice.

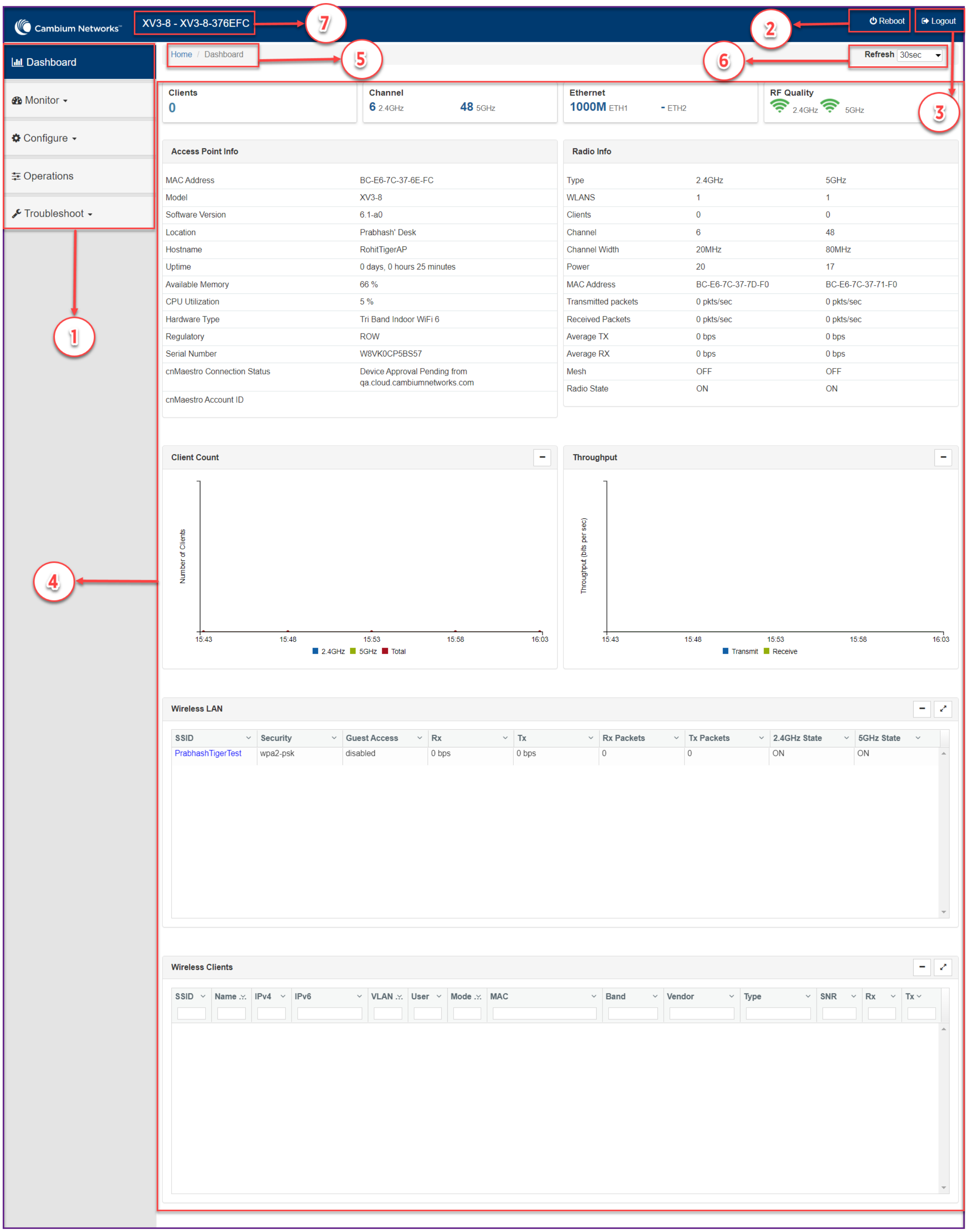
Figure 4 : *UI Login page*



Home page (Dashboard)

On logging into Enterprise Wi-Fi AP login page, the UI Home page is displayed. Figure 5 displays the parameters that are displayed in Enterprise Wi-Fi AP Home page.

Figure 5 : *Enterprise Wi-Fi AP UI Home page*



Access Point Info

MAC Address	BC-E6-7C-37-6E-FC
Model	XV3-8
Software Version	6.1-a0
Location	Prabhash' Desk
Hostname	RohitTigerAP
Uptime	0 days, 0 hours 25 minutes
Available Memory	66 %
CPU Utilization	5 %
Hardware Type	Tri Band Indoor WiFi 6
Regulatory	ROW
Serial Number	W8VK0CP5BS57
cnMaestro Connection Status	Device Approval Pending from qa.cloud.cambiumnetworks.com
cnMaestro Account ID	

Radio Info

Type	2.4GHz	5GHz
WLANS	1	1
Clients	0	0
Channel	6	48
Channel Width	20MHz	80MHz
Power	20	17
MAC Address	BC-E6-7C-37-7D-F0	BC-E6-7C-37-71-F0
Transmitted packets	0 pkts/sec	0 pkts/sec
Received Packets	0 pkts/sec	0 pkts/sec
Average TX	0 bps	0 bps
Average RX	0 bps	0 bps
Mesh	OFF	OFF
Radio State	ON	ON

Wireless LAN

SSID	Security	Guest Access	Rx	Tx	Rx Packets	Tx Packets	2.4GHz State	5GHz State
PrabhashTigerTest	wpa2-psk	disabled	0 bps	0 bps	0	0	ON	ON

Wireless Clients

SSID	Name	IPv4	IPv6	VLAN	User	Mode	MAC	Band	Vendor	Type	SNR	Rx	Tx

Table 5 :Enterprise Wi-Fi AP web interface elements

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

Monitor

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

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

Configure

This section allows user to configure Enterprise Wi-Fi AP device based on deployment requirement. This tab has multiple sections as follows:

- System: Provision to configure System UI parameter.
- Radio: Provision to configure Radio settings (2.4GHz/5GHz).
- WLAN: Provision to configure WLAN parameters as per the end user requirement and type of wireless station.
- Network: Provides information related to VLAN, Routes, Ethernet ports etc.
- Services: Provides information related to Network and Bonjour Gateway.

Operations

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

- Firmware update: Provision to upgrade Enterprise Wi-Fi AP devices.
- System: Provides different methods of debugging field issues and recovering device.
- Configuration: Provision to modify configuration of device.

Troubleshoot

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

- WiFi Analyzer: When this is initialized, device provides information related to air quality.
- WiFi Perf Speed Test: Provision for the user to check the speed of link connectivity, either wireless or wired.
- Connectivity: Provides different modes network reachability of Enterprise Wi-Fi AP device.
- Packet Capture: Provides feasibility for the user to capture packets on operational interfaces.
- Logs: Feasibility to check logs of different modules of Enterprise Wi-Fi AP devices which will help support and the customer to debug an issue.

Chapter 5: Configuration - System

This chapter describes the following topics:

- System
- Management
- Time settings
- Event Logging

System

Table 6 lists configurable parameters that are available under Configuration > System UI tab:

Table 6 :Configuration: System parameters

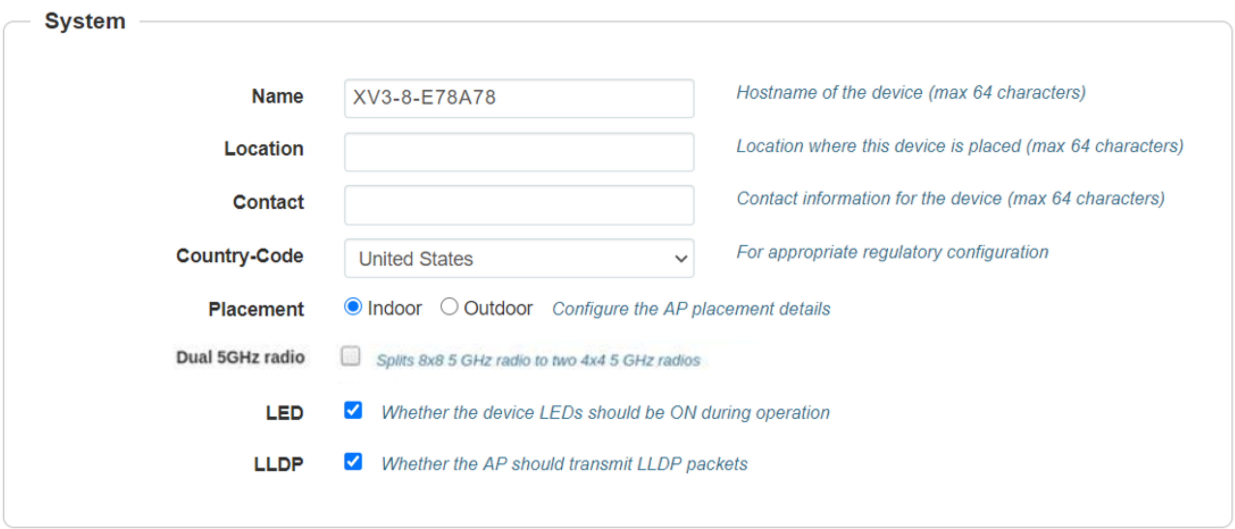
Parameter	Description	Range	Default
Name	Hostname of the device. Configurable maximum length of hostname is 64 characters.	-	Enterprise Wi-Fi AP Model Number-Last 3 Bytes of ESN
Location	The location where the device is placed. The maximum length of location is 64 characters.	-	-
Contact	Contact information for the device.	-	-
Country-Code	To be set by the administrator to the country-of-operation of the device. The allowed operating channels and the transmit power levels on those channels depends on the country of operation. Radios remain disabled unless this is set. The list of countries supported depends on the SKU of the device (FCC, ROW etc.).	-	-
Placement	Enterprise Wi-Fi AP device supports both Indoor and Outdoor deployments. Based on deployment user can configure it as follows: • Indoor When selected, only Indoor channels for country code configured will be available and operational. • Outdoor When selected, only outdoor channels for country code configured will be available and operational.	-	Indoor
Dual 5 GHz radio	Provision to enable Dual 5 GHz radio. This provides the flexibility of splitting 8x8 5 GHz radio into two 4x4 5 GHz radios.	-	Disabled

Parameter	Description	Range	Default
LED	Select the LED checkbox for the device LEDs to be ON during operation.	-	Enabled
LLDP	Provision to advertise device capabilities and information in the L2 network.	-	Enabled

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

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

Figure 6 : *Configuration: System page*



System

Name: XV3-8-E78A78 — *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: United States — *For appropriate regulatory configuration*

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

Dual 5GHz radio: □ *Splits 8x8 5 GHz radio to two 4x4 5 GHz radios*

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

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

Link Layer Discovery Protocol (LLDP)

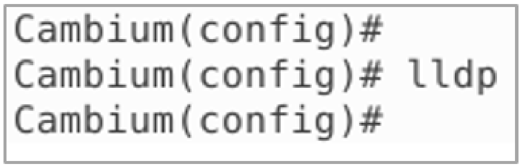
Link Layer Discovery Protocol (LLDP) is a Layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. APs can both advertise their presence by sending LLDP announcements and gather and display information sent by neighbors.

When LLDP settings are applied, power negotiation is also enabled by default. LLDP negotiates with Power over Ethernet (PoE) powered devices to allocate power.

This window allows you to establish your LLDP settings. When finished, use the Save button if you wish to make your changes permanent.

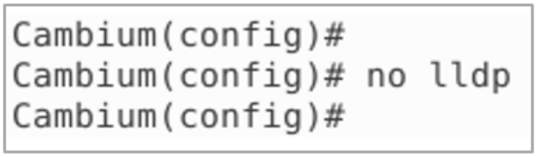
CLI Configuration

To Enable:



```
Cambium(config)#
Cambium(config)# lldp
Cambium(config)#
```

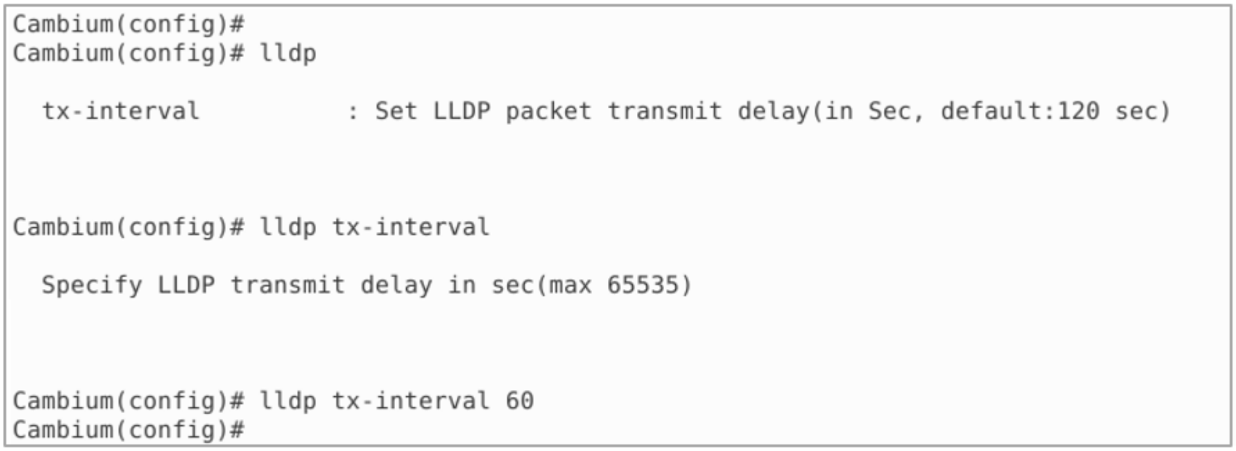
To Disable:



```
Cambium(config)#
Cambium(config)# no lldp
Cambium(config)#
```

Transmit Interval

The AP sends out LLDP announcements advertising its presence at this interval. The default is 120 seconds.



```
Cambium(config)#
Cambium(config)# lldp

  tx-interval          : Set LLDP packet transmit delay(in Sec, default:120 sec)


Cambium(config)# lldp tx-interval

  Specify LLDP transmit delay in sec(max 65535)


Cambium(config)# lldp tx-interval 60
Cambium(config)#
```

Power Negotiation

LLDP discovers a device port that supplies power to this AP (on a powered switch, for example), the AP checks that the port is able to supply the peak power that is required by this AP model. AP sends the required peak power (in watts) via LLDP packet to the PoE source, and it expects the PoE source to reply with the amount of power allocated. If the AP does not receive a response confirming that the power allocated by the PoE source is equal to or greater than the power requested, then the AP issues a Syslog message and keeps the radios down for five minutes and restarts it after that.

This provides a more graceful way of handling an underpowered situation on a Wi-Fi device. When the radios are turned off, XMS can notify you so that you don't have to hunt down an intermittent problem.

Management

Table 7 lists configurable fields that are displayed in the Configuration > System > Management tab:

Table 7 :Configuration: System > Management parameters

Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	-	admin
Telnet	Enables Telnet access to the device CLI.	-	Disabled
SSH	Enables SSH access to the device CLI.	-	Enabled
SSH Key	Provision to login to device using SSH Keys. User needs to add Public Key in this section. If configured, user has to login to AP using Private Keys. This is applicable for both CLI and GUI.	-	Disabled
HTTP	Enables HTTP access to the device UI.	-	Enabled
HTTP Port	Provision to configure HTTP port number to access device UI.	1-65535	80
HTTPS	Enables HTTPS access to the device UI.	-	Enabled
HTTPS Port	Provision to configure HTTPS port number to access device UI.	1-65535	443
RADIUS Mgmt Auth	User has provision to control login to AP using RADIUS authentication. If enabled, every credential that are provided by user undergo RADIUS authentication. If success, allowed to login to UI of AP. This is applicable for both CLI and GUI.	-	Disabled
RADIUS Server	Provision to configure RADIUS IPv4 server for Management Authentication.	-	-
RADIUS Secret	Provision to configure RADIUS shared secret for Management authentication.	-	-
cnMaestro			
Cambium Remote Mgmt.	Enables support for Cambium Remote Management of this device.	-	Enabled
Validate Server Certificate	This allows HTTPs connection between cnMaestro and Enterprise Wi-Fi AP device.	-	Enabled
cnMaestro URL	Static provision to onboard devices either using IPv4/IPv6/URL.	-	-
Cambium ID	Cambium ID used for provisioning cnMaestro (Cambium Remote Management) of this device.	-	-

Parameter	Description	Range	Default
Onboarding Key	Password used for onboarding the device to cnMaestro.	-	-
SNMP			
Enable	Provision to enable SNMPv2 or SNMPv3 support on device	-	-
SNMPv2c RO community	SNMP v2c read-only community string.	-	-
SNMPv2c RW community	SNMP v2c read-write community string.	-	-
Trap Receiver IP	Provision to configure SNMP trap receiver IPv4 server.	-	-
SNMPv3 Username	Enter username for SNMPv3.	-	-
SNMPv3 Password	Enter password for SNMPv3.	-	-
Authentication	choose Authentication type as MD5 or SHA.	-	MD5
Access	Choose Access type as RO or RW.	-	RO
Encryption	Choose ON or OFF.	-	ON

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

1. Enter the admin password of the device in the Admin Password textbox.
2. Enable the Telnet checkbox to enable telnet access to the device CLI.
3. Enable the SSH checkbox to enable SSH access to the device CLI.
    a. If certificate-based login is required, enter SSH Key in the textbox else disabled
4. Enable the HTTP checkbox to enable HTTP access to the device UI.
5. If custom port other than default is required, enter HTTP port number value for HTTP access in the textbox.
6. Enable the HTTPS checkbox to enable HTTPS access to the device UI.
7. If custom port other than default is required, enter HTTP port number value for HTTP access in the textbox.
8. If RADIUS based login is required, enable RADIUS Mgmt Auth checkbox and enter the details of RADIUS server as follows:
    a. Enter RADIUS Server parameter in the textbox.
    b. Enter RADIUS Secret parameter in the textbox.

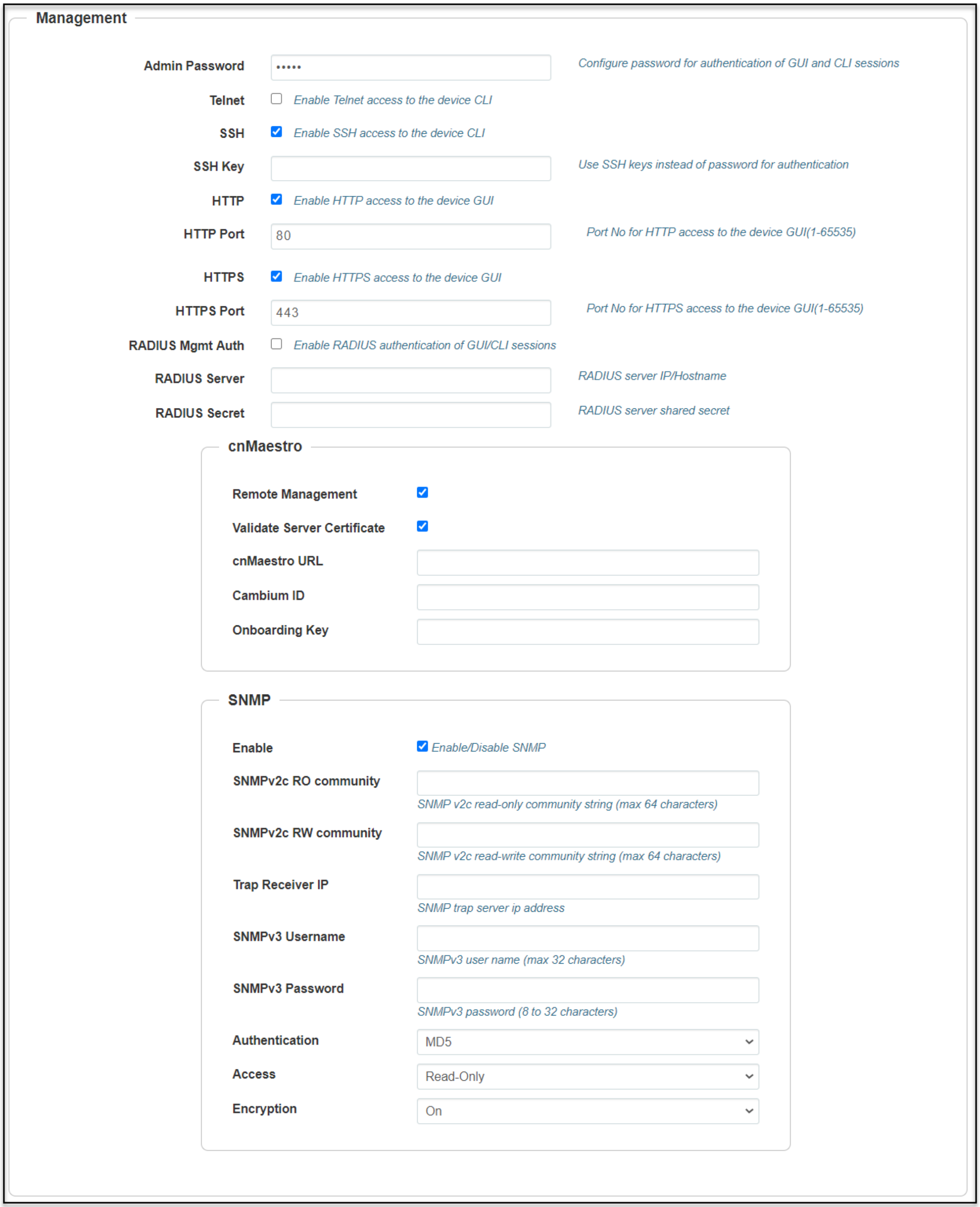
To configure cnMaestro:

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

To configure SNMP:

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

Figure 7 : *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*	
SSH Key		*Use SSH keys instead of password for authentication*
HTTP	☑ *Enable HTTP access to the device GUI*	
HTTP Port	80	*Port No for HTTP access to the device GUI(1-65535)*
HTTPS	☑ *Enable HTTPS access to the device GUI*	
HTTPS Port	443	*Port No for HTTPS access to the device GUI(1-65535)*
RADIUS Mgmt Auth	□ *Enable RADIUS authentication of GUI/CLI sessions*	
RADIUS Server		*RADIUS server IP/Hostname*
RADIUS Secret		*RADIUS server shared secret*

cnMaestro

Remote Management	☑
Validate Server Certificate	☑
cnMaestro URL	
Cambium ID	
Onboarding Key	

SNMP

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

Time settings

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

Table 8 lists the fields that are displayed in the Configuration > System > Time Settings section:

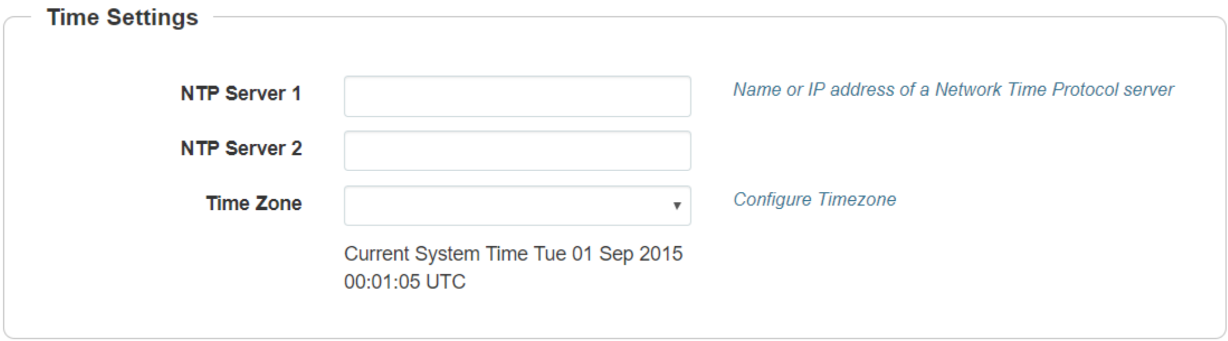
Table 8 :Configuration: System > Time Settings parameters

Parameter	Description	Range	Default
NTP Server 1	Name or IPv4 address of a Network Time Protocol server 1.	-	-
NTP Server 2	Name or IPv4 address of a Network Time Protocol server 2.	-	-
Time zone	**Note** Accurate time on the AP is critical for features such as WLAN Scheduled Access, Syslogs etc. Time zone can be set according to the location where the AP is installed. By selecting the appropriate time zone from the drop-down list, ensures that the device clock is synced with the wall clock time.	-	-

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

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

Figure 8 : *Configuration: Time settings page*



Time Settings

NTP Server 1		*Name or IP address of a Network Time Protocol server*
NTP Server 2		
Time Zone	▾	*Configure Timezone*

Current System Time Tue 01 Sep 2015 00:01:05 UTC

Event Logging

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

Table 9 lists the fields that are displayed in the **Configuration > System > Event Logging** section.

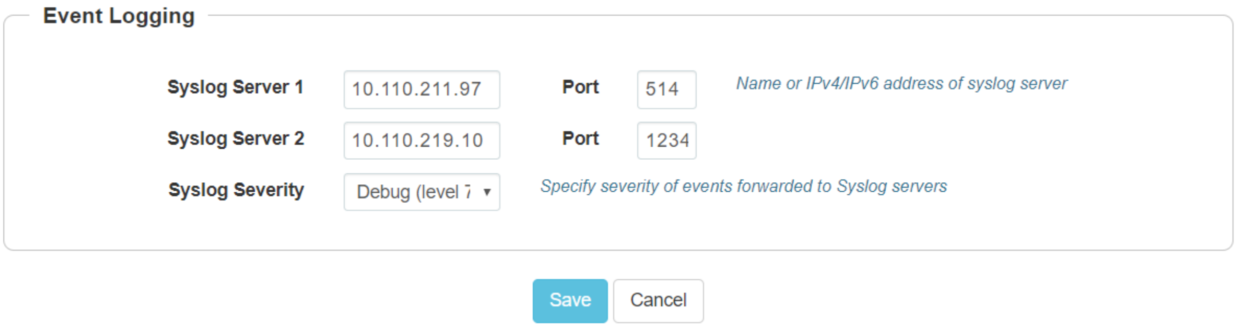
Table 9 :Configuration: System > Event Logging parameters

Parameter	Description	Range	Default
Syslog Server 1	Hostname or IPv4/IPv6 address of the Syslog server and respective port number.	-	514
Syslog Server 2	Hostname or IPv4/IPv6 address of the Syslog server and respective port number.	-	514
Syslog Severity	Provision to configure severity of Logs that must be forwarded to the server. The Log levels supported are as per RFC.	-	Debug

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

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

Figure 9 : *Configuration: Event Logging page*



Event Logging

Syslog Server 1: 10.110.211.97 Port: 514 *Name or IPv4/IPv6 address of syslog server*

Syslog Server 2: 10.110.219.10 Port: 1234

Syslog Severity: Debug (level 7 *Specify severity of events forwarded to Syslog servers*

Maximum of two Syslog servers can be configured on Enterprise Wi-Fi AP device. Events are sent to both configured Syslog servers if they are up and running.

Chapter 6: Filter Management

Filters are used to define the rules used for blocking or passing traffic and also to change QoS/DSCP and rate limiting for selected traffic.

The Wireless AP's integrated firewall uses stateful inspection to accelerate the decision of whether to allow or deny traffic user connections managed by the firewall are maintained statefully. Once user flow is established through the AP, it is recognized and passes through without application of all defined filtering rules. Stateful inspection runs automatically on the AP.

Filter List

Filters are organized in groups, called Filter Lists. A filter list allows user to apply a uniform set of filters to SSIDs. AP supports 16 filter list and each filter list supports 50 Filter rules in precedence order.

Filters

These settings create and manage filters with precedence that belong to the current filter list, based on the filter criteria you specify.

Filters can be configured in Layer2 and Layer 3 or application/category control (Layer 7). Layer 2 rule taking high precedence over Layer 3 application control and Layer 2 support MAC/IP/protocol-based rules.

Filters are an especially powerful feature when combined with the intelligence provided by the "Application Control Windows".

Based on Application Control's analysis of your wireless traffic, you can create filters to enhance wireless usage for your business needs:

1. Usage of non-productive and risky applications like BitTorrent can be restricted.
2. Traffic for mission-critical applications like VoIP and WebEx may be given higher priority (QoS).
3. Non- critical traffic from applications like YouTube may be given lower priority (QoS) or bandwidth allowed may be capped per station or for all stations.

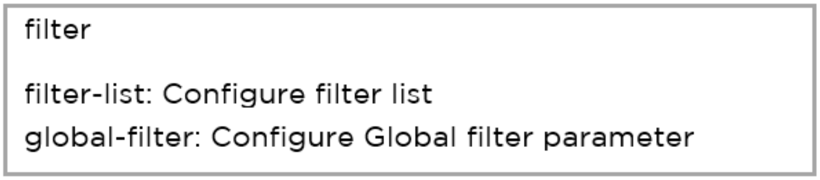
Note

The Air Cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic. Air Cleaner can be configured from XMS. For more information, please refer to latest XMS-Cloud Help document.

Configuring Filter CLI

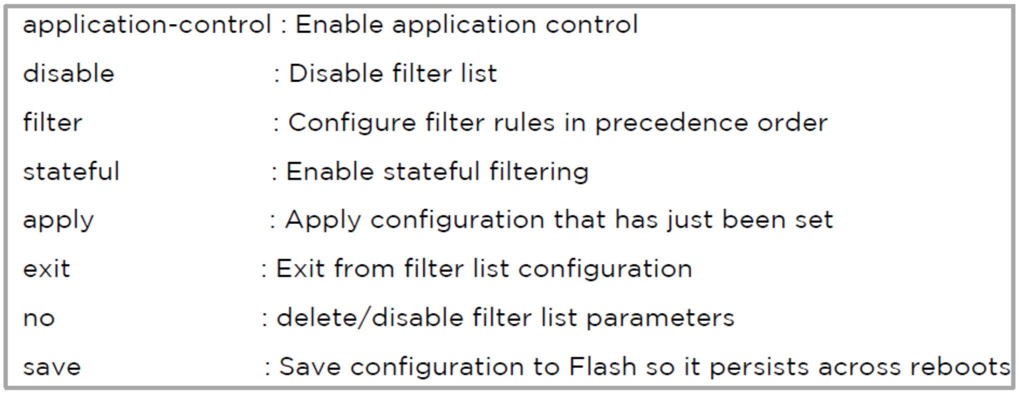
By configuring Filter CLI, user can define rules for blocking or passing traffic (ACL) or /DSCP/QoS level and rate limiting for selected traffic.

1. Create filter list/filter profile using global filter command (Filter: configure filter parameters).



```
filter

filter-list: Configure filter list
global-filter: Configure Global filter parameter
```

2. Global-filter is for global rules in AP. Global-filter include below options.



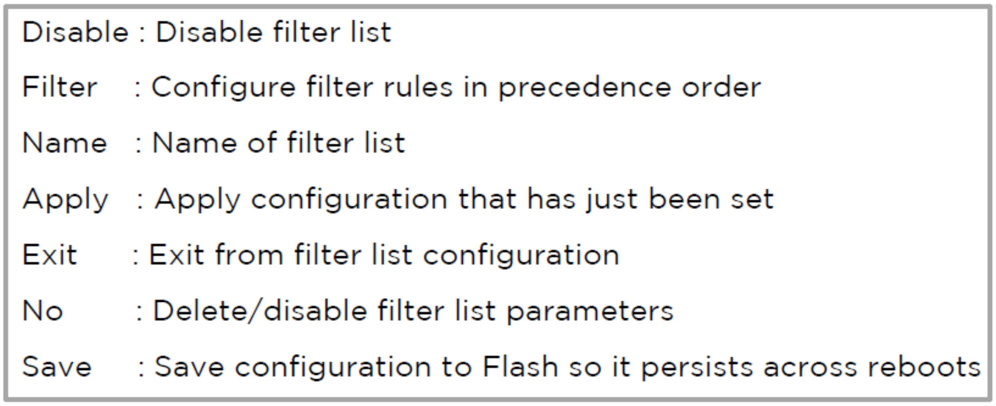
```
application-control : Enable application control
disable              : Disable filter list
filter               : Configure filter rules in precedence order
stateful             : Enable stateful filtering
apply                : Apply configuration that has just been set
exit                : Exit from filter list configuration
no                  : delete/disable filter list parameters
save                 : Save configuration to Flash so it persists across reboots
```

Stateful Filtering: Stateful operation of the integrated firewall can be Enabled or Disabled. By default, it is enabled.

Application Control: Operation of the Application Control feature may be Enabled or Disabled.

Disable: Disable or enable filter list.

3. Each filter list includes below options:



```
Disable : Disable filter list
Filter   : Configure filter rules in precedence order
Name     : Name of filter list
Apply    : Apply configuration that has just been set
Exit     : Exit from filter list configuration
No       : Delete/disable filter list parameters
Save     : Save configuration to Flash so it persists across reboots
```

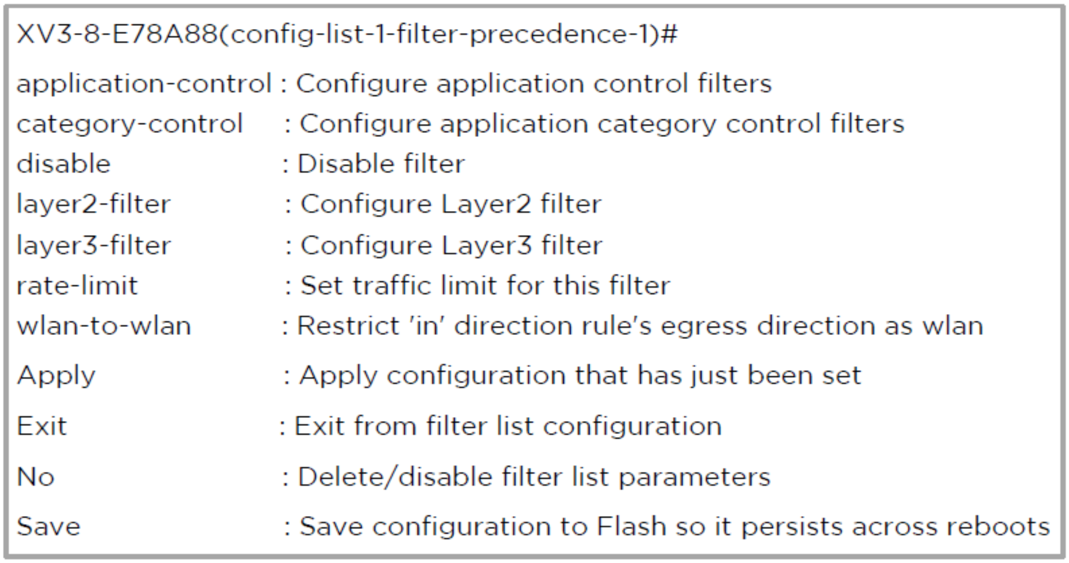
Note

Global-filter rules will take precedence over filter-list rules

- Global filter and filter-list can include 50 filter rules with precedence order.

  XV3-8-E78A88(config-filter-list-1)# filter precedence {1-50}

4. Then create filter rule from precedence level (1 to 50).

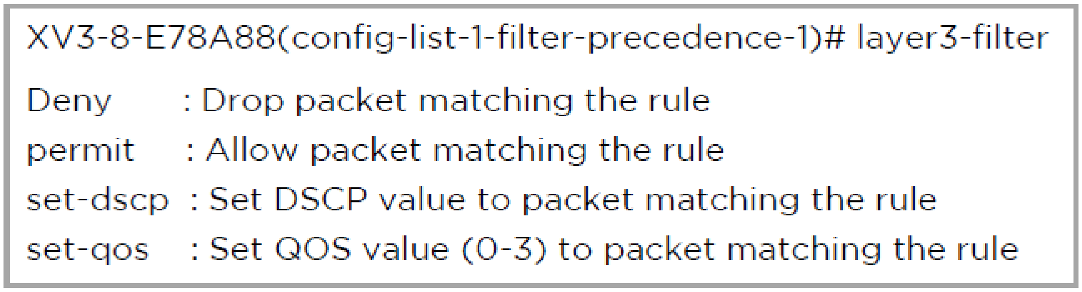


```
XV3-8-E78A88(config-list-1-filter-precedence-1)#
application-control : Configure application control filters
category-control     : Configure application category control filters
disable              : Disable filter
layer2-filter        : Configure Layer2 filter
layer3-filter        : Configure Layer3 filter
rate-limit           : Set traffic limit for this filter
wlan-to-wlan         : Restrict 'in' direction rule's egress direction as wlan
Apply                : Apply configuration that has just been set
Exit                 : Exit from filter list configuration
No                   : Delete/disable filter list parameters
Save                 : Save configuration to Flash so it persists across reboots
```

Note

Filter type is either layer3 or layer 2 or application control can be added in one precedence level.

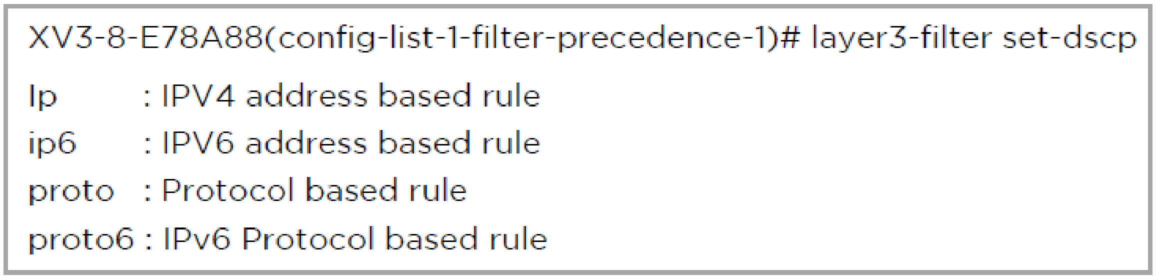
5. Layer3 filter has the below provisions.



```
XV3-8-E78A88(config-list-1-filter-precedence-1)# layer3-filter
Deny      : Drop packet matching the rule
permit    : Allow packet matching the rule
set-dscp  : Set DSCP value to packet matching the rule
set-qos   : Set QOS value (0-3) to packet matching the rule
```

a. QoS: Set packets QoS level (0 to 3). Level 0 has the lowest priority; level 3 has the highest priority
b. DSCP: Differentiated Services Code Point or DiffServ (DSCP). DSCP level (0 to 63. Level 0 has the lowest priority and level 63 has the highest priority.
c. Rate limit: Filters support rate limiting per station or all stations and support Kbps/Mbps/pps.
d. Disable: Each filter and filter list can be turned on/off.

6. Each layer 3 rule category has below types



```
XV3-8-E78A88(config-list-1-filter-precedence-1)# layer3-filter set-dscp
Ip      : IPV4 address based rule
ip6     : IPV6 address based rule
proto   : Protocol based rule
proto6 : IPv6 Protocol based rule
```

7. For proto or port number-based rule, select proto or proto6 (for IPv6).

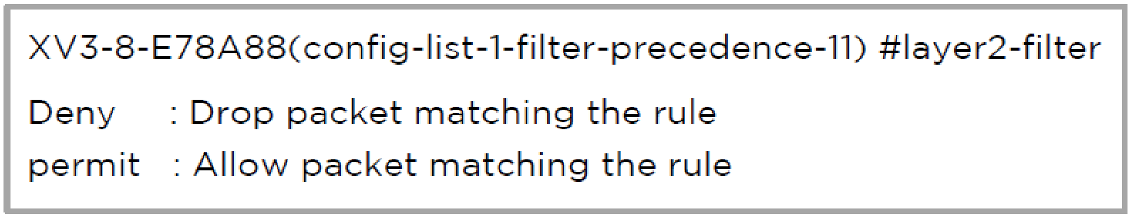
```
XV3-8-E78A88(config-list-1-filter-precedence-1)# layer3-filter set-dscp proto
layer3-filter set-dscp proto (tcp|udp|icmp|igmp|srp|sctp|any) (SOURCE-IP{/{mask|prefix-length}}|any)
(SOURCE-PORT|any) (DESTINATION-IP{/{mask|prefix-length}}|any) (DESTINATION-PORT|any) (in|out|any)
(DSCP{0-63}) <(optional)//Filter_name>
```

> **Note**
>
> All fields are mandatory. If no parameter to configure, give 'any'. Direction is direction of rule. if it is 'in', rule applicable for traffic from wireless side. If it is 'out', rule applicable for traffic to wireless.

8. For non proto or port number-based rule, select IP/IP6 (for IPv6).

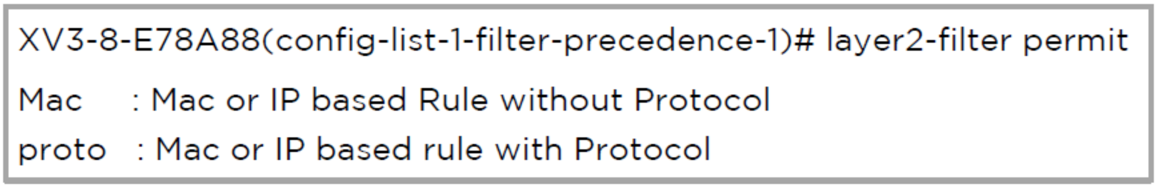
```
XV3-8-E78A88(config-list-1-filter-precedence-1)# layer3-filter set-dscp ip
layer3-filter set-dscp ip (SOURCE-IP{/{mask|prefix-length}}|any) (DESTINATION-IP{/{mask|/prefix-
length}}|any) (in|out|any) (DSCP{0-63}) <(optional)//Filter_name>
```

9. Layer 2 filter has below options:



```
XV3-8-E78A88(config-list-1-filter-precedence-11) #layer2-filter
Deny     : Drop packet matching the rule
permit   : Allow packet matching the rule
```

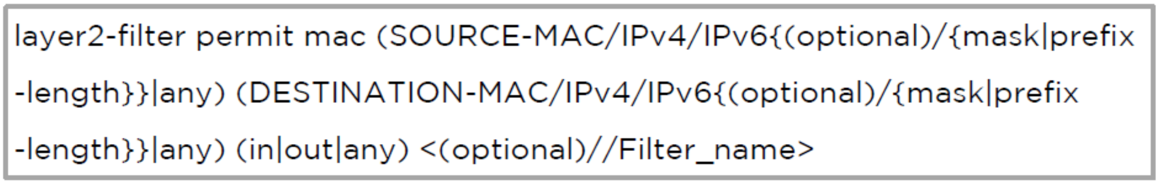
10. Each layer 2 rule category has below two cases.



```
XV3-8-E78A88(config-list-1-filter-precedence-1)# layer2-filter permit
Mac     : Mac or IP based Rule without Protocol
proto   : Mac or IP based rule with Protocol
```

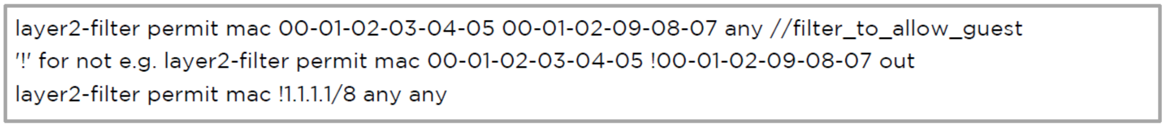
Layer 2 rule support IP, MAC, Port or Protocol-based rules.

11. XV3-8-E78A88 (config-list-1-filter-precedence-1) # layer2-filter permit mac



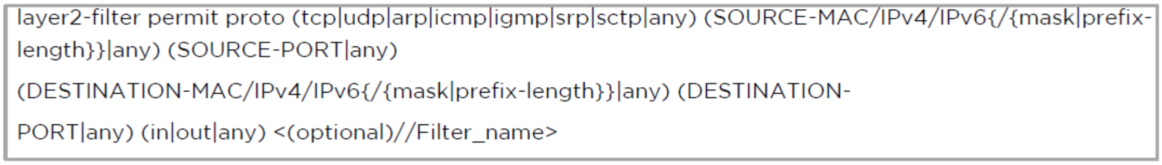
```
layer2-filter permit mac (SOURCE-MAC/IPv4/IPv6{(optional)/{mask|prefix
-length}}|any) (DESTINATION-MAC/IPv4/IPv6{(optional)/{mask|prefix
-length}}|any) (in|out|any) <(optional)//Filter_name>
```

Example:



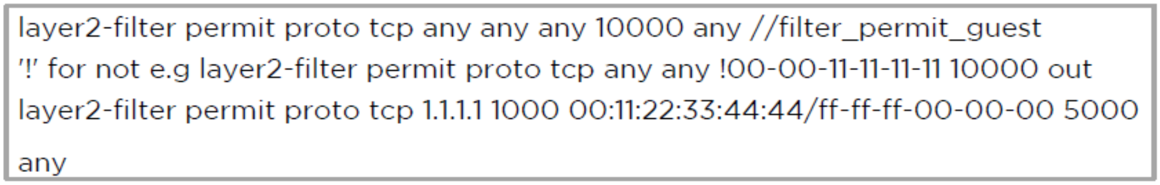
```
layer2-filter permit mac 00-01-02-03-04-05 00-01-02-09-08-07 any //filter_to_allow_guest
'!' for not e.g. layer2-filter permit mac 00-01-02-03-04-05 !00-01-02-09-08-07 out
layer2-filter permit mac !1.1.1.1/8 any any
```

12. XV3-8-E78A88 (config-list-1-filter-precedence-1) # layer2-filter permit proto



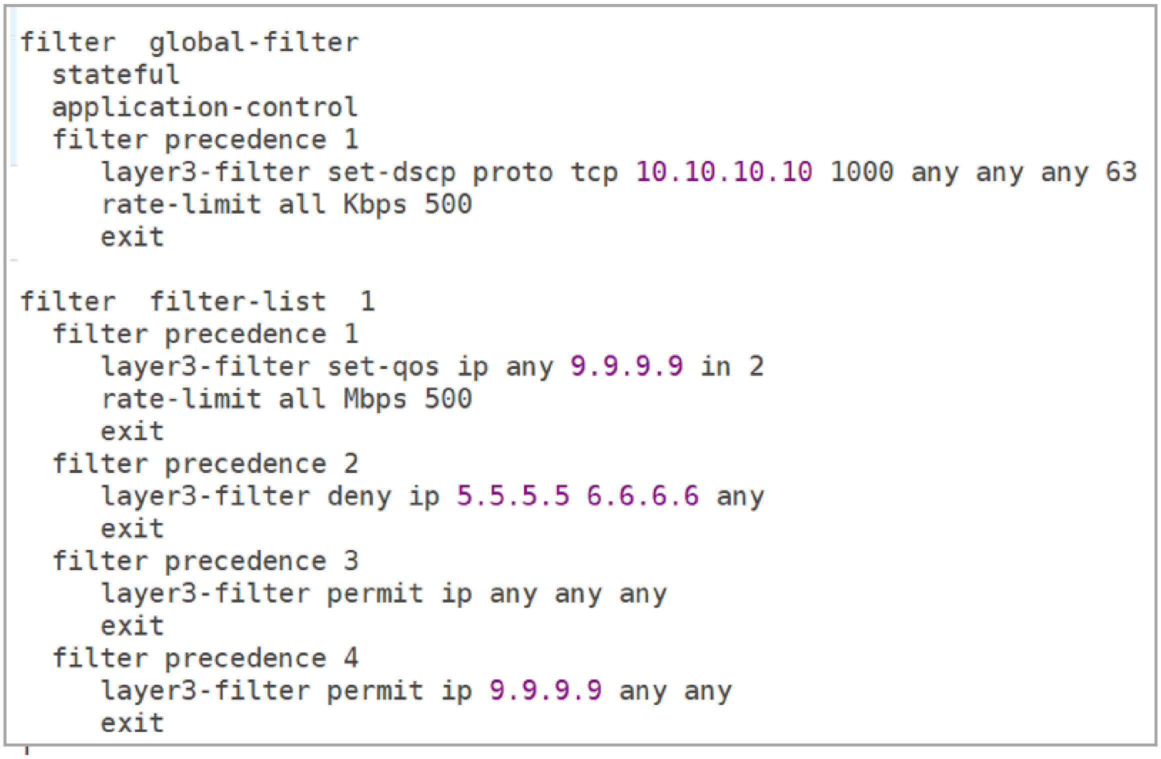
```
layer2-filter permit proto (tcp|udp|arp|icmp|igmp|srp|sctp|any) (SOURCE-MAC/IPv4/IPv6{/{mask|prefix-
length}}|any) (SOURCE-PORT|any)
(DESTINATION-MAC/IPv4/IPv6{/{mask|prefix-length}}|any) (DESTINATION-
PORT|any) (in|out|any) <(optional)//Filter_name>
```

Example



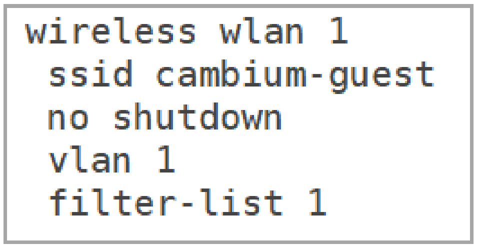
```
layer2-filter permit proto tcp any any any 10000 any //filter_permit_guest
'!' for not e.g layer2-filter permit proto tcp any any !00-00-11-11-11-11 10000 out
layer2-filter permit proto tcp 1.1.1.1 1000 00:11:22:33:44:44/ff-ff-ff-00-00-00 5000
any
```

Sample configuration



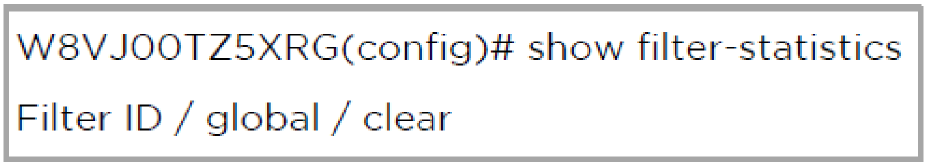
```
filter  global-filter
  stateful
  application-control
  filter precedence 1
     layer3-filter set-dscp proto tcp 10.10.10.10 1000 any any any 63
     rate-limit all Kbps 500
     exit

filter  filter-list  1
  filter precedence 1
     layer3-filter set-qos ip any 9.9.9.9 in 2
     rate-limit all Mbps 500
     exit
  filter precedence 2
     layer3-filter deny ip 5.5.5.5 6.6.6.6 any
     exit
  filter precedence 3
     layer3-filter permit ip any any any
     exit
  filter precedence 4
     layer3-filter permit ip 9.9.9.9 any any
     exit
```

13. In order to attach filter list into WLAN profile, filter-list < filter-list ID>.



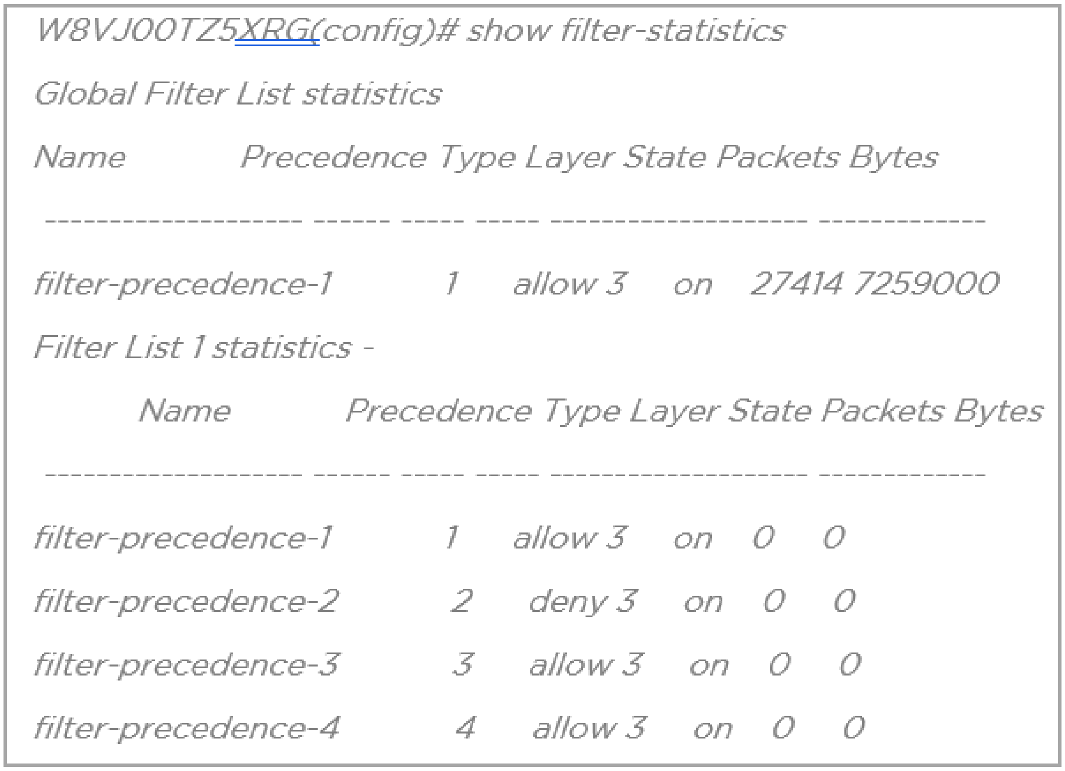
```
wireless wlan 1
 ssid cambium-guest
 no shutdown
 vlan 1
 filter-list 1
```

14. To show filter statistics:



```
W8VJ00TZ5XRG(config)# show filter-statistics

Filter ID / global / clear
```

Example



```
W8VJ00TZ5XRG(config)# show filter-statistics

Global Filter List statistics

Name          Precedence Type Layer State Packets Bytes

 -------------------- ------ ----- ----- -------------------- -------------

filter-precedence-1         1     allow 3     on    27414 7259000

Filter List 1 statistics -

        Name          Precedence Type Layer State Packets Bytes

 -------------------- ------ ----- ----- -------------------- -------------

filter-precedence-1         1     allow 3     on     0     0

filter-precedence-2          2     deny 3     on     0     0

filter-precedence-3          3     allow 3     on     0     0

filter-precedence-4          4     allow 3     on     0     0
```

Application Control

Note

This feature is only available if the AP license includes Application Control. For more information, refer About Licensing and Upgrades section in XIRRUS Wireless Access Point User Guide.

- For XMS-Cloud, this feature is available with the base package (No license required).
- For cnMaestro, this feature is available only with cnMaestro pro.

The Application Control feature provides real-time visibility of application usage by users across the wireless network. Network usage has changed enormously in the last few years, with the increase in smartphone and tablet usage stressing networks. Increasing traffic from legitimate business needs such as cloud- and web-based applications, streaming media, and VoIP must be handled with an adequate quality of experience. To achieve this purpose Application Control filters are used to define the rules used for blocking or passing and change QoS/DSCP and rate-limiting for the specific Application or a specific category of application. For more details, refer the Application Control Filters section in the user guide

Application Control can track application usage over time to monitor trends. Usage may be tracked by AP, VLAN, or station. Many hundreds of applications are recognized and grouped into a number of categories. The distributed architecture of Cambium Enterprise APs allows Application Control to scale naturally as you grow the network.

Deep Packet Inspection (DPI)

The AP uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productiveness. Filters can be used to implement per-application policies that keep network usage focused on productive uses.

Application Control Policy

When you find risky or unproductive applications consuming bandwidth on the network, you can easily create Filters to control them. You may use filters to:

- Block problematic traffic, such as BitTorrent or Y8.
- Prioritize mission critical traffic: By increasing the QoS assigned to the traffic, applications like VoIP and WebEx may be given higher priority (QoS).
- Lower the priority of less productive traffic: Use filters to decrease the QoS assigned to traffic for applications like YouTube and Facebook.
- A nonproductive specific application can be rate limited to avoid impact on the productive application. (E.g.: YouTube streaming can be rate limited to avoid impact on applications like VoIP)

Risk and Productivity

Application Control ranks applications in terms of their levels of risk and productivity.

Productivity: Indicates how appropriate an application is useful for business purposes. The higher the rating number, the more business-oriented an application is:

1. Primarily recreational
2. Mostly recreational
3. Combination of business and recreational purposes
4. Mainly used for business
5. Primarily used for business

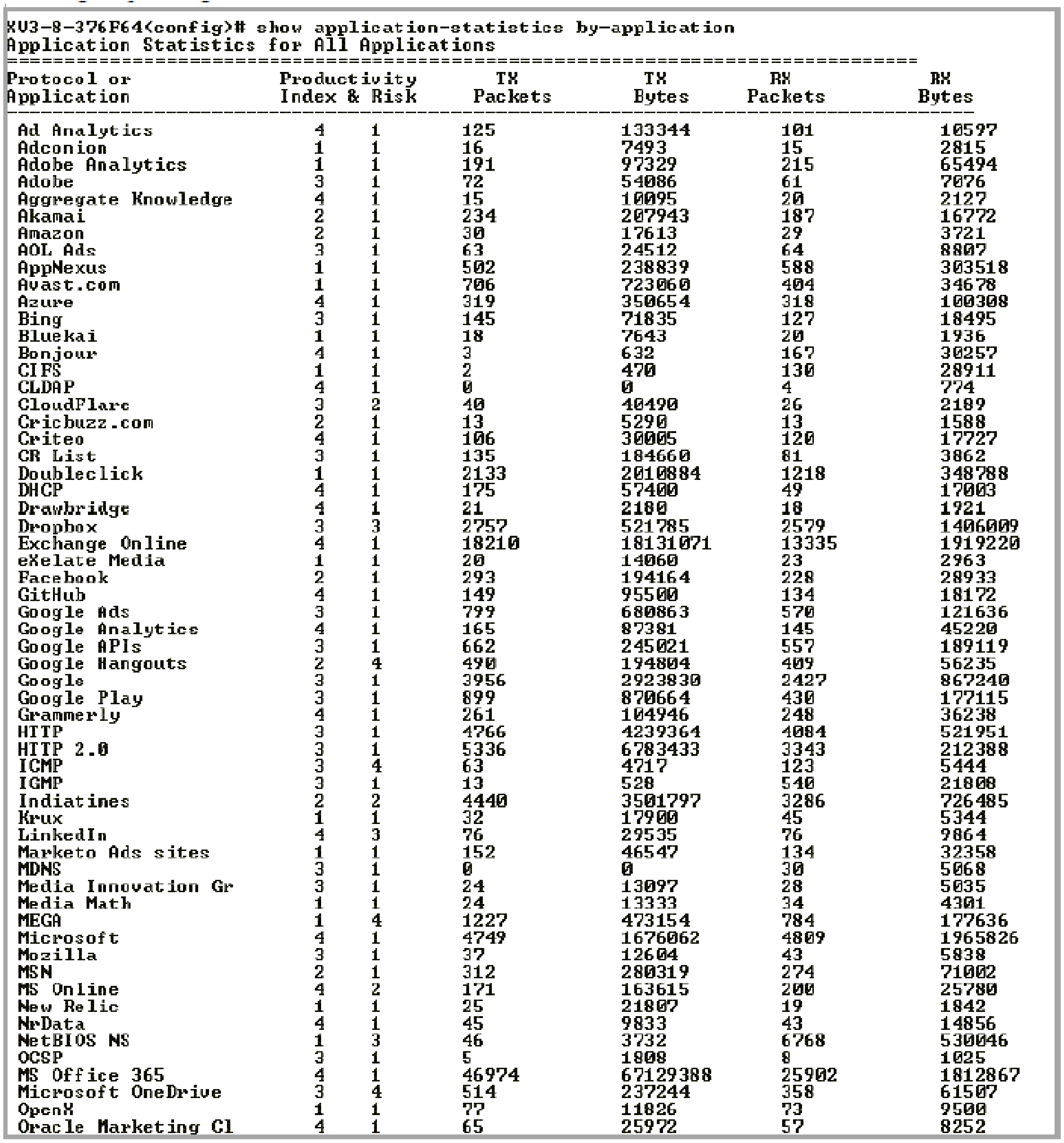
Risk: indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the more risky of an application is:

1. No threat
2. Minimal threat
3. Some risk: maybe misused
4. High risk: maybe malware or allow data leaks
5. Very high risk: threat circumvents firewalls or avoids detection

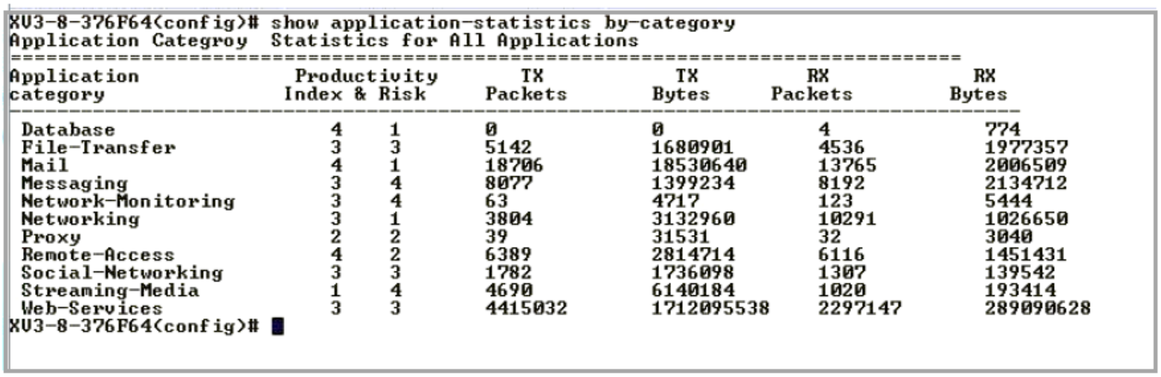
Selection Criteria

From AP CLI, below options are available to view the Application Statistics:

- By Application: This gives detailed information about the application seen from the wireless traffic.
- By Category: This gives the combined statistics of the application which belongs to a particular category (E.g. Games, Network monitor etc.).

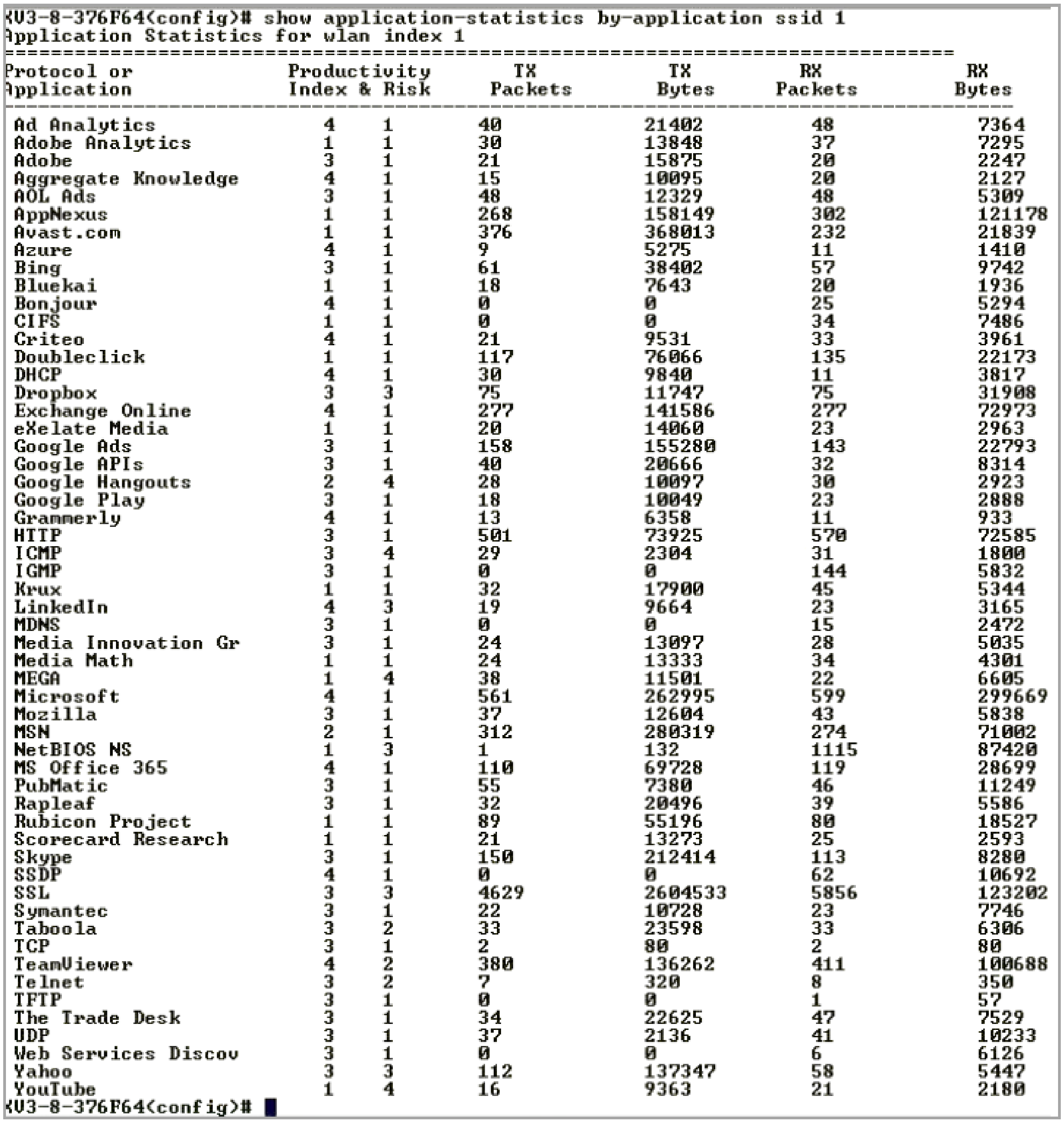


```
XV3-8-376F64(config)# show application-statistics by-application
Application Statistics for All Applications
================================================================================
Protocol or             Productivity       TX           TX         RX            RX
Application             Index & Risk     Packets      Bytes    Packets        Bytes
-------------------------------------------------------------------------------------
 Ad Analytics              4    1       125           133344        101           10597
 Adconion                  1    1       16            7493          15            2815
 Adobe Analytics           1    1       191           97329         215           65494
 Adobe                     3    1       72            54086         61            7076
 Aggregate Knowledge       4    1       15            10095         20            2127
 Akamai                    2    1       234           207943        187           16772
 Amazon                    2    1       30            17613         29            3721
 AOL Ads                   3    1       63            24512         64            8807
 AppNexus                  1    1       502           238839        588           303518
 Avast.com                 1    1       706           723060        404           34678
 Azure                     4    1       319           350654        318           100308
 Bing                      3    1       145           71835         127           18495
 Bluekai                   1    1       18            7643          20            1936
 Bonjour                   4    1       3             632           167           30257
 CIFS                      1    1       2             470           130           28911
 CLDAP                     4    1       0             0             4             774
 CloudFlare                3    2       40            40490         26            2189
 Cricbuzz.com              2    1       13            5290          13            1588
 Criteo                    4    1       106           30005         120           17727
 CR List                   3    1       135           184660        81            3862
 Doubleclick               1    1       2133          2010884       1218          348788
 DHCP                      4    1       175           57400         49            17003
 Drawbridge                4    1       21            2180          18            1921
 Dropbox                   3    3       2757          521785        2579          1406009
 Exchange Online           4    1       18210         18131071      13335         1919220
 eXelate Media             1    1       20            14060         23            2963
 Facebook                  2    1       293           194164        228           28933
 GitHub                    4    1       149           95500         134           18172
 Google Ads                3    1       799           680863        570           121636
 Google Analytics          4    1       165           87381         145           45220
 Google APIs               3    1       662           245021        557           189119
 Google Hangouts           2    4       490           194804        409           56235
 Google                    3    1       3956          2923830       2427          867240
 Google Play               3    1       899           870664        430           177115
 Grammerly                 4    1       261           104946        248           36238
 HTTP                      3    1       4766          4239364       4084          521951
 HTTP 2.0                  3    1       5336          6783433       3343          212388
 ICMP                      3    4       63            4717          123           5444
 IGMP                      3    1       13            528           540           21808
 Indiatimes                2    2       4440          3501797       3286          726485
 Krux                      1    1       32            17900         45            5344
 LinkedIn                  4    3       76            29535         76            9864
 Marketo Ads sites         1    1       152           46547         134           32358
 MDNS                      3    1       0             0             30            5068
 Media Innovation Gr       3    1       24            13097         28            5035
 Media Math                1    1       24            13333         34            4301
 MEGA                      1    4       1227          473154        784           177636
 Microsoft                 4    1       4749          1676062       4809          1965826
 Mozilla                   3    1       37            12604         43            5838
 MSN                       2    1       312           280319        274           71002
 MS Online                 4    2       171           163615        200           25780
 New Relic                 1    1       25            21807         19            1842
 NrData                    4    1       45            9833          43            14856
 NetBIOS NS                1    3       46            3732          6768          530046
 OCSP                      3    1       5             1808          8             1025
 MS Office 365             4    1       46974         67129388      25902         1812867
 Microsoft OneDrive        3    4       514           237244        358           61507
 OpenX                     1    1       77            11826         73            9500
 Oracle Marketing Cl       4    1       65            25972         57            8252
```



```
XV3-8-376F64(config)# show application-statistics by-category
Application Categroy  Statistics for All Applications
================================================================================
Application              Productivity      TX            TX          RX            RX
category                Index & Risk     Packets       Bytes      Packets        Bytes
-----------------------------------------------------------------------------------------
 Database                   4    1       0             0             4             774
 File-Transfer              3    3       5142          1680901       4536          1977357
 Mail                       4    1       18706         18530640      13765         2006509
 Messaging                  3    4       8077          1399234       8192          2134712
 Network-Monitoring         3    4       63            4717          123           5444
 Networking                 3    1       3804          3132960       10291         1026650
 Proxy                      2    2       39            31531         32            3040
 Remote-Access              4    2       6389          2814714       6116          1451431
 Social-Networking          3    3       1782          1736098       1307          139542
 Streaming-Media            1    4       4690          6140184       1020          193414
 Web-Services               3    3       4415032       1712095538    2297147       289090628
XV3-8-376F64(config)# █
```

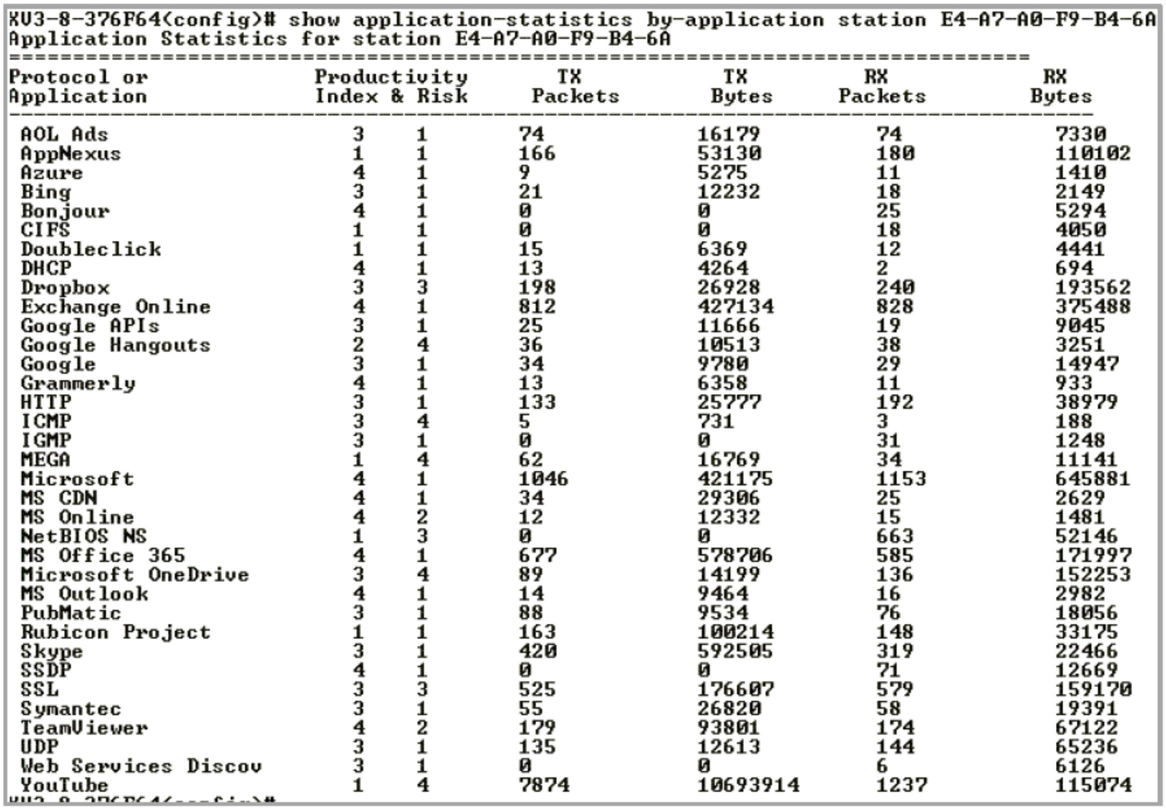
- By SSID: This gives the application list seen on particular SSID. The SSID number is the BSS index configured.



```
XV3-8-376F64(config)# show application-statistics by-application ssid 1
Application Statistics for wlan index 1
================================================================================
Protocol or             Productivity     TX           TX        RX           RX
Application             Index & Risk   Packets       Bytes    Packets       Bytes
-------------------------------------------------------------------------------
 Ad Analytics               4    1      40           21402       48          7364
 Adobe Analytics            1    1      30           13848       37          7295
 Adobe                      3    1      21           15875       20          2247
 Aggregate Knowledge        4    1      15           10095       20          2127
 AOL Ads                    3    1      48           12329       48          5309
 AppNexus                   1    1      268          158149      302         121178
 Avast.com                  1    1      376          368013      232         21839
 Azure                      4    1      9            5275        11          1410
 Bing                       3    1      61           38402       57          9742
 Bluekai                    1    1      18           7643        20          1936
 Bonjour                    4    1      0            0           25          5294
 CIFS                       1    1      0            0           34          7486
 Criteo                     4    1      21           9531        33          3961
 Doubleclick                1    1      117          76066       135         22173
 DHCP                       4    1      30           9840        11          3817
 Dropbox                    3    3      75           11747       75          31908
 Exchange Online            4    1      277          141586      277         72973
 eXelate Media              1    1      20           14060       23          2963
 Google Ads                 3    1      158          155280      143         22793
 Google APIs                3    1      40           20666       32          8314
 Google Hangouts            2    4      28           10097       30          2923
 Google Play                3    1      18           10049       23          2888
 Grammerly                  4    1      13           6358        11          933
 HTTP                       3    1      501          73925       570         72585
 ICMP                       3    4      29           2304        31          1800
 IGMP                       3    1      0            0           144         5832
 Krux                       1    1      32           17900       45          5344
 LinkedIn                   4    3      19           9664        23          3165
 MDNS                       3    1      0            0           15          2472
 Media Innovation Gr        3    1      24           13097       28          5035
 Media Math                 1    1      24           13333       34          4301
 MEGA                       1    4      38           11501       22          6605
 Microsoft                  4    1      561          262995      599         299669
 Mozilla                    3    1      37           12604       43          5838
 MSN                        2    1      312          280319      274         71002
 NetBIOS NS                 1    3      1            132         1115        87420
 MS Office 365              4    1      110          69728       119         28699
 PubMatic                   3    1      55           7380        46          11249
 Rapleaf                    3    1      32           20496       39          5586
 Rubicon Project            1    1      89           55196       80          18527
 Scorecard Research         1    1      21           13273       25          2593
 Skype                      3    1      150          212414      113         8280
 SSDP                       4    1      0            0           62          10692
 SSL                        3    3      4629         2604533     5856        123202
 Symantec                   3    1      22           10728       23          7746
 Taboola                    3    2      33           23598       33          6306
 TCP                        3    1      2            80          2           80
 TeamViewer                 4    2      380          136262      411         100688
 Telnet                     3    2      7            320         8           350
 TFTP                       3    1      0            0           1           57
 The Trade Desk             3    1      34           22625       47          7529
 UDP                        3    1      37           2136        41          10233
 Web Services Discov        3    1      0            0           6           6126
 Yahoo                      3    3      112          137347      58          5447
 YouTube                    1    4      16           9363        21          2180
XV3-8-376F64(config)# █
```

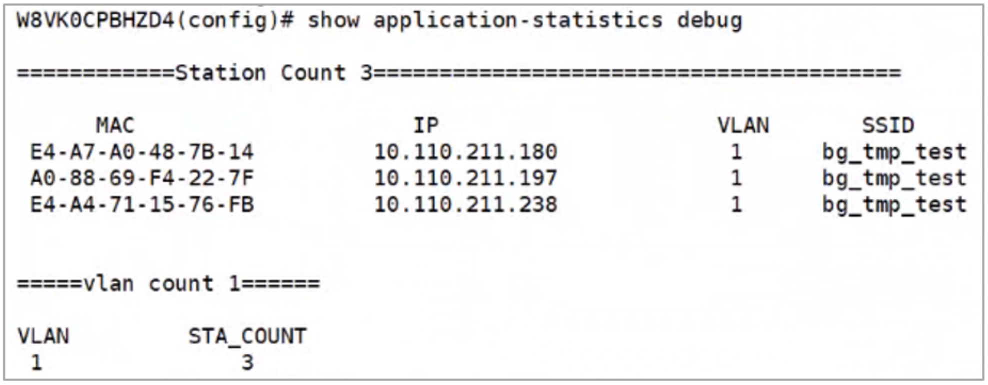
- Display for Station: This gives detailed information about a particular station. Provide the station MAC address the user want to check for statistics.

- Tx means downlink traffic with respect to AP and Rx means uplink traffic with respect to AP.



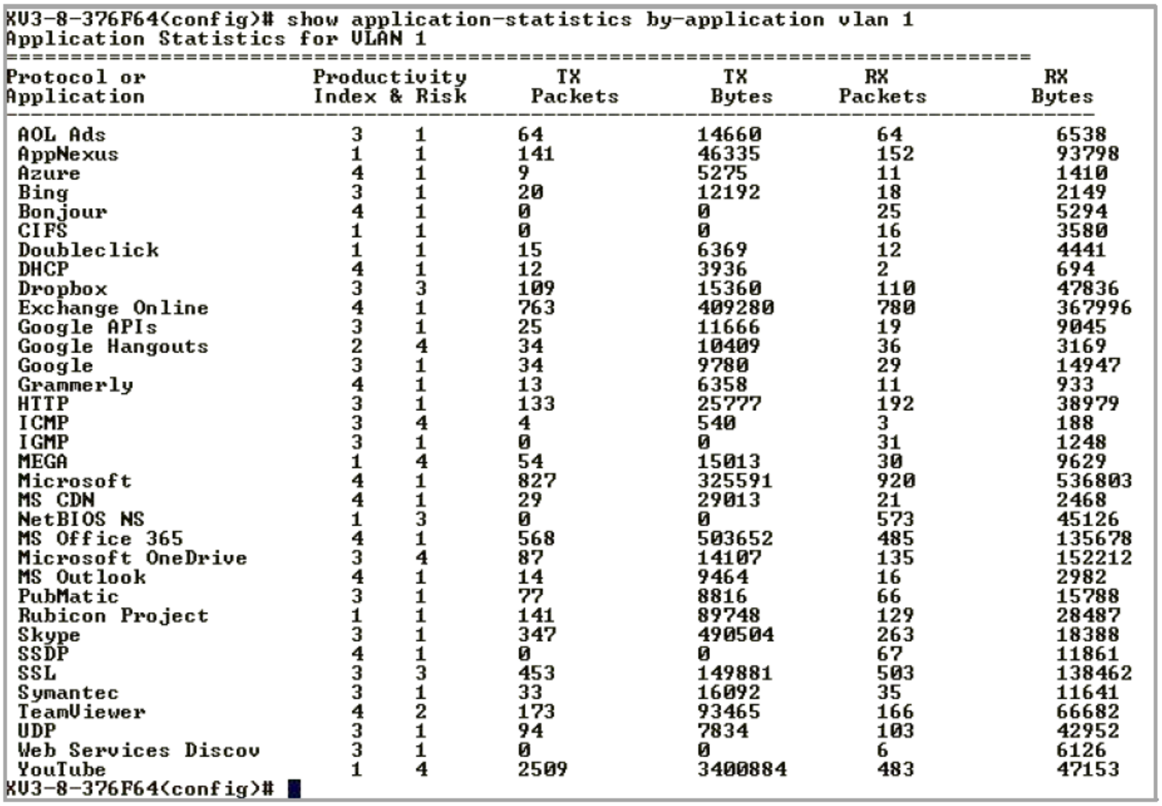
```
XV3-8-376F64(config)# show application-statistics by-application station E4-A7-A0-F9-B4-6A
Application Statistics for station E4-A7-A0-F9-B4-6A
===============================================================================
Protocol or             Productivity      TX           TX         RX             RX
Application             Index & Risk    Packets       Bytes     Packets        Bytes
------------------------------------------------------------------------------------
 AOL Ads                   3    1      74            16179         74            7330
 AppNexus                  1    1      166           53130         180           110102
 Azure                     4    1      9             5275          11            1410
 Bing                      3    1      21            12232         18            2149
 Bonjour                   4    1      0             0             25            5294
 CIFS                      1    1      0             0             18            4050
 Doubleclick               1    1      15            6369          12            4441
 DHCP                      4    1      13            4264          2             694
 Dropbox                   3    3      198           26928         240           193562
 Exchange Online           4    1      812           427134        828           375488
 Google APIs               3    1      25            11666         19            9045
 Google Hangouts           2    4      36            10513         38            3251
 Google                    3    1      34            9780          29            14947
 Grammerly                 4    1      13            6358          11            933
 HTTP                      3    1      133           25777         192           38979
 ICMP                      3    4      5             731           3             188
 IGMP                      3    1      0             0             31            1248
 MEGA                      1    4      62            16769         34            11141
 Microsoft                 4    1      1046          421175        1153          645881
 MS CDN                    4    1      34            29306         25            2629
 MS Online                 4    2      12            12332         15            1481
 NetBIOS NS                1    3      0             0             663           52146
 MS Office 365             4    1      677           578706        585           171997
 Microsoft OneDrive        3    4      89            14199         136           152253
 MS Outlook                4    1      14            9464          16            2982
 PubMatic                  3    1      88            9534          76            18056
 Rubicon Project           1    1      163           100214        148           33175
 Skype                     3    1      420           592505        319           22466
 SSDP                      4    1      0             0             71            12669
 SSL                       3    3      525           176607        579           159170
 Symantec                  3    1      55            26820         58            19391
 TeamViewer                4    2      179           93801         174           67122
 UDP                       3    1      135           12613         144           65236
 Web Services Discov       3    1      0             0             6             6126
 YouTube                   1    4      7874          10693914      1237          115074
XV3-8-376F64(config)#
```

Below CLI command gives list of stations present along with station count per VLAN.



```
W8VK0CPBHZD4(config)# show application-statistics debug

============Station Count 3========================================

      MAC                      IP                      VLAN       SSID
 E4-A7-A0-48-7B-14          10.110.211.180              1       bg_tmp_test
 A0-88-69-F4-22-7F          10.110.211.197              1       bg_tmp_test
 E4-A4-71-15-76-FB          10.110.211.238              1       bg_tmp_test


=====vlan count 1======

VLAN         STA_COUNT
 1              3
```

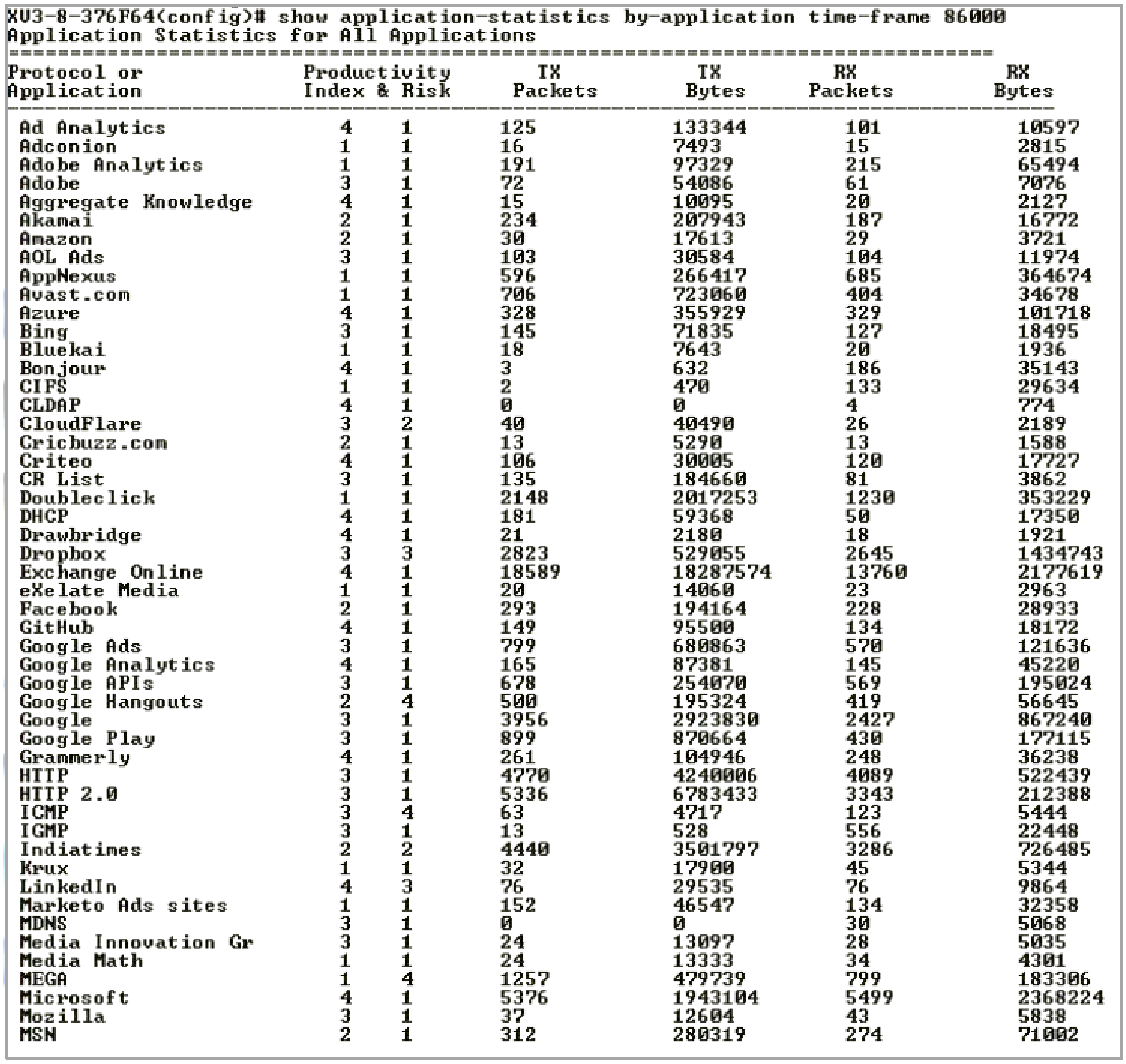
- Display for VLAN: This gives information about the particular VLANs.



```
XV3-8-376F64(config)# show application-statistics by-application vlan 1
Application Statistics for VLAN 1
================================================================================
Protocol or             Productivity       TX           TX         RX            RX
Application             Index & Risk     Packets       Bytes     Packets       Bytes
-------------------------------------------------------------------------------------
 AOL Ads                   3    1       64            14660         64            6538
 AppNexus                  1    1       141           46335         152           93798
 Azure                     4    1       9             5275          11            1410
 Bing                      3    1       20            12192         18            2149
 Bonjour                   4    1       0             0             25            5294
 CIFS                      1    1       0             0             16            3580
 Doubleclick               1    1       15            6369          12            4441
 DHCP                      4    1       12            3936          2             694
 Dropbox                   3    3       109           15360         110           47836
 Exchange Online           4    1       763           409280        780           367996
 Google APIs               3    1       25            11666         19            9045
 Google Hangouts           2    4       34            10409         36            3169
 Google                    3    1       34            9780          29            14947
 Grammerly                 4    1       13            6358          11            933
 HTTP                      3    1       133           25777         192           38979
 ICMP                      3    4       4             540           3             188
 IGMP                      3    1       0             0             31            1248
 MEGA                      1    4       54            15013         30            9629
 Microsoft                 4    1       827           325591        920           536803
 MS CDN                    4    1       29            29013         21            2468
 NetBIOS NS                1    3       0             0             573           45126
 MS Office 365             4    1       568           503652        485           135678
 Microsoft OneDrive        3    4       87            14107         135           152212
 MS Outlook                4    1       14            9464          16            2982
 PubMatic                  3    1       77            8816          66            15788
 Rubicon Project           1    1       141           89748         129           28487
 Skype                     3    1       347           490504        263           18388
 SSDP                      4    1       0             0             67            11861
 SSL                       3    3       453           149881        503           138462
 Symantec                  3    1       33            16092         35            11641
 TeamViewer                4    2       173           93465         166           66682
 UDP                       3    1       94            7834          103           42952
 Web Services Discov       3    1       0             0             6             6126
 YouTube                   1    4       2509          3400884       483           47153
XV3-8-376F64(config)#
```

- By Time frame: This gives information about the application seen in last the duration (E.g. 1 day).

- For low risk number the productivity is high and vice versa. (E.g. For GitHub (Shown in below figure) the risk index number is 1 and the productive index is 4, this means the application is low risk and more productive)



```
XV3-8-376F64(config)# show application-statistics by-application time-frame 86000
Application Statistics for All Applications
================================================================================
Protocol or             Productivity      TX             TX          RX            RX
Application             Index & Risk    Packets         Bytes      Packets         Bytes
-------------------------------------------------------------------------------------
 Ad Analytics              4     1       125           133344        101           10597
 Adconion                  1     1       16            7493          15            2815
 Adobe Analytics           1     1       191           97329         215           65494
 Adobe                     3     1       72            54086         61            7076
 Aggregate Knowledge       4     1       15            10095         20            2127
 Akamai                    2     1       234           207943        187           16772
 Amazon                    2     1       30            17613         29            3721
 AOL Ads                   3     1       103           30584         104           11974
 AppNexus                  1     1       596           266417        685           364674
 Avast.com                 1     1       706           723060        404           34678
 Azure                     4     1       328           355929        329           101718
 Bing                      3     1       145           71835         127           18495
 Bluekai                   1     1       18            7643          20            1936
 Bonjour                   4     1       3             632           186           35143
 CIFS                      1     1       2             470           133           29634
 CLDAP                     4     1       0             0             4             774
 CloudFlare                3     2       40            40490         26            2189
 Cricbuzz.com              2     1       13            5290          13            1588
 Criteo                    4     1       106           30005         120           17727
 CR List                   3     1       135           184660        81            3862
 Doubleclick               1     1       2148          2017253       1230          353229
 DHCP                      4     1       181           59368         50            17350
 Drawbridge                4     1       21            2180          18            1921
 Dropbox                   3     3       2823          529055        2645          1434743
 Exchange Online           4     1       18589         18287574      13760         2177619
 eXelate Media             1     1       20            14060         23            2963
 Facebook                  2     1       293           194164        228           28933
 GitHub                    4     1       149           95500         134           18172
 Google Ads                3     1       799           680863        570           121636
 Google Analytics          4     1       165           87381         145           45220
 Google APIs               3     1       678           254070        569           195024
 Google Hangouts           2     4       500           195324        419           56645
 Google                    3     1       3956          2923830       2427          867240
 Google Play               3     1       899           870664        430           177115
 Grammerly                 4     1       261           104946        248           36238
 HTTP                      3     1       4770          4240006       4089          522439
 HTTP 2.0                  3     1       5336          6783433       3343          212388
 ICMP                      3     4       63            4717          123           5444
 IGMP                      3     1       13            528           556           22448
 Indiatimes                2     2       4440          3501797       3286          726485
 Krux                      1     1       32            17900         45            5344
 LinkedIn                  4     3       76            29535         76            9864
 Marketo Ads sites         1     1       152           46547         134           32358
 MDNS                      3     1       0             0             30            5068
 Media Innovation Gr       3     1       24            13097         28            5035
 Media Math                1     1       24            13333         34            4301
 MEGA                      1     4       1257          479739        799           183306
 Microsoft                 4     1       5376          1943104       5499          2368224
 Mozilla                   3     1       37            12604         43            5838
 MSN                       2     1       312           280319        274           71002
```

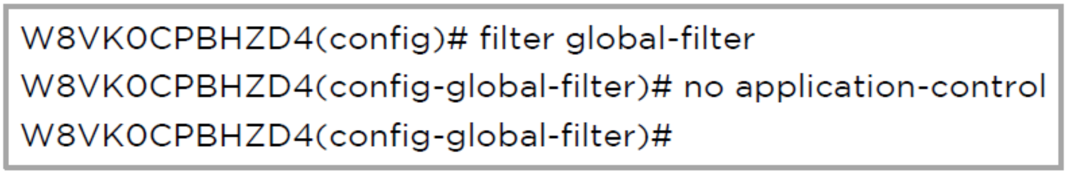
DPI CLI Configuration

User can enable Application Control globally by using below commands:

Enable DPI Support

```
W8VK0CPBHZD4(config)# filter global-filter
W8VK0CPBHZD4(config-global-filter)# application-control
W8VK0CPBHZD4(config-global-filter)#
```

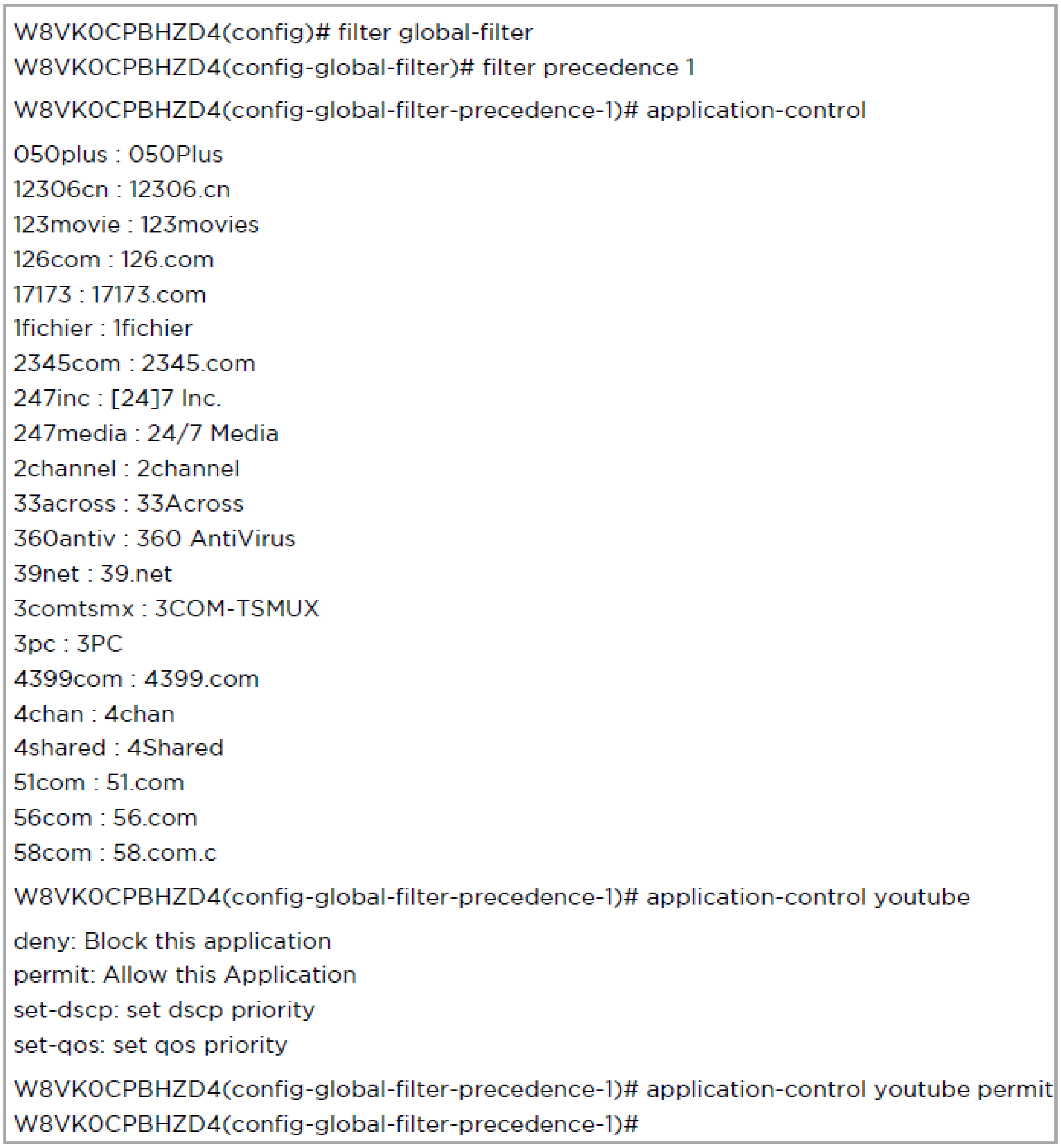
Disable DPI Support



```
W8VK0CPBHZD4(config)# filter global-filter
W8VK0CPBHZD4(config-global-filter)# no application-control
W8VK0CPBHZD4(config-global-filter)#
```

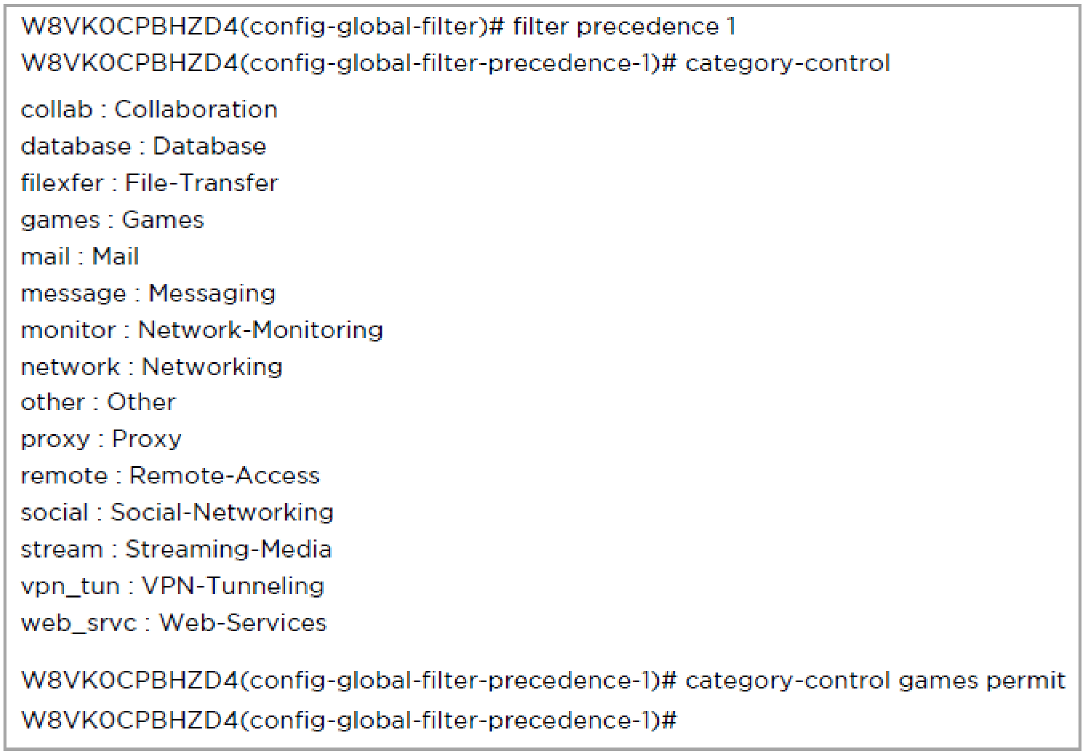
Global Application Policy

Per Application Policy



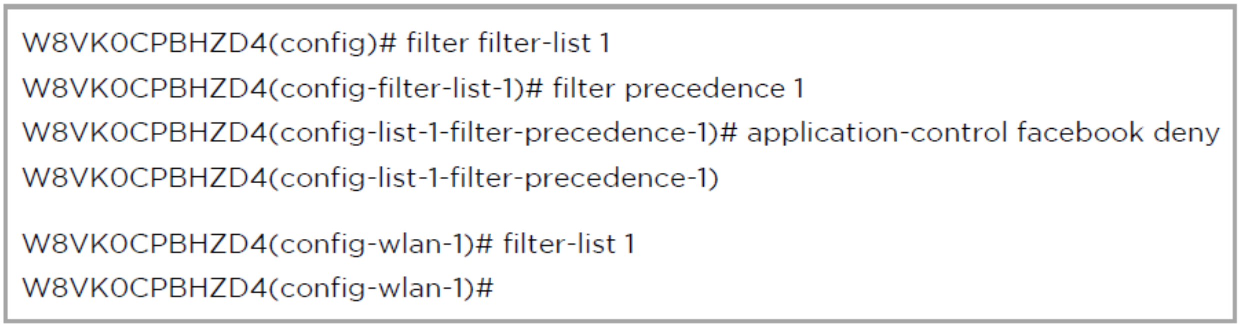
```
W8VK0CPBHZD4(config)# filter global-filter
W8VK0CPBHZD4(config-global-filter)# filter precedence 1
W8VK0CPBHZD4(config-global-filter-precedence-1)# application-control
050plus : 050Plus
12306cn : 12306.cn
123movie : 123movies
126com : 126.com
17173 : 17173.com
1fichier : 1fichier
2345com : 2345.com
247inc : [24]7 Inc.
247media : 24/7 Media
2channel : 2channel
33across : 33Across
360antiv : 360 AntiVirus
39net : 39.net
3comtsmx : 3COM-TSMUX
3pc : 3PC
4399com : 4399.com
4chan : 4chan
4shared : 4Shared
51com : 51.com
56com : 56.com
58com : 58.com.c
W8VK0CPBHZD4(config-global-filter-precedence-1)# application-control youtube
deny: Block this application
permit: Allow this Application
set-dscp: set dscp priority
set-qos: set qos priority
W8VK0CPBHZD4(config-global-filter-precedence-1)# application-control youtube permit
W8VK0CPBHZD4(config-global-filter-precedence-1)#
```

Set per Category Policy



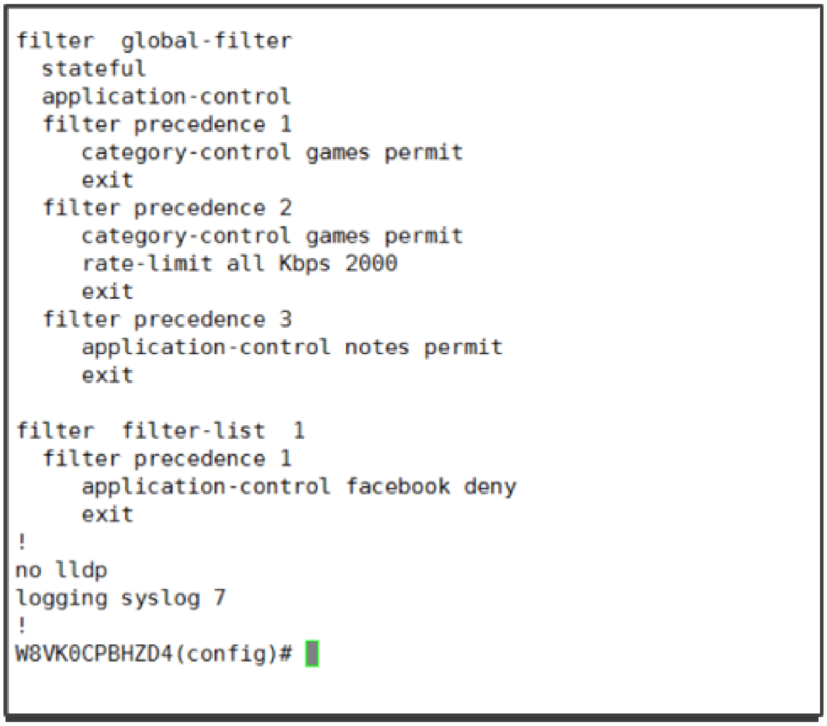
```
W8VK0CPBHZD4(config-global-filter)# filter precedence 1
W8VK0CPBHZD4(config-global-filter-precedence-1)# category-control

collab : Collaboration
database : Database
filexfer : File-Transfer
games : Games
mail : Mail
message : Messaging
monitor : Network-Monitoring
network : Networking
other : Other
proxy : Proxy
remote : Remote-Access
social : Social-Networking
stream : Streaming-Media
vpn_tun : VPN-Tunneling
web_srvc : Web-Services

W8VK0CPBHZD4(config-global-filter-precedence-1)# category-control games permit
W8VK0CPBHZD4(config-global-filter-precedence-1)#
```

SSID Application Policy



```
W8VK0CPBHZD4(config)# filter filter-list 1
W8VK0CPBHZD4(config-filter-list-1)# filter precedence 1
W8VK0CPBHZD4(config-list-1-filter-precedence-1)# application-control facebook deny
W8VK0CPBHZD4(config-list-1-filter-precedence-1)

W8VK0CPBHZD4(config-wlan-1)# filter-list 1
W8VK0CPBHZD4(config-wlan-1)#
```

Show configuration



```
filter  global-filter
  stateful
  application-control
  filter precedence 1
     category-control games permit
     exit
  filter precedence 2
     category-control games permit
     rate-limit all Kbps 2000
     exit
  filter precedence 3
     application-control notes permit
     exit

filter  filter-list  1
  filter precedence 1
     application-control facebook deny
     exit
!
no lldp
logging syslog 7
!
W8VK0CPBHZD4(config)#
```

BSS Coloring

Multiple APs operate on a shared channel by mitigating co-channel interference. This is made possible by a spatial reuse technique known as BSS Coloring, which enables devices in one BSS to ignore frames from other BSSs on the same channel, which are typically some distance away.

Target Wake Time (TWT)

The target wake time (TWT) feature included in the IEEE 802.11ax amendment provides a mechanism to schedule transmissions in a specific time or set of times for individual STAs to wake to exchange frames with AP. Using TWT, each STA negotiates awake periods with the AP to transmit and receive data packets and can go to doze mode to minimize energy consumption and reduce contention within the basic service set (BSS).

Note

By default, BSS Coloring and TWT is enabled.

XV2-2 ETSI DFS and LBT Certification

Starting from 6.2 release, XV2-2 AP is DFS and LBT certified in ETSI region.

XIRCON Support

The Xirrus console (Xircon) is a necessary tool for daily management, troubleshooting, and testing. Xirrus customers and field engineers used them for initial configuration, troubleshooting individual AP problems, changing IP addresses, and recovering units that would not boot. Since Cambium Networks acquired Xirrus and we expect the XV series APs to be deployed along with legacy Xirrus APs, limited Xircon support is added to the XV series APs.

The name "Xircon" refers to the feature in general, including the AP functionality, the communication protocol, and the client software used for discovering and controlling Xirrus APs.

- Xircon detects APs by listening for Xircon beacon packets. These packets are sent via UDP to a defined port and multicast address. This is the existing Multicast beacons sent by AOS.
- Control is established over unicast UDP on a different port from discovery. Only one client device can control an AP at any given time.
- Individual packets are RC4 encrypted. The payload includes a hash to ensure that any tampering or packet corruption is detected, and the packet discarded.
- Starting with System release 6.2, XV series APs can be detected by Xirrus AOS APs and the Xircon client. It is not possible to establish a Xircon console connection to XV series APs – for that identify the IP address from Xircon and use standard SSH to connect.

Chapter 7: Configuration – Radio

This chapter describes the following topics:

- Overview
- Configuring Radio parameters

Overview

Enterprise Wi-Fi AP devices support numerous configurable radio parameters to enhance the quality of service as per the deployment.

Configuring Radio parameters

The XV3-8 Tri-Band Indoor Wi-Fi 6 AP can operate in either Dual Band Simultaneous (DBS) or Single Band Simultaneous (SBS). This feature provides the flexibility of splitting 5GHz radio into two independently configurable and operational radios. In DBS mode, 5GHz radio operates as single radio with 8x8 configuration. In SBS mode, 5GHz Radio operates as split radio with each 4x4 configuration. Information of each band radio configurable parameters are listed in nelow table.

Table 10 :Configure: Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables operation of radio.	-	Enabled
Channel	User can select the channel from the drop-down list. Channels in drop-down list is populated based on Country selected in Configuration > System UI.	**2.4 GHz:** 1 - 14 **5 GHz:** 36 - 173	Auto
Channel Width	User can select operating width of the channel. • For 2.4GHz: Only 20MHz channel width is supported. • For 5GHz: 20MHz, 40MHz, 80MHz and 160MHz channel width is supported.	-	20MHz for 2.4GHz. 80MHz for 5GHz
Transmit Power	User can configure transmit power of each radio based on coverage and SLA. Unit of transmit power is in dBm and its range is from 4 to 30. Maximum transmit power of Enterprise Wi-Fi AP devices varies based on model number. More details of transmit power supported by each Enterprise Wi-Fi AP device is available at https://www.cambiumnetworks.com/products/wifi/. Transmit power drop-down box varies as per the country selected in Configuration > System UI. Default value is AUTO, which means radio transmit power is	**2.4GHz:** 4 - 30 **5GHz:** 4 - 30	Auto

Parameter	Description	Range	Default
	configured to maximum as per the county configured selected in Configuration > System UI.		
Beacon Interval	User can configure time durations between two consecutive Beacon's. It is termed as Beacon interval.	50ms - 3400ms.	100
Minimum Unicast rate	Provision to adjust the coverage area of Enterprise Wi-Fi AP device. Higher the rate selected, lesser the range. User can configure this value based on SLA in deployment. Drop-down list contains all values that are advertised by Enterprise Wi-Fi AP device which includes legacy, HT and VHT rates.	Standard 802.11b and 802.11g data rates	1Mbps
Candidate Channels	Enterprise Wi-Fi AP provides user to configure selective channels based on their requirement. Options vary based on band of operation and is as follows: • For 2.4GHz: • All • Specific • For 5GHz: • All • Specific • Prefer Non-DFS • Prefer DFS	• 2.4GHz: 1 - 14 • 5GHz: 36 - 173	All
Mode	All Enterprise Wi-Fi AP devices are either 802.11ax, 802.11ac Wave 1 or 802.11ac Wave 2 supported. There are few legacy clients which might not work as expected, hence this parameter can be tuned to backward compatibility based on wireless clients.	• 2.4GHz: b/g/n/ax. • 5GHz: a/n/ac/ ax.	• 11ax for 2.4 GHz • 11ax for 5GHz
Short Guard Interval	Standard 802.11 parameter to increase the throughput of Enterprise Wi-Fi AP device.	-	Enabled
Off Channel Scan (OCS)			
Enable	Provision to enable OCS on device to capture neighbour clients and APs.	-	-
Dwell-time	Configure the time period to spend scanning of Wi-Fi devices on a channel.	50-300	50ms

Parameter	Description	Range	Default
Auto-RF			
Dynamic Power	Provision to enable dynamic power management.	-	-
Mode	Select the required dynamic power modes. Two modes are supported: 1. By-channel 2. By-band	-	By-channel
Minimum Transmit Power	The minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes	5-15 dBm	8 dBm
Minimum Neighbour Threshold	The minimum number of neighbors to consider for power reduction by autocell logic.	1-10	2
Cellsize Overlap Threshold	Cell overlap that will be allowed when the AP is determining automatic cell sizes.	0-100%	50%

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

1. Select the **Enable** checkbox to enable the operations of this radio.
2. Select the primary operating channel from the **Channel** drop-down list.
3. Select the operating width (20 MHz, 40 MHz, 80 MHz or 160 MHz) of the channel from the Channel Width drop-down list for 5 GHz only. Enterprise Wi-Fi AP do not support 40 MHz, 80 MHz and 160 MHz in 2.4 GHz.
4. Select radio transmit power from the **Transmit Power** drop-down list.
5. Enter the beacon interval in the **Beacon Interval** textbox.
6. Select the preferred **Candidate Channels** from the drop-down list.
7. Select **Mode** details from the drop-down list.
8. Enable **Short Guard Interval** checkbox.
9. Click **Save**.

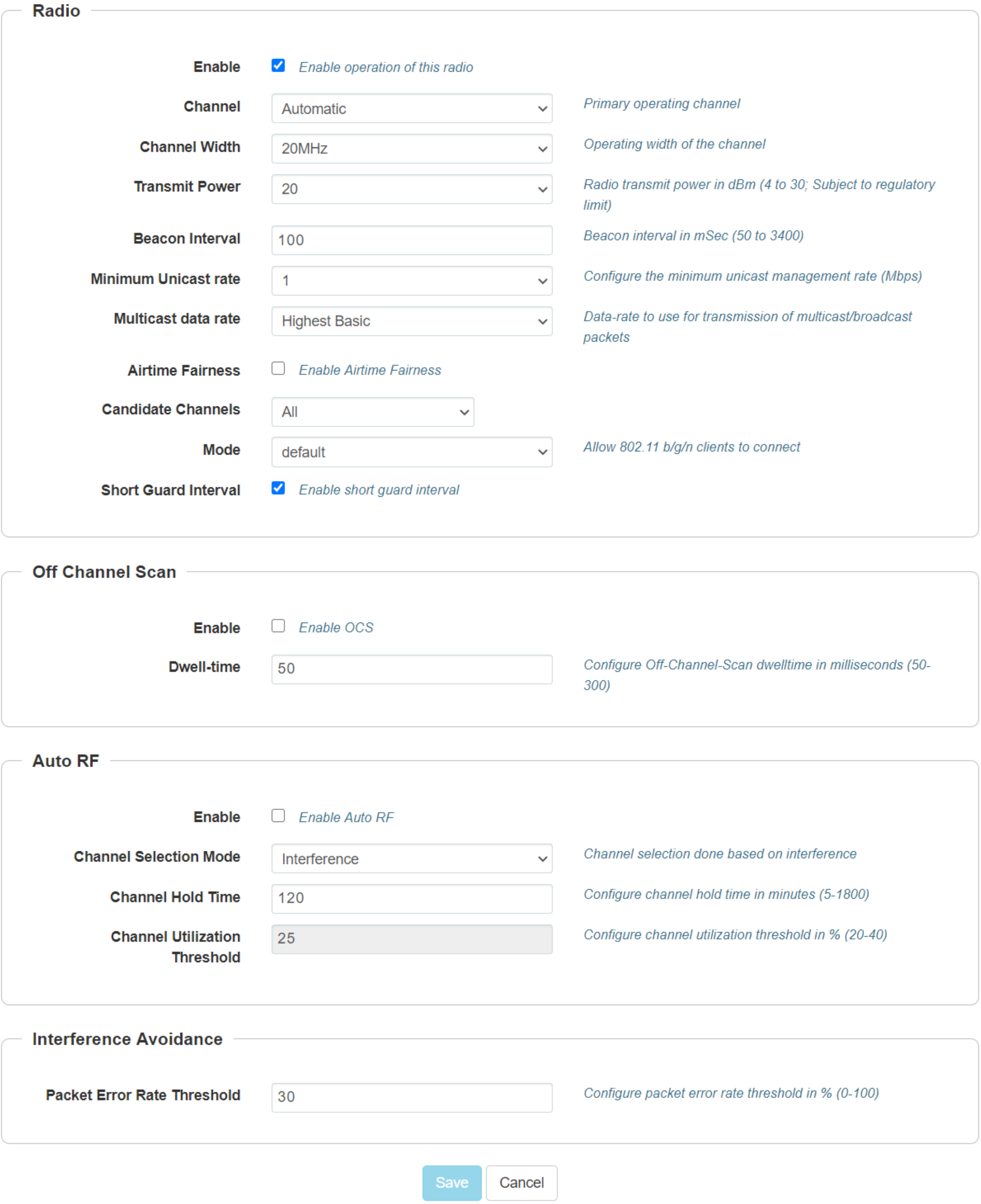
To configure Off Channel Scan:

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

To configure Auto-RF:

1. Select **Dynamic Power** checkbox to enable the operations of this radio.
2. Select the required dynamic power **Mode** as By-channel or By-hand..
3. Enter the **Minimum Transmit Power** in the textbox.
4. Enter **Minimum Neighbour Threshold** parameter in the textbox.
5. Click **Save**.

Figure 10 : *Configure: Radio parameters*



Radio

Enable	☑ *Enable operation of this radio*	
Channel	Automatic	*Primary operating channel*
Channel Width	20MHz	*Operating width of the channel*
Transmit Power	20	*Radio transmit power in dBm (4 to 30; Subject to regulatory limit)*
Beacon Interval	100	*Beacon interval in mSec (50 to 3400)*
Minimum Unicast rate	1	*Configure the minimum unicast management rate (Mbps)*
Multicast data rate	Highest Basic	*Data-rate to use for transmission of multicast/broadcast packets*
Airtime Fairness	□ *Enable Airtime Fairness*	
Candidate Channels	All	
Mode	default	*Allow 802.11 b/g/n clients to connect*
Short Guard Interval	☑ *Enable short guard interval*	

Off Channel Scan

Enable	□ *Enable OCS*	
Dwell-time	50	*Configure Off-Channel-Scan dwelltime in milliseconds (50-300)*

Auto RF

Enable	□ *Enable Auto RF*	
Channel Selection Mode	Interference	*Channel selection done based on interference*
Channel Hold Time	120	*Configure channel hold time in minutes (5-1800)*
Channel Utilization Threshold	25	*Configure channel utilization threshold in % (20-40)*

Interference Avoidance

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

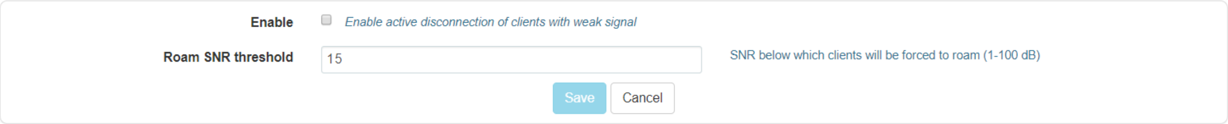
To configure Enhanced Roaming:

1. Select the Enable checkbox to enable the operations of this radio.

2. Enter Roam SNR threshold parameter in the textbox.

3. Click Save.

Figure 11 : *Configure: Radio > Enhanced Roaming parameters*



Enable □ *Enable active disconnection of clients with weak signal*

Roam SNR threshold 15 SNR below which clients will be forced to roam (1-100 dB)

Chapter 8: Configuration - Wireless LAN

This chapter describes the following topics:

- Overview
- Configuring WLAN parameters

Overview

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

Configuring WLAN parameters

Configurable parameters under WLAN profile are categorized into two sections:

1. Basic
2. Advanced

Table 11 lists the configurable parameters for a WLAN profile which is common across bands.

Table 11 : Configure: WLAN > Basic parameters

Parameters	Description	Range	Default
WLAN > Basic			
Enable	Option to enable a WLAN profile. Once enabled, a Beacon is broadcasted with SSID and respective configured parameters in a WLAN profile.	-	-
SSID	SSID is the unique network name that wireless stations scans and associates.	-	-
VLAN	VLAN is configured to segregate wireless station traffic from AP traffic in the network. Wireless stations obtain IP address from the subnet configured in VLAN field of WLAN profile.	1-4094	1
Security	This parameter determines key values that is encrypted based on selected algorithm. Following security methods are supported by Enterprise Wi-Fi AP devices: 1. Open This method is preferred when Layer 2 authentication is built in the network. With this configured on Enterprise Wi-Fi AP device, any wireless station will be able to connect. 2. Osen This method is extensively used when Passpoint 2.0 is enabled on	-	Open

Paramet ers	Description	Range	Default
	Enterprise Wi-Fi AP devices. If Passpoint 2.0 is disabled, this security plays no role in wireless station association. 3. WPA2-Pre-Shared Keys This mode is supported with AES and TKIP encryption. WPA-TKIP and WPA-AES can be enabled from the CLI with the “allow-tkip” CLI option. 4. WPA2 Enterprise This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication method. WPA-TKIP and WPA-AES can be enabled from the CLI with the “allow-tkip” CLI option. 5. WPA2/WPA3 Pre-shared Keys WPA2/WPA3 is a method of securing the network using WPA2/WPA3 with the use of the optional Pre-shared Key (PSK) authentication, that is designed for home users without an enterprise authentication server. To encrypt a network with WPA2/WPA3-PSK, the user to provide the router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. (E.g: Welcome@123). 6. WPA3 Pre-shared Keys WPA3 security protocol provides a much more secure and reliable method replacing WPA2 and the older security protocols. WPA3 has further security improvements that make it harder to break into networks by guessing passwords. 7. WPA3 Enterprise WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates mixing and matching of security protocols that are defined in 802.11 standard. 8. WPA3 Enterprise CNSA WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates mixing and matching of security protocols that are defined in 802.11 standard. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite, and commonly used in high-security Wi-Fi networks in government, defence, Finance and industrial verticals.		
Passphr ase	String that is a key value to generate keys based on security method configured.	-	123456 78

Parameters	Description	Range	Default
Radios	Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options available to configure transmit mode of SSID: • 2.4GHz and 5GHz • 2.4GHz • 5GHz	-	2.4GHz and 5GHz
VLAN Pooling	This parameter is required when user requires to distribute clients across multiple subnets. Different modes of VLAN pooling is supported by Enterprise Wi-Fi AP devices, based on infrastructure available at deployment site. Modes supported are as follows: 1. Disabled This feature is disabled for this WLAN. 2. Radius Based User is expected to configure WPA2 Enterprise for this mode to support. During association phase, AP obtains pool name form RADIUS transaction and based on present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IP address from the VLAN selected by Enterprise Wi-Fi AP device. 3. Static For this mode to support, user requires to configure VLAN Pool details available under **Configure > Network > VLAN pool**. During association phase, AP obtains pool and based on present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4/IPv6 address from the VLAN selected by Enterprise Wi-Fi AP device.	—	Disabled
Max Clients	This specifies the maximum number of wireless stations that can be associated to a WLAN profile. This varies based on Enterprise Wi-Fi AP device model number. Refer Table 12 for more details.	1-512 (Refer Table 12)	127
Client Isolation	This feature needs to be enabled when there is a need for restriction of wireless station to station communication across the network or on an AP. Four options are available to configure based on requirement: 1. **Disable** This option when selected disables client isolation feature. i.e. any wireless stations can communicate to other wireless stations.		

Parameters	Description	Range	Default
	2. **Local** This options when selected enables client isolation feature. This option prevents wireless station communications connected to same AP. 3. **Network Wide** This options when selected enables client isolation feature. It prevents wireless stations communications connected to different AP deployed in same L2 network. **Note** - Network wide mode is not supported when Redundancy Gateway protocol is used on deployment. - In Redundancy Gateway case, Network wide static can be used providing list of Gateway MAC addresses. 4. **Network Wide Static** This option when configured enables client isolation feature across network. Wireless stations can communicate only to statically added MAC list. Communication to rest other MAC addresses are blocked. **Note** When Network Wide and Network Wide Static selected, user has the provision to add the whitelist MAC addresses to allow the communication. A maximum 64 MAC addresses can be added.		
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	-	Disabled
Session Timeout	This field is specific to non-guest wireless stations. When a wireless station connects, a session timer is triggered. Once session time expires, wireless station must undergo either re-authentication or re-association based on state of wireless station. By default, it is enabled.	60-604800	28800
Inactivity Timeout	Inactivity timer triggers whenever there is no communication between Enterprise Wi-Fi AP device and wireless station associated to Enterprise Wi-Fi AP device. Once the timer reaches the configured Inactivity timeout value, APs sends a de-authentication to that wireless station. By default, it is enabled.	60-28800	1800

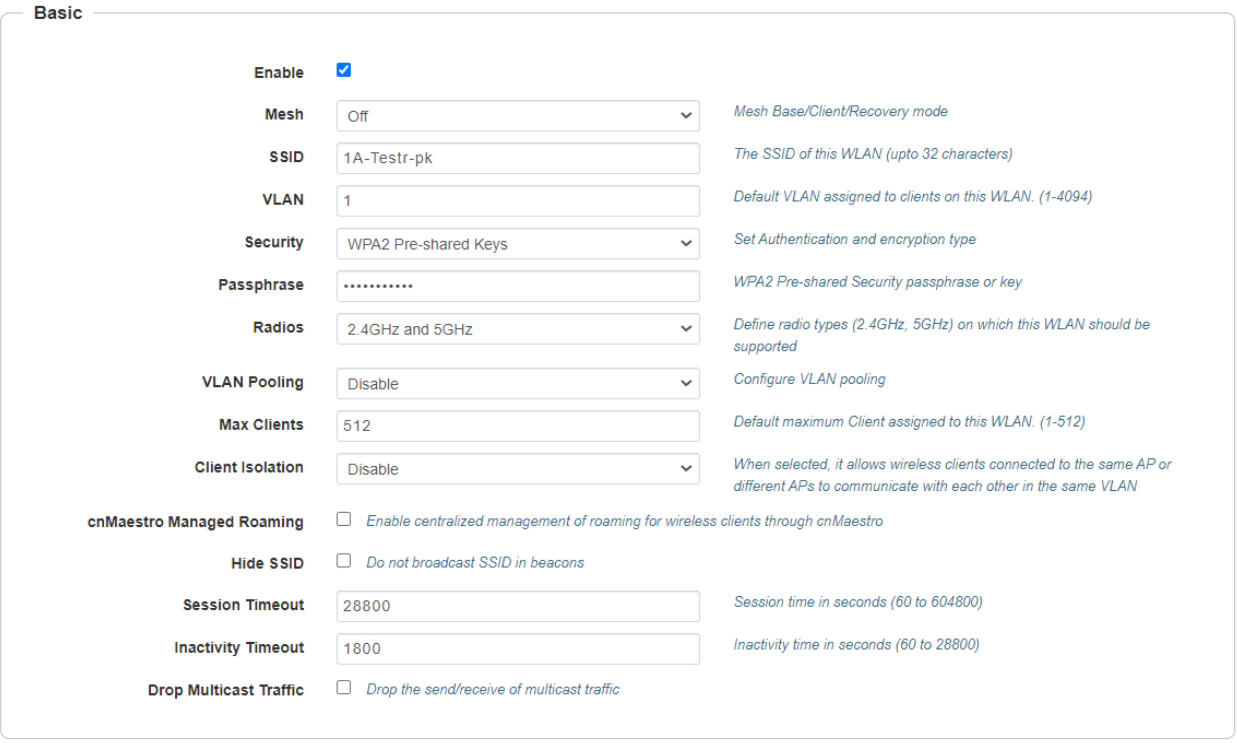
To configure the above parameters, navigate to the Configure > WLAN > Basic tab and provide the details as given below:

1. Select the **Enable** checkbox to enable a particular WLAN.
2. Enter the SSID name for this WLAN in the **SSID** textbox.
3. Enter the default VLAN assigned to the clients on this WLAN in the **VLAN** textbox.
4. Select **Security** type from the drop-down list.
5. Enter WPA2 Pre-shared security passphrase or key in the **Passphrase** textbox.
6. Select the radio type (2.4GHz, 5GHz) on which the WLAN should be supported from the **Radios** drop-down list.
7. Select the required **VLAN Pooling** parameters from the drop-down list.
8. Select **Max Clients** parameter value from the drop-down list.
9. Select the required **Client Isolation** parameter from the drop-down list.
10. Enable **Hide SSID** checkbox.
11. Enter the session timeout value in the **Session Timeout** textbox.
12. Enter the inactivity timeout value in the **Inactivity timeout** textbox.
13. Click **Save**.

Table 12 :WLAN (Max Clients) parameters

Number of Clients	2.4GHz	5GHz	Concurrent
XV3-8	512	512	1024
XV2-2	512	512	1024

Figure 12 : *Configure: WLAN > Basic parameter*



Basic

Enable: ☑

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

SSID: 1A-Testr-pk — *The SSID of this WLAN (upto 32 characters)*

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

Security: WPA2 Pre-shared Keys — *Set Authentication and encryption type*

Passphrase: ••••••••••• — *WPA2 Pre-shared Security passphrase or key*

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

VLAN Pooling: Disable — *Configure VLAN pooling*

Max Clients: 512 — *Default maximum Client assigned to this WLAN. (1-512)*

Client Isolation: Disable — *When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN*

cnMaestro Managed Roaming: ☐ *Enable centralized management of roaming for wireless clients through cnMaestro*

Hide SSID: ☐ *Do not broadcast SSID in beacons*

Session Timeout: 28800 — *Session time in seconds (60 to 604800)*

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

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

Table 13 :Configure: WLAN > Advanced parameters

<table>
<tr><th>Parameters</th><th>Description</th><th>Range</th><th>Default</th></tr>
<tr><td colspan="4"><b>WLAN > Advanced</b></td></tr>
<tr><td>UAPSD</td><td>When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming etc. is in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by Enterprise Wi- Fi AP device.
<table>
<tr><th>Priority</th><th>802.1D Priority (= UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr>
<tr><td rowspan="8">lowest
↓
highest</td><td>1</td><td>BK</td><td rowspan="2">AC_BK</td><td rowspan="2">Background</td></tr>
<tr><td>2</td><td>-</td></tr>
<tr><td>0</td><td>BE</td><td rowspan="2">AC_BE</td><td rowspan="2">Best Effort</td></tr>
<tr><td>3</td><td>EE</td></tr>
<tr><td>4</td><td>CL</td><td rowspan="2">AC_VI</td><td rowspan="2">Video</td></tr>
<tr><td>5</td><td>VI</td></tr>
<tr><td>6</td><td>VO</td><td rowspan="2">AC_VO</td><td rowspan="2">Voice</td></tr>
<tr><td>7</td><td>NC</td></tr>
</table></td><td>—</td><td>Disabled</td></tr>
<tr><td>QBSS</td><td>When enabled, appends QBSS IE in Management frames.</td><td>—</td><td>Disabled</td></tr>
</table>

Parameters	Description	Range	Default
	This IE provides information of channel usage by AP, so that smart wireless station can decide better AP for connectivity. Station count, Channel utilization and Available admission capacity are the information available in this IE.		
DTIM interval	This parameter plays a key role when power save supported mobile stations are part of infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.	1-255	1
DNS Logging Host	This feature is required when an Administrator requires to monitor the websites accessed by wireless stations connected to WLAN profile.	—	Disabled
Connection Logging Host	When enabled provides information of all TCP connections accessed by a wireless station that is associated to WLAN.	—	Disabled
Fast-Roaming Protocol	One of the important aspects to support voice applications on Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 msec to avoid any call drop. This is easily achievable when WPA2-PSK security mechanism is in use. However, in enterprise environments there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with AAA server and hence depending on the location of AAA server the roaming-time will be above 700 msec. Select any one of the following: 1. OKC This roaming method is a proprietary solution to bring scalability to the roaming problem. This method avoids the need to authenticate with AAA server every time a client moves to new AP. 2. 802.11r This is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP, which is called Fast Transition (FT). Two modes of FT roaming are supported: • Over-the-Air By default, this is enabled. • Over-the-DS	—	Disabled

Parameters	Description	Range	Default
Re-association Timeout	It's the number of seconds after which the reassociation attempt of a client to an AP should timeout. This is applicable only when FT roaming is enabled.	1-100	20
RRM (802.11k)	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 11k clients. Following parameters needs to be enabled: • Enable RRM • Support for WPA2 authentication method	—	Disabled
PMF (802.11w)	802.11w, also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames makes wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	• Optional • Mandatory • Disabled	—
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms
Association Comeback Time	This value is included in the Association Response as an Association Comeback Time information element. AP will deny association for the configured interval.	1-20	1 Sec

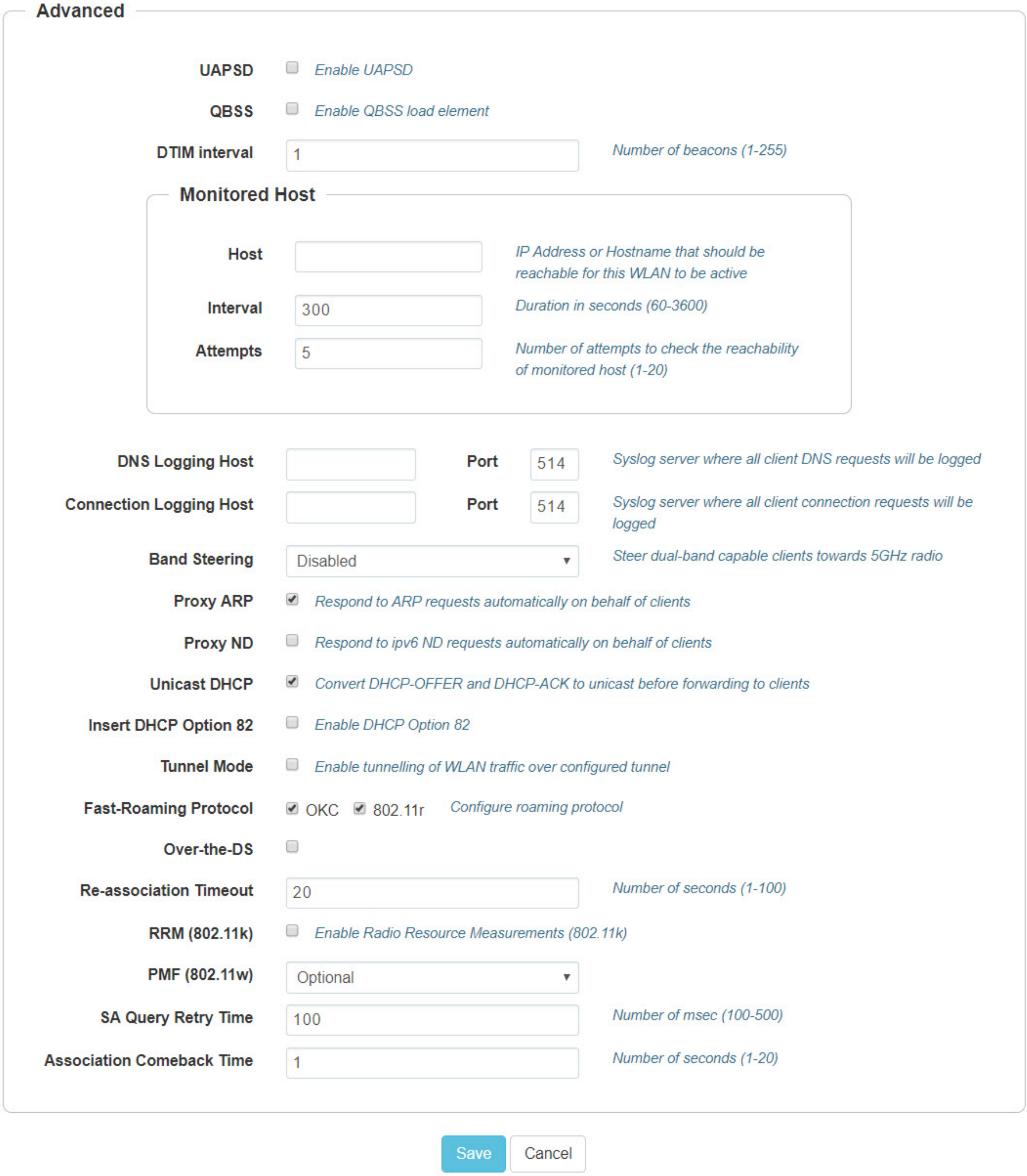
To configure the above parameters, navigate to the Configure > WLAN > Basic tab and provide the details as given below:

1. Select the UAPSD checkbox to enable UAPSD.
2. Select the QBSS checkbox to enable QBSS.
3. Enter the value in the DTIM interval textbox to configure DTIM interval.
4. Enter IP address or Hostname in Host textbox.
5. Enter Interval time duration in the textbox.
6. Select number of attempts to check the reachability of monitored host in the Attempts drop-down list.
7. Enter the FQDN or IP address of the Server where all the client DNS requests will be logged in the DNS Logging Host server along with customized port number in the textbox. If the port number is not entered, AP will take default value as 514.
8. Enter the FQDN or IP address of the Server where all wireless client connectivity events/logs will be displayed in the configured Connection Logging Host server along with customized port number in the textbox. If the port number is not entered, AP will take default value as 514.
9. Enable the required OKC or 802.11r configure roaming protocol in the Fast-Roaming Protocol

checkbox.

10. Enable RRM (802.11k) checkbox.
11. Select PMF (802.11w) parameter from the drop-down list.
    a. Enter SQ Query Retry Time in the textbox.
    b. Enter Association Comeback Time in the textbox.
12. Click Save.

Figure 13 : *Configure: WLAN > Advanced parameter*



Advanced

UAPSD ☐ *Enable UAPSD*

QBSS ☐ *Enable QBSS load element*

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

Monitored Host

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

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

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

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

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

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

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

Proxy ND ☐ *Respond to ipv6 ND requests automatically on behalf of clients*

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

Insert DHCP Option 82 ☐ *Enable DHCP Option 82*

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

Fast-Roaming Protocol ☑ OKC ☑ 802.11r — *Configure roaming protocol*

Over-the-DS ☐

Re-association Timeout: 20 — *Number of seconds (1-100)*

RRM (802.11k) ☐ *Enable Radio Resource Measurements (802.11k)*

PMF (802.11w): Optional ▾

SA Query Retry Time: 100 — *Number of msec (100-500)*

Association Comeback Time: 1 — *Number of seconds (1-20)*

Table 14 :Configure: WLAN > Radius Server parameters

Parameters	Description	Range	Default
Authentication	Provision to configure RADIUS Authentication server details such	-	Disabled

Parameters	Description	Range	Default
Server	as Hostname/IPv4/IPv6, Shared Secret, Port Number and Realm. Maximum of three RADIUS server can be configured.		
Accounting Server	Provision to configure Accounting server details such as Hostname/IPv4/IPv6, Shared Secret, Port Number. Maximum of three RADIUS server can be configured.	-	Disabled
Timeout	Wait time period for response from AAA server.	1-30	3
Attempts	Parameter to configure number of attempts that a device should send AAA request to server if no response is received within configured timeout period.	1-3	1
Accounting Mode	This field is enabled based on customer requirement. Accounting packet is transmitted based on mode selected. 1. Start-Stop Accounting packets are transmitted by AP to AAA server when a wireless station is connected and then disconnects. 2. Start-Interim-Stop Accounting packets are transmitted by AP to AAA server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects. 3. None Accounting mode will be disable	-	Disabled
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Server Pool Mode	User can configure multiple Authorization and Accounting servers. Based on number of wireless stations, user can choose Failover mode. • Failover AP selects the RADIUS server which is up and running based on the order of configuration.	-	Failover
NAS Identifier	This is configurable parameter and is appended in RADIUS request packet.	-	Hostname/ System Name
Dynamic Authorization	This option is required, where there is a CoA requests from AAA/RADIUS server.	-	Disabled
Dynamic VLAN	When enabled, AP honors the VLAN information provided in RADIUS transaction. Wireless station requests IP address from the same VLAN learnt through RADIUS.	-	Enabled

Parameters	Description	Range	Default
Interim Update Interval	This field is used when RADIUS accounting is enabled, and mode selected as Start-Interim-Stop.	10-65535	1800

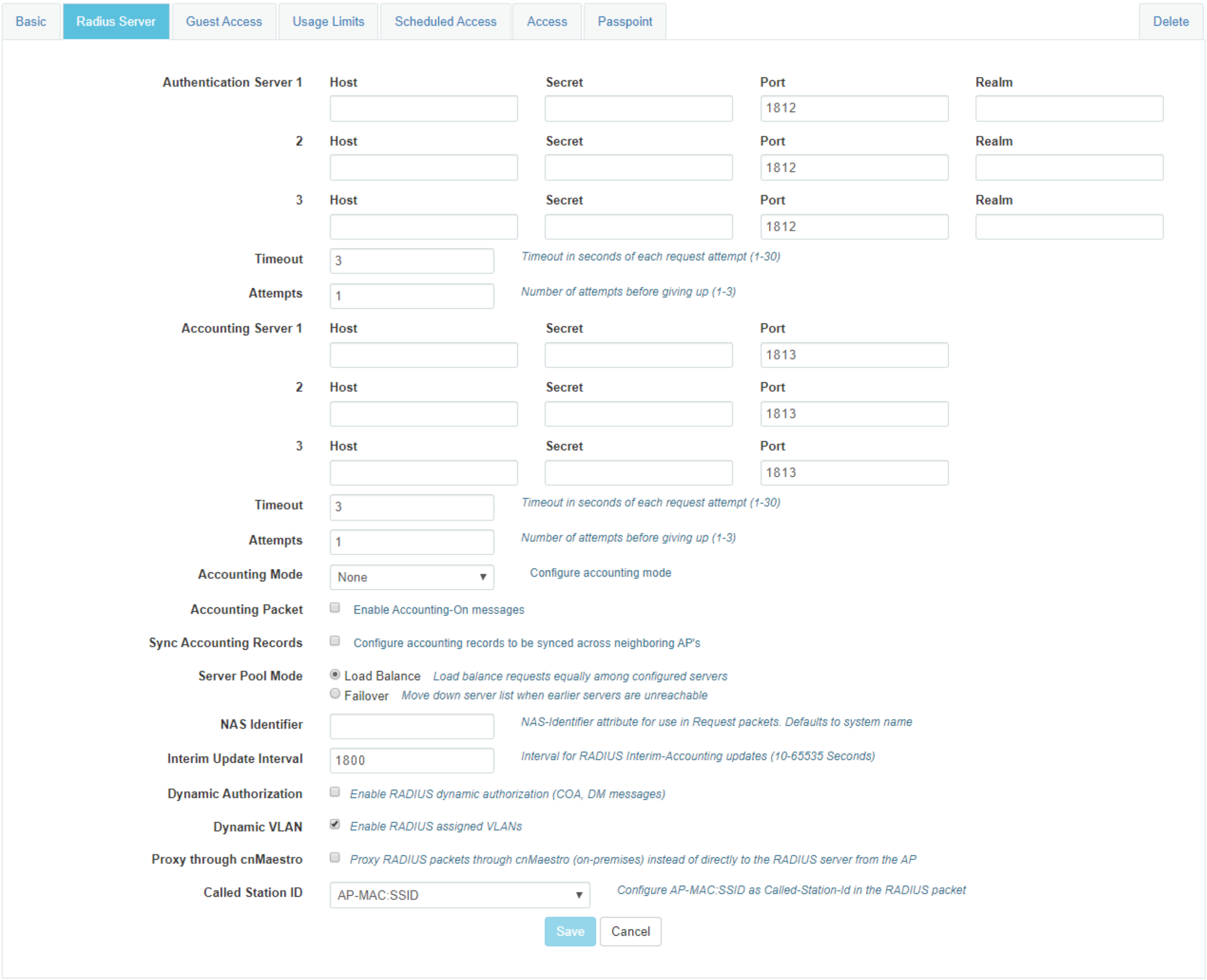
To configure the above parameters, navigate to the Configure > WLAN tab and select Radius Server tab and provide the details as given below:

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

Table 15 :NAS IP with AP dual stack

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

Figure 14 : *Configure: WLAN > Radius Server parameter*



Authentication Server 1	Host:	Secret:	Port: 1812	Realm:
2	Host:	Secret:	Port: 1812	Realm:
3	Host:	Secret:	Port: 1812	Realm:
Timeout	3	Timeout in seconds of each request attempt (1-30)		
Attempts	1	Number of attempts before giving up (1-3)		
Accounting Server 1	Host:	Secret:	Port: 1813	
2	Host:	Secret:	Port: 1813	
3	Host:	Secret:	Port: 1813	
Timeout	3	Timeout in seconds of each request attempt (1-30)		
Attempts	1	Number of attempts before giving up (1-3)		
Accounting Mode	None ▾	Configure accounting mode		
Accounting Packet	□ Enable Accounting-On messages			
Sync Accounting Records	□ Configure accounting records to be synced across neighboring AP's			
Server Pool Mode	● Load Balance *Load balance requests equally among configured servers* ○ Failover *Move down server list when earlier servers are unreachable*			
NAS Identifier		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			
Called Station ID	AP-MAC:SSID ▾	Configure AP-MAC:SSID as Called-Station-Id in the RADIUS packet		

Table 16 :Configure: WLAN > Guest Access > Internal Access Point parameters

Parameters	Description	Range	Default
WLAN > Guest Access > Internal Access Point			
Enable	Enables the Guest Access feature.	-	Disabled
Access Policy	There are four types of access types provided for the user: • Clickthrough This mode allows the users to get access data without any authentication mechanism. User can access internet as soon as he is connected and accepts Terms and Conditions.	-	Clickthrough
Redirect Mode	This option helps the user to configure the HTTP or HTTPS mode of redirection URL.	-	HTTP

Parameters	Description	Range	Default
	1. HTTP AP sends a HTTP POSTURL to the associated client, which will be http://<Pre-defined-URL>. 2. HTTPS AP sends HTTPS POSTURL to the successful associated client, which will be https://<Pre-defined-URL>.		
Title	User can configure a Title to the splash page. Configured text in this parameter will be displayed in the redirection page. This text is usually Bold.	Up to 255 characters	Welcome To Cambium Powered Hotspot
Contents	User can configure the contents of Splash page using this field. Displays the text configured under the Title section of redirection page.	Up to 255 characters	Please enter username and password to get Web Access
Terms	Splash page displays the text configured when user accepts Terms and Agreement.	Up to 255 characters	-
Logo	Displays the logo image updated in URL http (s)://<ipaddress>/logo.png. Either PNG or JPEG format of logo are supported.	-	-
Background Image	Displays the background image updated in URL http (s)://<ipaddress>/backgroundimage.png. Either PNG or JPEG format of logo are supported.	-	-
Success Action	Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL: 1. Internal Logout Page After successful login, wireless client is redirected to logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to URL which is configured on device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to URL that is accessed by user before successful captive portal authentication.	-	Internal Logout page

Parameters	Description	Range	Default
Redirect user to External URL	Provision to configure re-direction URL after successful login and an additional information of AP and wireless station information can be appended in the URL. • Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: • SSID • AP MAC • NAS ID • AP IP • Client MAC • Redirection URL • User can provide either HTTP or HTTPS URL	-	-
Redirection user to Original URL	Users will be redirected to URL that is accessed by user before successful captive portal authentication. There is additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below: • Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: • SSID • AP MAC • NAS ID • AP IP • Client MAC	-	-
Success message	Provision to configure text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	-	-
Redirect	• If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	-	Enabled
Session	This is the duration of time, client will be allowed to access	60 -	28800

Parameters	Description	Range	Default
Timeout	internet if quota persists, after which AP sends de-authentication. Wireless station has to undergo Guest Access authentication after session timeout.	2592000	
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
Whitelist	Provision to configure either IPv4/IPv6 or URLs to bypass traffic, therefor user can access those IPs or URLs without Guest Access authentication.	-	-

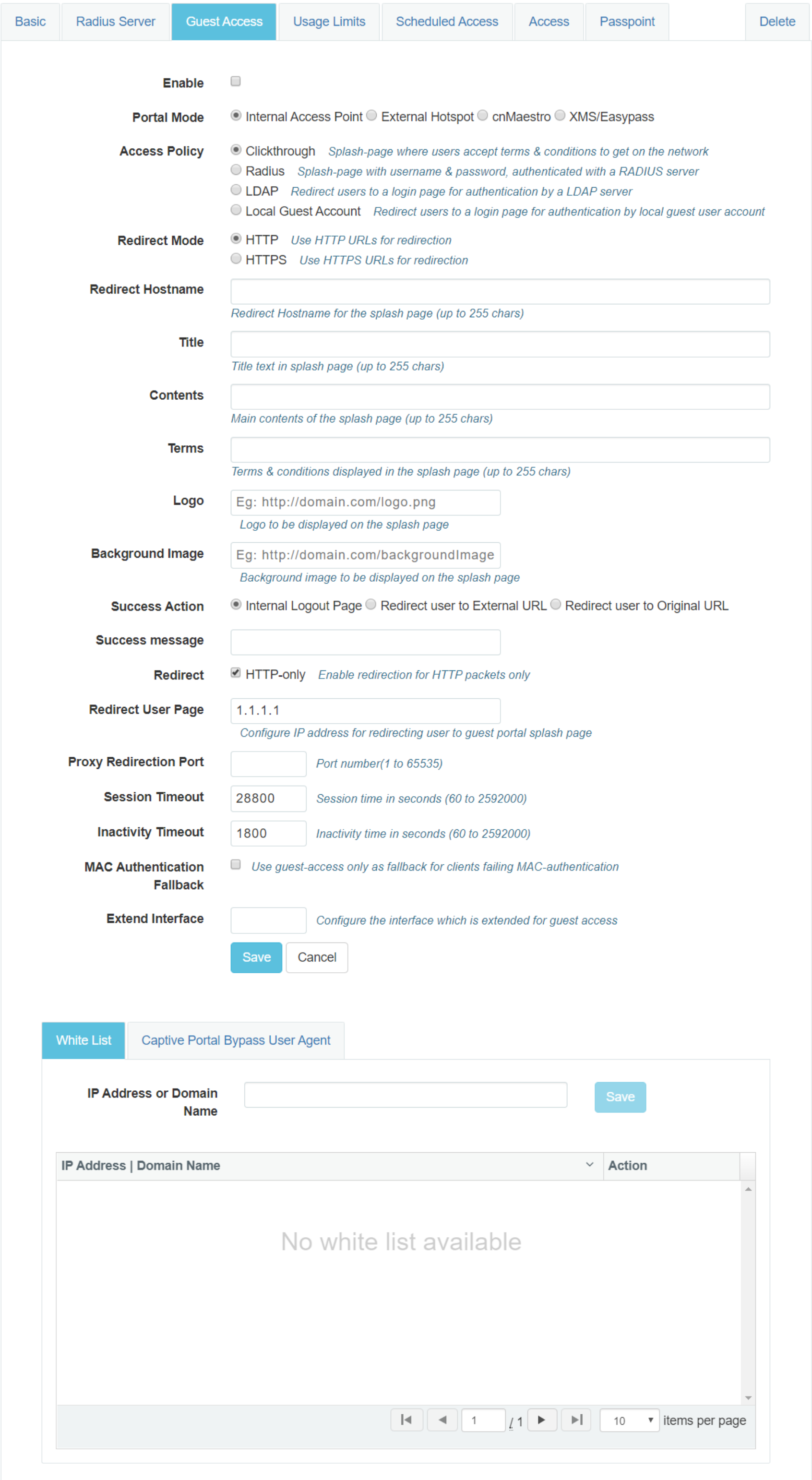
To configure the above parameters, navigate to the Configure > WLAN > Guest Access tab and provide the details as given below:

1. Select Enable checkbox to enable the Guest Access feature.
2. Enable Internal Access Point checkbox.
3. Enable the required access types from the Access Policy checkbox.
4. Enable HTTP or HTTPS from the Redirect Mode checkbox.
5. Enter the title to appear in the splash page in the Title textbox.
6. Enter the content to appear in the splash page in the Contents textbox.
7. Enter the terms and conditions to appear in the splash page in the Terms textbox.
8. Enter the logo to be displayed in the Logo textbox.
9. Select the Background Image to be displayed on the splash page in the textbox.
10. Enable configured modes of redirection URL in Success Action checkbox.
11. Enter Success message to appear in the textbox.
12. Enable Redirect checkbox for HTTP packets.
13. Enter the session timeout in seconds in the Session Timeout textbox.
14. Enter the inactivity timeout in seconds in the Inactivity Timeout textbox.
15. Click Save.

To configure Whitelist parameter:

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

Figure 15 : *Configure: WLAN > Guest Access > Internal Access Point parameter*



Enable ☐

Portal Mode ● Internal Access Point ○ External Hotspot ○ cnMaestro ○ XMS/Easypass

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 *Background image to be displayed on the splash page*

Success Action ● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL

Success message

Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

Redirect User Page 1.1.1.1 *Configure IP address for redirecting user to guest portal splash page*

Proxy Redirection Port *Port number(1 to 65535)*

Session Timeout 28800 *Session time in seconds (60 to 2592000)*

Inactivity Timeout 1800 *Inactivity time in seconds (60 to 2592000)*

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

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

IP Address or Domain Name

IP Address | Domain Name	Action

No white list available

Table 17 :Configure: WLAN > Guest Access > External Hotspot parameters

Parameters	Description	Range	Default
WLAN > Guest Access > External Hotspot			
Access Policy	There are four types of access types provided for the end user: 1. Clickthrough This mode allows users to get access data without any authentication mechanism. User can access internet as soon as he is connected and accepts Terms and Conditions. 2. Radius This mode when selected, user has to provide username and password, which is then redirected to RADIUS server for authentication. If successful, user is provided with data access.	—	Clickthrough
LDAP Server baseDN	Provision to configure the point from where the server will search for users.	—	—
LDAP Server adminDN	Provision to configure the Admin Domain which binds with LDAP server for successful search of LDAP/AD server.	—	—
Redirect Mode	Provision to configure the HTTP or HTTPS mode of redirection URL. 1. HTTP AP sends a HTTP POSTURL to the associated client, which will be http://<Pre-defined-URL>. 2. HTTPS AP sends HTTPS POSTURL to the successful associated client, which will be https://<Pre-defined-URL>.	—	HTTP
WISPr Clients External Server Login	Provision to enable re-direction of guest access portal URL obtained through WISPr.	—	Disabled
External Page URL	User can configure landing/login page which is posted to wireless stations that are not Guest Access authenticated.	—	—
External Portal Post Through cnMaestro	This is required when HTTPS is only supported by external guest access portal. This option when enabled minimizes certification. Certificate is required to install only in cnMaestro On-Premises.	—	Disabled

Parameters	Description	Range	Default
External Portal Type	Enterprise Wi-Fi AP products are supported by below portal types: • Standard This mode is selected, for all third-party vendors whose Guest Access services is certified and integrated with Enterprise Wi-Fi AP products.	—	Standard
Success Action	Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL: 1. Internal Logout Page After successful login, Wireless client is redirected to logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to URL which is configured on device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to URL that is accessed by user before successful captive portal authentication.	—	Internal Logout Page
Redirect user to External URL	Provision to configure re-direction URL after successful login and an additional information of AP and wireless station information can be appended in the URL. • Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: • SSID • AP MAC • NAS ID • AP IP • Client MAC • Redirection URL User can provide either HTTP or HTTPS URL.	—	—
Redirection user to Original URL	Users will be redirected to URL that is accessed by user before successful captive portal authentication. There is additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below:	—	—

Parameters	Description	Range	Default
	• Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: • SSID • AP MAC • NAS ID • AP IP • Client MAC		
Success message	Provision to configure text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	—	—
Redirect	• If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	—	Enabled
Redirect User Page	IP address configured in this field is used as logout/disconnect/redirect to captive portal URL for Guest Access sessions. IP address configured should not be reachable to internet.	—	1.1.1.1
Session Timeout	This is the duration of time, client will be allowed to access internet if quota persists, after which AP sends de-authentication. Wireless station has to undergo Guest Access authentication after session timeout.	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication. This parameter is valid for standard portal type.	—	—

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

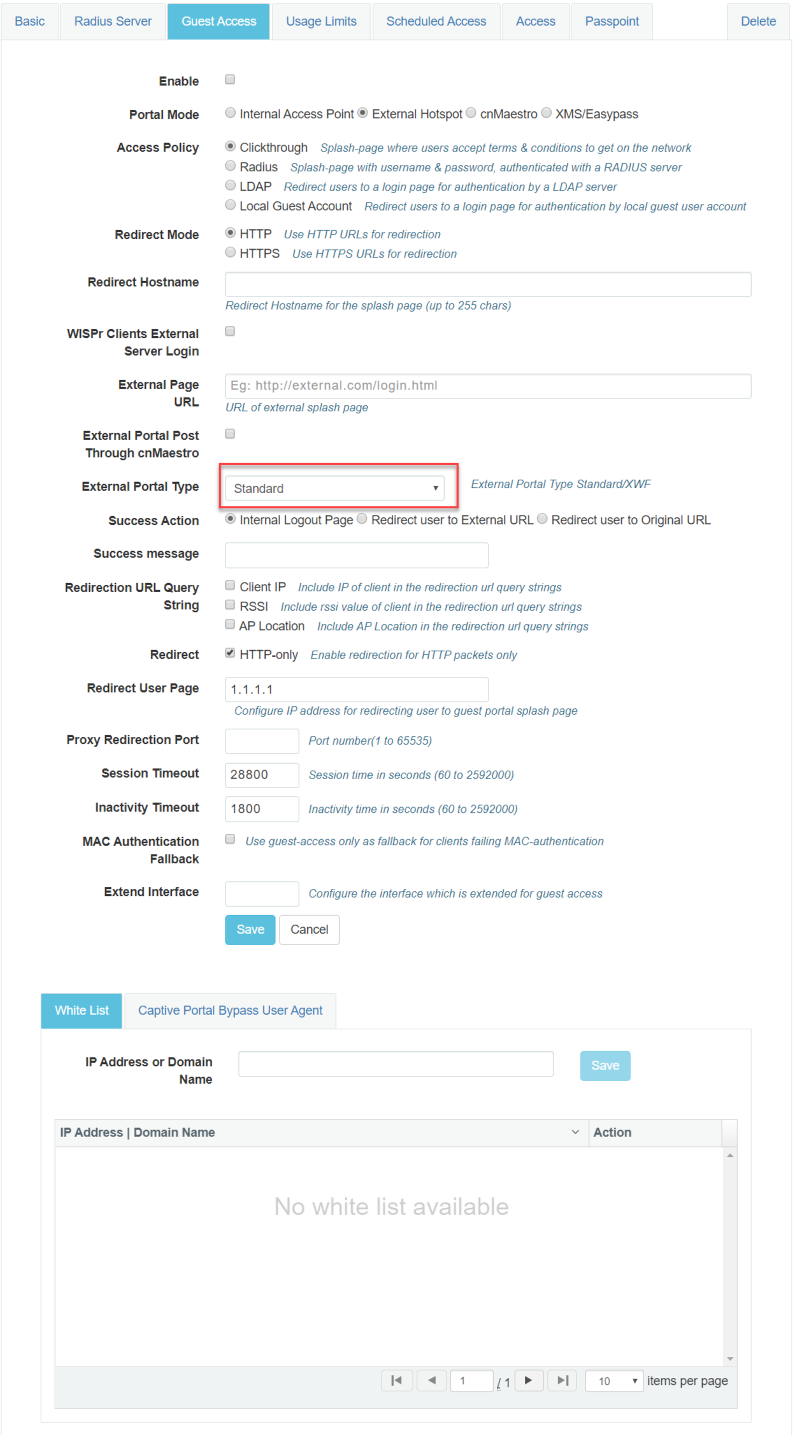
1. Enable the required access types from the Access Policy checkbox.
2. Enable HTTP or HTTPS from the Redirect Mode checkbox.
3. Enter Redirect Hostname in the textbox.
4. Enable WISPr Clients External Server Login checkbox.

5. Enter External Page URL in the textbox.
6. Enable External Portal Post Through cnMaestro checkbox.
7. Select External Portal Type from the drop-down list.
8. Enable configured modes of redirection URL in Success Action checkbox.
9. Enter Success message to appear in the textbox.
10. Enable the required Redirection URL Query String checkbox.
11. Enable Redirect checkbox for HTTP packets.
12. Enter the session timeout in seconds in the Session Timeout textbox.
13. Enter the inactivity timeout in seconds in the Inactivity Timeout textbox.
14. Click Save.

To configure Whitelist:

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

Figure 16 : *Configure: WLAN > Guest Access > External Hotspot (Standard) parameter*



Enable □

Portal Mode ○ Internal Access Point ● External Hotspot ○ cnMaestro ○ XMS/Easypass

Access Policy
● Clickthrough *Splash-page where users accept terms & conditions to get on the network*
○ Radius *Splash-page with username & password, authenticated with a RADIUS server*
○ LDAP *Redirect users to a login page for authentication by a LDAP server*
○ Local Guest Account *Redirect users to a login page for authentication by local guest user account*

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

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

WISPr Clients External Server Login □

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

External Portal Post Through cnMaestro □

External Portal Type Standard ▾ *External Portal Type Standard/XWF*

Success Action ● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL

Success message

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

Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

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

Proxy Redirection Port *Port number(1 to 65535)*

Session Timeout 28800 *Session time in seconds (60 to 2592000)*

Inactivity Timeout 1800 *Inactivity time in seconds (60 to 2592000)*

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

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

IP Address or Domain Name

IP Address | Domain Name	Action
No white list available	

Table 18 :Configure: WLAN > Guest Access > cnMaestro parameters

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	—	—
Redirect	• If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	—	Enabled
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	—	—

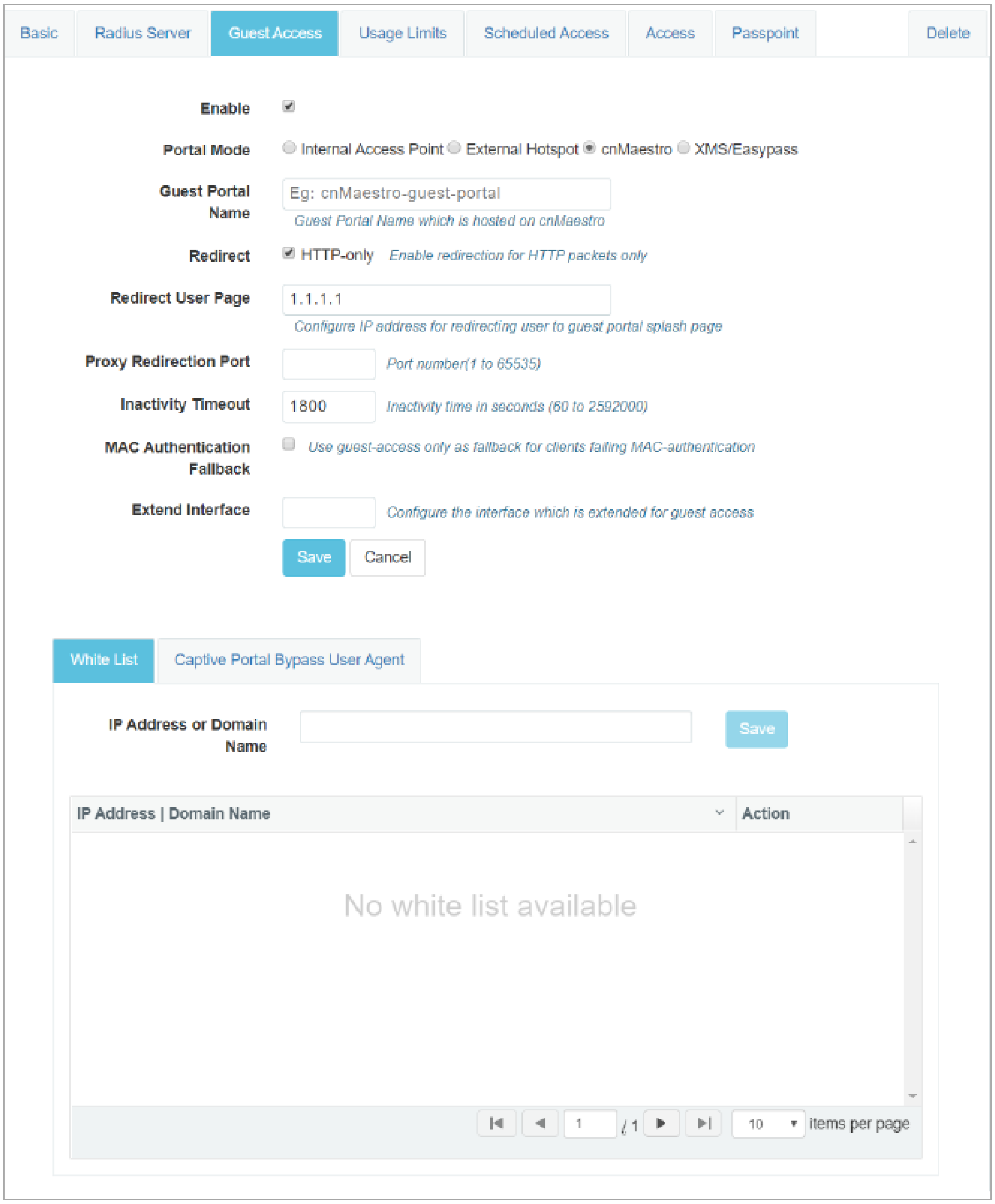
To configure the above parameters, navigate to the Configure > WLAN > cnMaestro tab and provide the details as given below:

1. Enter Guest Portal Name which is hosted on cnMaestro in the textbox.
2. Enable Redirect checkbox for HTTP packets.
3. Enter the inactivity timeout in seconds in the Inactivity Timeout textbox.
4. 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 17 : *Configure: WLAN > Guest Access > cnMaestro parameter*



Enable ☑

Portal Mode ○ Internal Access Point ○ External Hotspot ● cnMaestro ○ XMS/Easypass

Guest Portal Name: Eg: cnMaestro-guest-portal
Guest Portal Name which is hosted on cnMaestro

Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

Redirect User Page: 1.1.1.1
Configure IP address for redirecting user to guest portal splash page

Proxy Redirection Port: *Port number(1 to 65535)*

Inactivity Timeout: 1800 *Inactivity time in seconds (60 to 2592000)*

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

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

IP Address or Domain Name:

IP Address | Domain Name	Action
No white list available	

Table 19 :Configure: WLAN > Guest Access > XMS/EasyPass

Parameters	Description	Range	Default
External Page URL	User can configure login page which is posted to wireless stations that are not Guest Access authenticated.	—	—
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	—	—

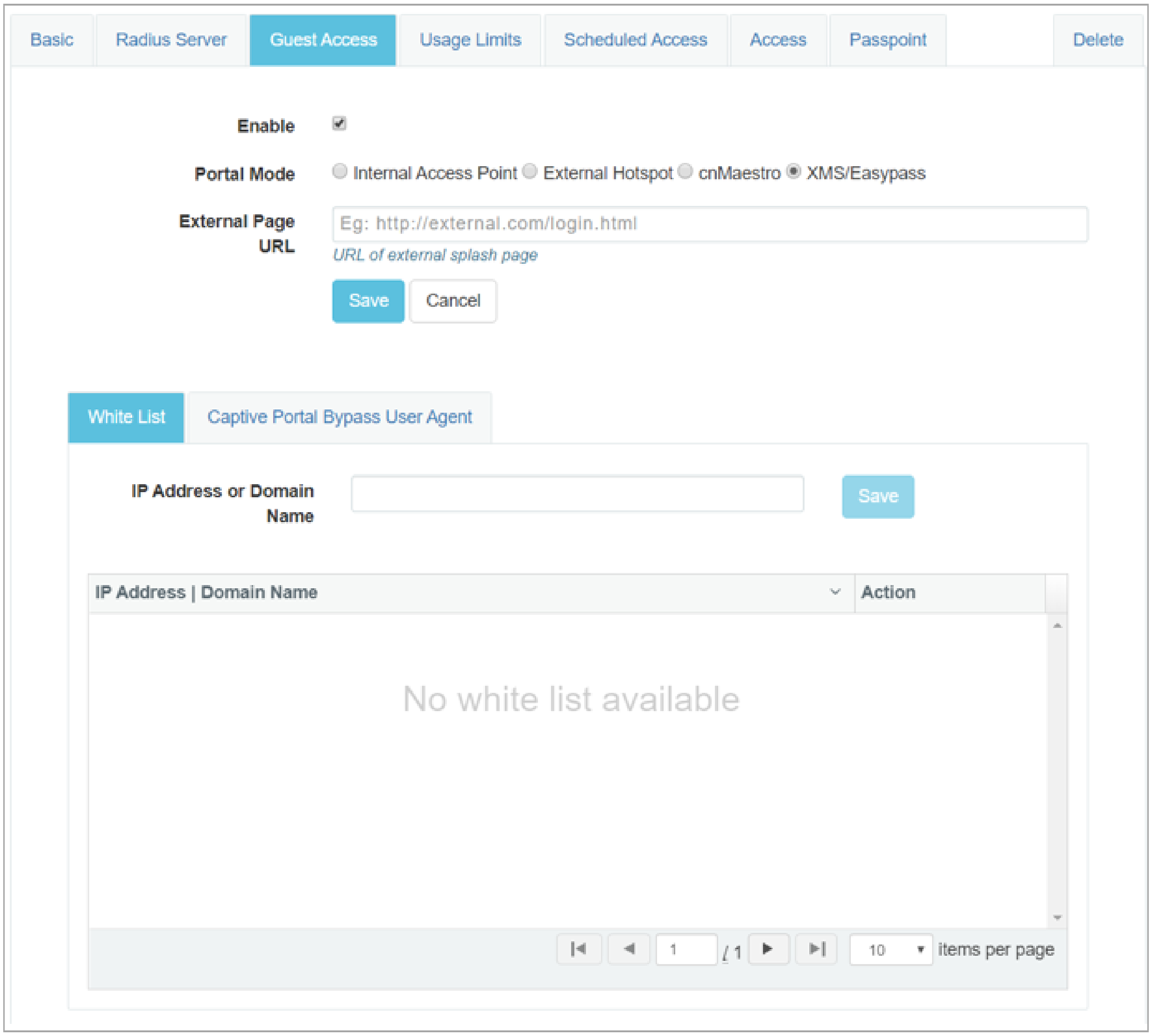
To configure the above parameters, navigate to the Configure > WLAN > XMS/EasyPass tab and provide the details as given below:

1. Enter External Page URL in the 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 18 : *Configure: WLAN > Guest Access > XMS/EasyPass*



Enable ☑

Portal Mode ○ Internal Access Point ○ External Hotspot ○ cnMaestro ● XMS/Easypass

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

URL of external splash page

IP Address or Domain Name

IP Address | Domain Name	Action

No white list available

Note

For more information about XMS-Cloud EasyPass settings and onboarding, please refer to latest XMS-Cloud Help document.

Note

For more information about cnMaestro Guest Access Portal and onboarding, please refer

https://docs.cloud.cambiumnetworks.com/help/2.4.0/index.htm#UG_files/WiFi/Guest%20Access.htm%3FTocPath%3DServices%253A%2520cnPilot%2520Guest%2520Access%2520%7C_____0

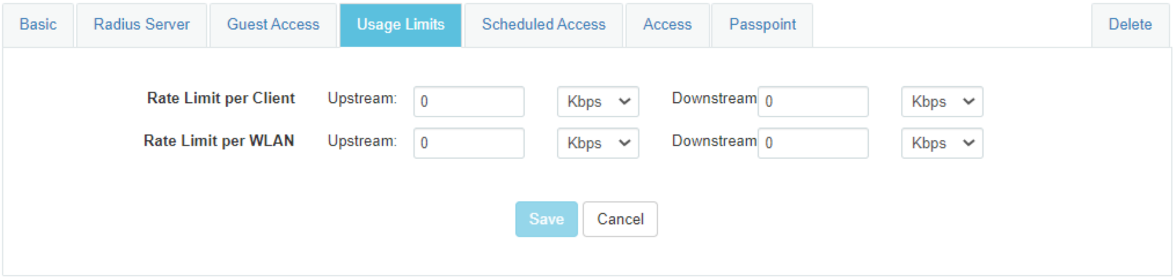
Table 20 :Configure: WLAN > Usage Limits parameters

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

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

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

Figure 19 : *Configure: WLAN > Usage Limits parameters*



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

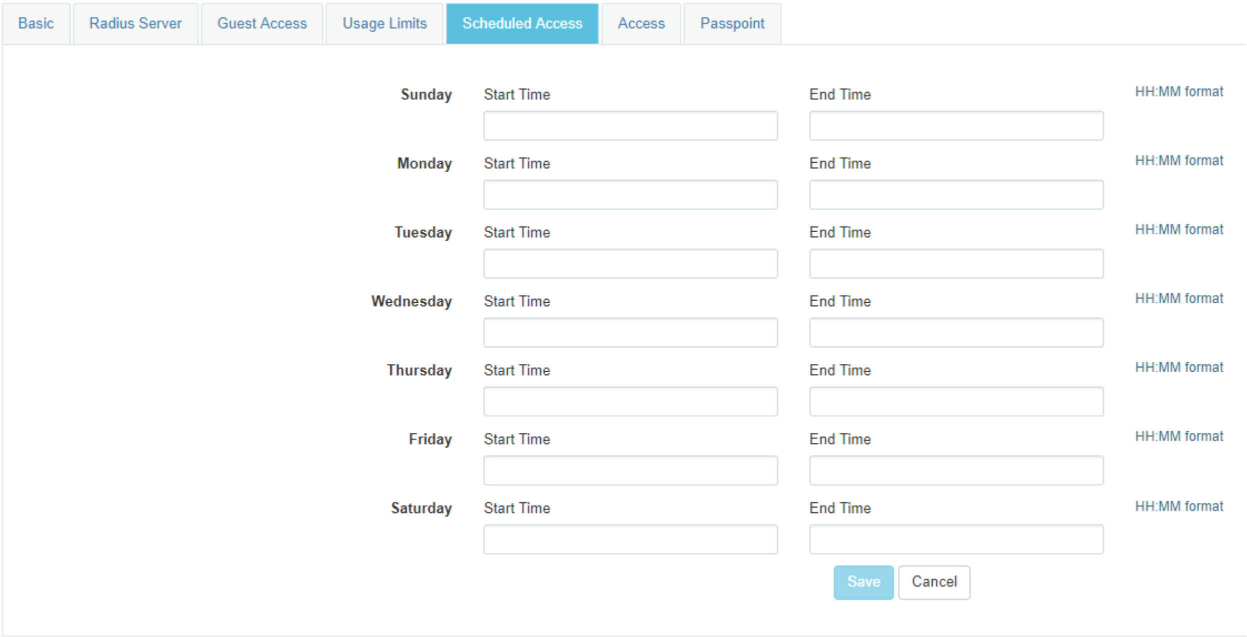
Table 21 :Configure: WLAN > Scheduled Access parameters

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

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

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

Figure 20 : *Configure: WLAN > Scheduled Access parameters*



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

Table 22 :Configure: WLAN > Access parameters

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

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

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

Table 23 :Configure: WLAN > Passpoint parameters

Parameters	Description	Range	Default
Configuration > Hotspot2.0 / Passpoint			
Enable	Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning.	—	Disabled
DGAF	Downstream Group Addressed Forwarding, when enabled the WLAN doesn't transmit any multicast and broadcast packets.	—	Disabled
ANQP	ANQP domain identifier included when the HS 2.0 indication element is	0-	0

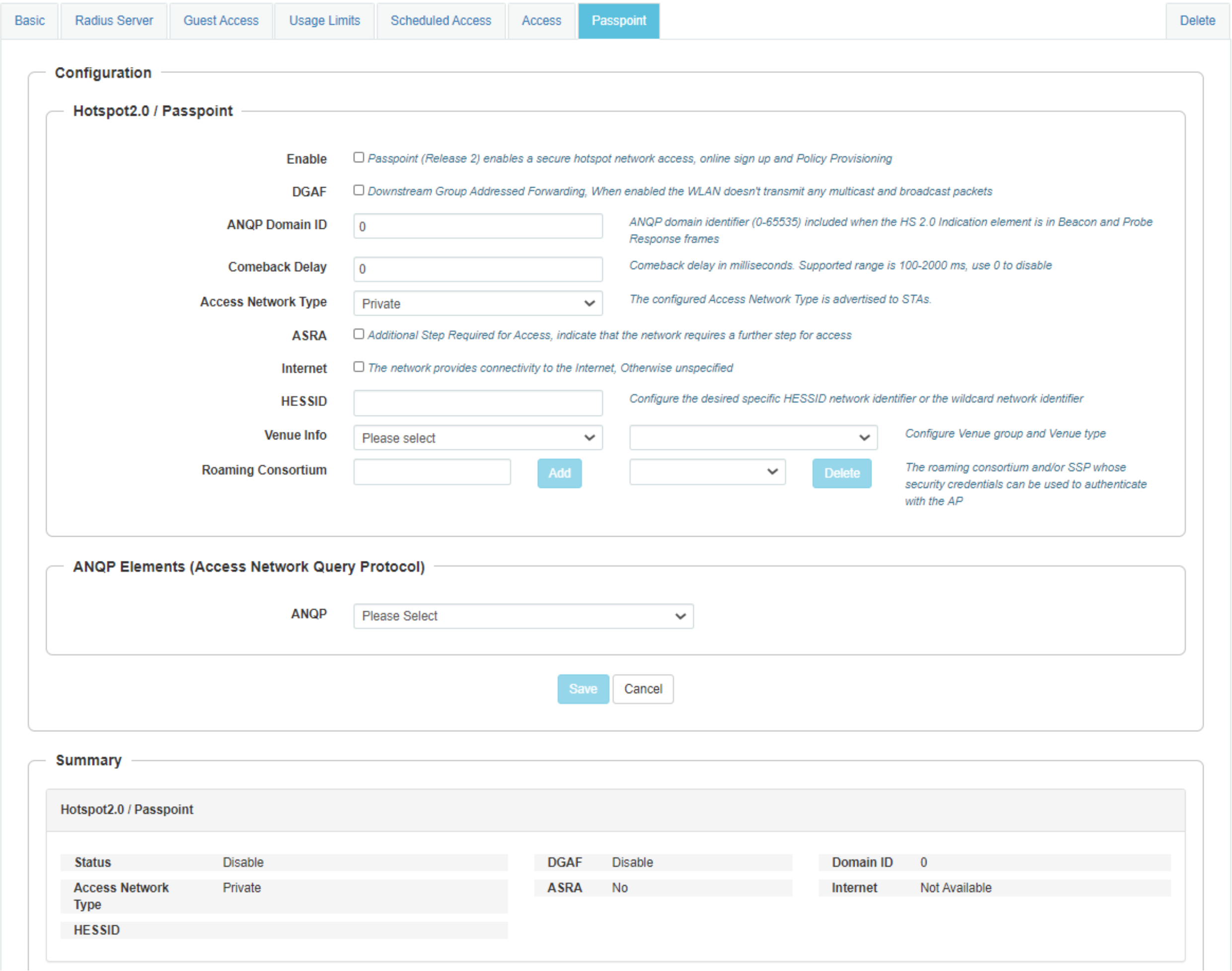
Parameters	Description	Range	Default
Domain ID	in Beacon and Probe Response frames.	65535	
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with Guest • Test • Wildcard	—	Private
ASRA	Indicates that the network requires a further step for access.	—	Disabled
Internet	The network provides connectivity to the Internet if not specified.	—	Disabled
HESSID	Configures the desired specific HESSID network identifier or the wildcard network identifier.	—	—
Venue Info	Configure venue group and venue type.	—	—
Roaming Consortium	The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.	—	—
ANQP Elements	Select any one of the following: • 3GPP Cellular Network Information • Connection Capability • Domain Name List • Icons • IP Address Type information • NAI Realm List • Network Authentication Type • Operating Class Indication • Operator Friendly Names • OSU Provider List • Venue Name Information • WAN Metrics	—	—

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

1. Select **Enable** checkbox to enable passpoint functionality.
2. Select **DGAF** checkbox to enable Downstream Group Addressed Forwarding functionality.
3. Enter the domain identifier value in **ANQP Domain ID** textbox.
4. Enter **Comeback Delay** in milliseconds in the textbox.
5. Choose the **Access Network Type** value from the drop-down list.
6. Enable **ASRA** checkbox if the network requires additional steps for access.

7. Enable **Internet** checkbox for the network to provide connectivity to the Internet.
8. Enter the **HESSID** to configure the desired specific HESSID network identifier or the wildcard network identifier.
9. Select **Venue Info** from the drop-down list.
10. To add **Roaming Consortium** value, enter the value in the textbox and click Add. To delete a **Roaming Consortium** value, select from the drop-down list and click **Delete**.
11. Click **Save**.

Figure 21 : *Configure: WLAN > Passpoint parameters*



Configuration

Hotspot2.0 / Passpoint

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

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

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

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

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

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

Internet ☐ The network provides connectivity to the Internet, Otherwise unspecified

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

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

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

ANQP Elements (Access Network Query Protocol)

ANQP: Please Select

Summary

Hotspot2.0 / Passpoint

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

Chapter 9: Configuration - Network

This chapter describes the following topics:

- Overview
- Configuring Network parameters

Overview

This chapter gives an overview of Enterprise Wi-Fi AP configurable parameters related to LAN, VLAN, Routes, DHCP server, ACL and Firewall.

Configuring Network parameters

Enterprise Wi-Fi AP network configuration parameters are segregated into following sections:

- VLAN
- Routes
- Ethernet Ports
- Security
- DHCP

IPv4 network parameters

VLAN

Table 24 :Configure: Network > VLAN > IPv4 parameters

Parameters	Description	Range	Default
VLAN > IPv4			
Edit	Provision to select the VLAN interface that user is intended to view/update configuration.	—	VLAN 1
Address	Provision to configure mode of IPv4 address configuration for an interface selected. Two modes are supported: 1. DHCP This is the default mode in which Enterprise Wi-Fi AP device tries to obtain IPv4 address from DHCP server. 2. Static IP User must explicitly configure IPv4 address and Netmask for a VLAN selected.	—	DHCP
NAT	This option is preferable when you defined local DHCP servers. This		Disabled

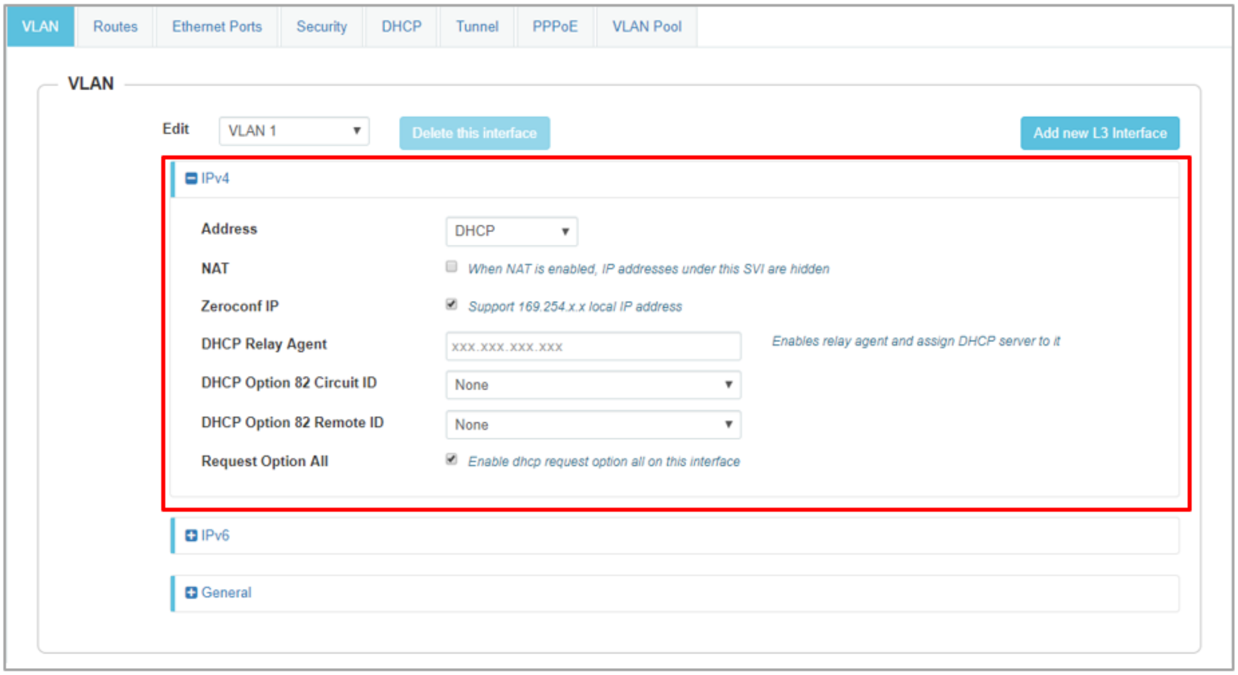
Parameters	Description	Range	Default
	option when selected, traffic from wireless stations are NAT'ed to the default gateway interface IP.		
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only on VLAN1 configuration section. If VLAN 1 is not allowed in Ethernet interfaces,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

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

To configure VLAN IPv4:

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

Figure 22 : *Configure: Network > VLAN > IPv4 parameters*



Edit: VLAN 1

Address	DHCP
NAT	□ When NAT is enabled, IP addresses under this SVI are hidden
Zeroconf IP	☑ Support 169.254.x.x local IP address
DHCP Relay Agent	xxx.xxx.xxx.xxx — Enables relay agent and assign DHCP server to it
DHCP Option 82 Circuit ID	None
DHCP Option 82 Remote ID	None
Request Option All	☑ Enable dhcp request option all on this interface

MTU

Enterprise Wi-Fi AP devices honour MTU advertised in DHCP Option 26. Below are the criteria for selecting MTU:

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

```
XV3-8-6E3A07(config)# interface vlan <VLAN ID>
XV3-8-6E3A07(config-vlan-<VLAN ID>)# ip dhcp mtu
XV3-8-6E3A07(config-vlan-<VLAN ID>)# save
```

DHCP Client Options

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

Table 25 :DHCP Options

Options	Description	Usage	Reference CLI
Option 1	The subnet mask option specifies the client's subnet mask as per RFC 950.	Based on state of “Request Option All”, device chooses subnet mask from respective VLAN interface.	*show ip route*
Option 3	This option specifies a list of IP addresses for routers on the client's subnet.	Based on state of “Request Option All”, device chooses route learnt from respective VLAN interface. Only first route is honored	*show ip route*
Option 6	The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers SHOULD be listed in order of preference.	Based on state of “Request Option All”, device chooses subnet mask from respective VLAN interface. Top two DNS servers are honored by Enterprise Wi-Fi AP device.	*show ip name-server*
Option 15	This option specifies the domain name that client should use when resolving hostnames via the Domain Name System.	More details are provided in Option 15.	*show ip dhcp-client info*
Option 26	This option specifies MTU size in a network.	More details are provided in MTU.	*show ip dhcp-client info*
Option 28	This option specifies the broadcast address that client should use	Broadcast address learnt for all VLAN interfaces are used respectively as per standards	*show ip dhcp-client-info*
Option 43	This option is used to help the AP in obtaining cnMaestro IP address from the DHCP server while DHCP request to get an IP address is sent to the DHCP server.	More details are provided in Option 43 (cnMaestro On- Premises 2.4.0 User Guide).	*show ip dhcp-client info*
Option 51	This option is used in a client request to allow the client to request a lease time for the IP address. In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.	Enterprise Wi-Fi AP renew leases for all VLAN interfaces configured based on lease time that has been learned from DHCP server.	*show ip dhcp-client info*
Option 54	DHCP clients use the contents of the 'server identifier' field as the destination address for any DHCP messages unicast to the DHCP server.	Enterprise Wi- Fi AP learns DHCP server IP for all VLAN interfaces configured.	*show ip dhcp-client info*
Option 60	This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.	For Enterprise Wi-Fi AP device, value is updated as Cambium-Wi-Fi-AP.	*show ip dhcp-client info*

Routing & DNS

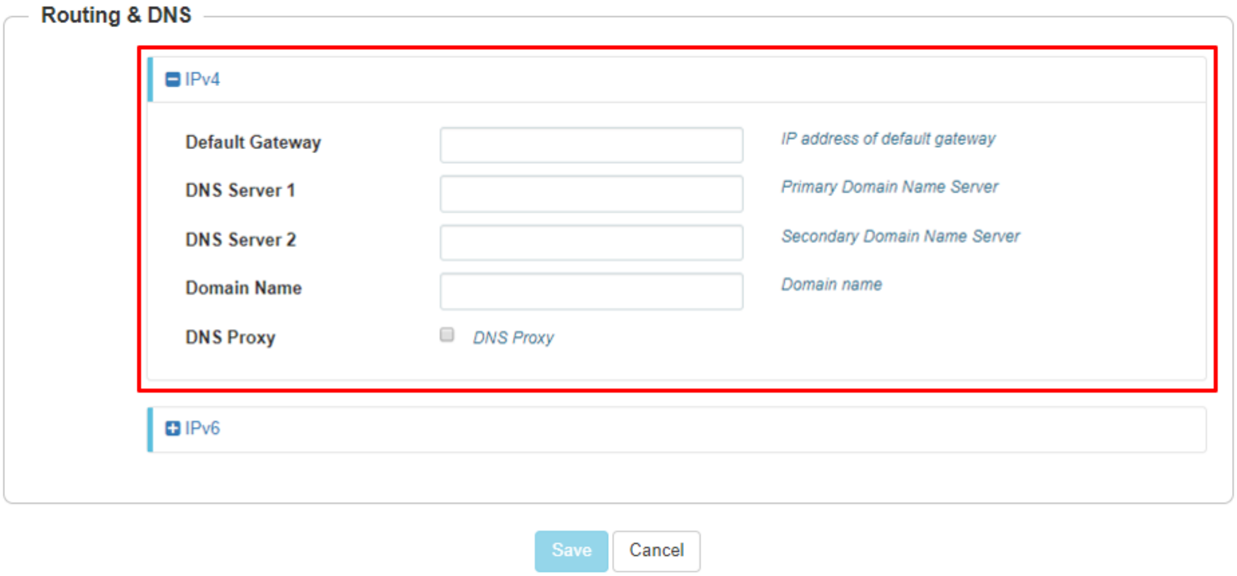
Table 26 :Configure: Network > VLAN > Routing & DNS > IPv4 parameters

Parameters	Description	Range	Default
Default Gateway	Provision to configure default gateway. If this is provided, Enterprise Wi-Fi AP device installs this gateway as this is the highest priority.	—	—
DNS Server	Provision to configure Static DNS server on Enterprise Wi-Fi AP device. Maximum of two DNS servers can be configured.	—	—
Domain Name	Provision to configure Domain Name. If this is provided, Enterprise Wi-Fi AP device installs this Domain Name as this is highest priority.	—	—
DNS Proxy	Enterprise Wi-Fi AP device can act as DNS proxy server when this parameter is enabled.	—	Disabled

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

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

Figure 23 : *Routing & DNS > IPv4 parameters*



Routes

Table 27 :Configure: Network > Routes> IPv4 parameters

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

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

To configure Gateway Source Precedence:

1. Select STATIC or DHCPC from the Gateway Source Precedence checkbox.
2. Click Save.

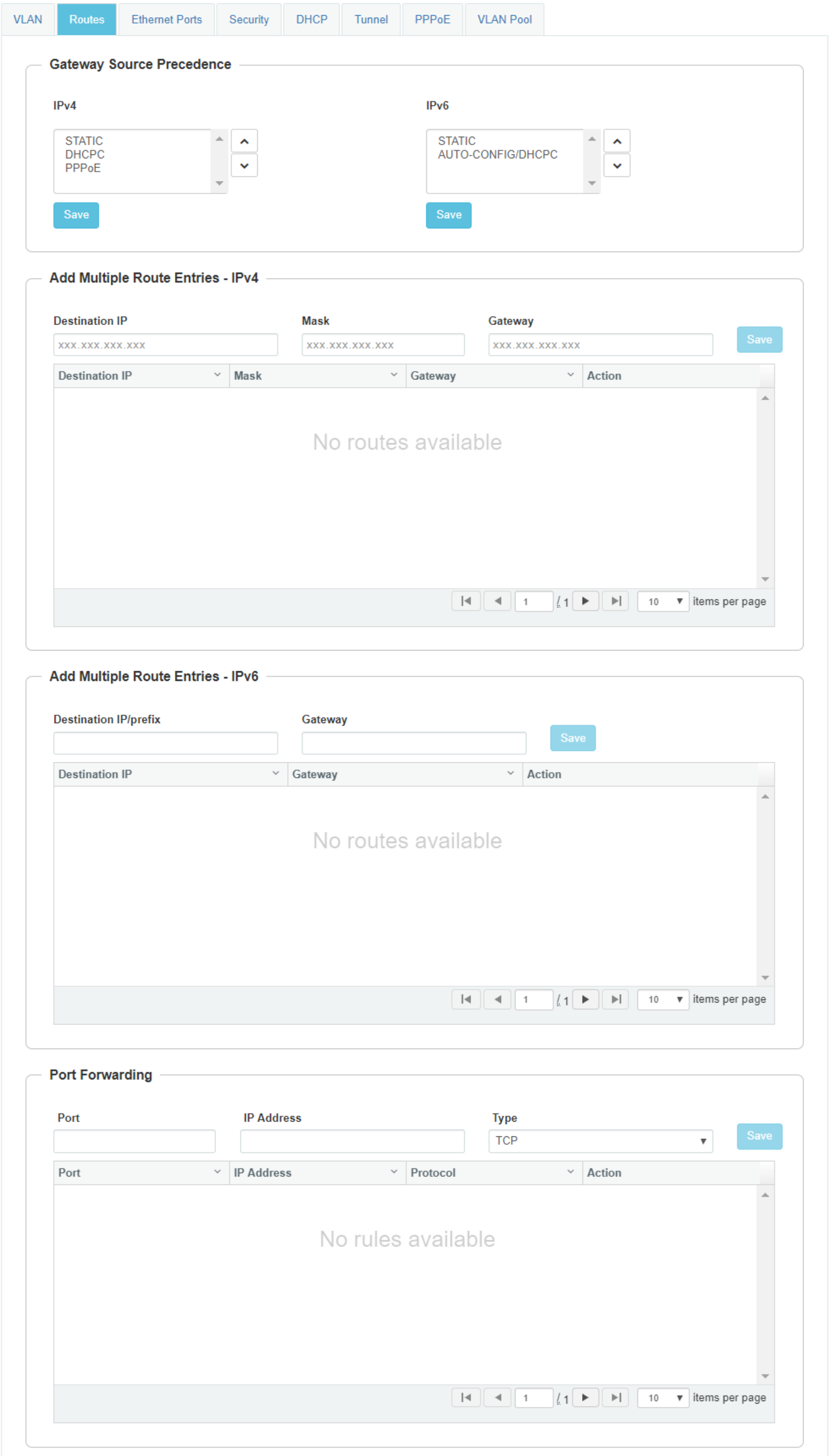
To configure Add Multiple Route Entries:

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

To configure Port Forwarding:

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

Figure 24 : *Routes > IPv4 parameters*



Gateway Source Precedence

IPv4: STATIC, DHCPC, PPPoE

IPv6: STATIC, AUTO-CONFIG/DHCPC

Add Multiple Route Entries - IPv4

Destination IP: xxx.xxx.xxx.xxx
Mask: xxx.xxx.xxx.xxx
Gateway: xxx.xxx.xxx.xxx

Destination IP	Mask	Gateway	Action

No routes available

1 / 1 · 10 items per page

Add Multiple Route Entries - IPv6

Destination IP/prefix
Gateway

Destination IP	Gateway	Action

No routes available

1 / 1 · 10 items per page

Port Forwarding

Port
IP Address
Type: TCP

Port	IP Address	Protocol	Action

No rules available

1 / 1 · 10 items per page

Ethernet Ports

Table 28 :Configure: Network > Ethernet Ports parameters

Parameters	Description	Range	Default
Ethernet	Enterprise Wi- Fi AP devices Ethernet port is provisioned to operate in following modes: 1. Access Single VLAN Single VLAN traffic is allowed in this mode. 2. Trunk Multiple VLANs Multiple VLANs are supported in this mode.	—	Access
ACL			
Precedence	Provision to configure index of ACL rule. Packets are validated and processed based on precedence value configured.	1-256	1
Policy	Provision to configure whether to permit or deny traffic.	Deny/Permit	Deny
Direction	Provision to apply the ACLs rules configured either in any direction or specific direction.	—	In
Type	Enterprise Wi-Fi AP devices support three layers of ACLs. A rule can be configured as below: • IP • MAC • Proto	—	IP
Source IP/Mask	This option is available when ACL type is configured to an IP address. This field helps user to configure if rule needs to be applied for a single IP address or range of IP addresses.	—	—
Destination IP/Mask	This option is available when ACL type is configured to an IP address. This field helps user to configure if rule needs to be applied for a single IP address or range of IP addresses.	—	—
Source MAC/Mask	This option is available when ACL type is configured to a MAC address. This field helps user to configure if rule needs to be applied for a single device MAC address or range of MAC addresses.	—	—
Destination MAC/Mask	This option is available when ACL type is configured to MAC address. This field helps user to configure if rule needs to be applied for a single device MAC address or range of MAC addresses.	—	—
Protocol	This option is available when user selects ACL type as proto. User can select following protocols: • TCP	—	TCP

Parameters	Description	Range	Default
	• UDP • ICMP • Any		
Source Port	Provision to apply ACL with combination of protocol and port.	—	—
Destination Port	Provision to apply ACL with combination of protocol and port.	—	—
Description	To make administrator easy to understand, a text string can be added for each ACL rule.	—	—

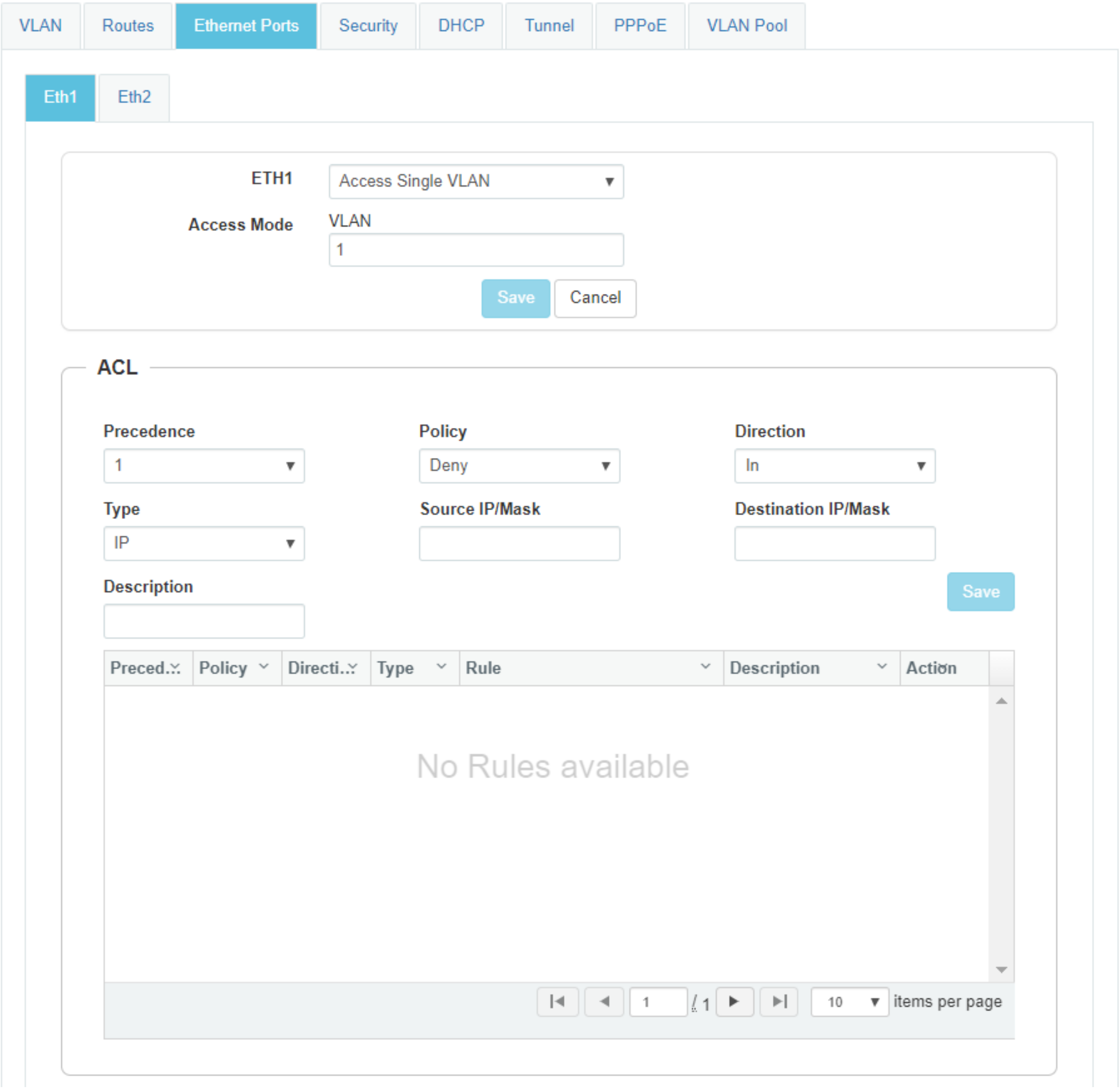
To configure the above parameter, navigate to the Configure > Network > Ethernet Ports tab and provide the details as given below:

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

To configure ACL:

1. Select Precedence from the drop-down list.
2. Select type of Policy from the drop-down list.
3. Select Direction from the drop-down list.
4. Select Type from the drop-down list.
5. Enter IP address of source in the Source IP/Mask textbox.
6. Enter IP address of destination in the Destination IP/Mask textbox.
7. Enter Description in the textbox.
8. Click Save.

Figure 25 : *Configure: Network > Ethernet Ports parameters*



ETH1: Access Single VLAN

Access Mode: VLAN 1

ACL

Precedence: 1

Policy: Deny

Direction: In

Type: IP

Source IP/Mask:

Destination IP/Mask:

Description:

Preced...	Policy	Directi...	Type	Rule	Description	Action

No Rules available

1 / 1 — 10 items per page

General network parameters

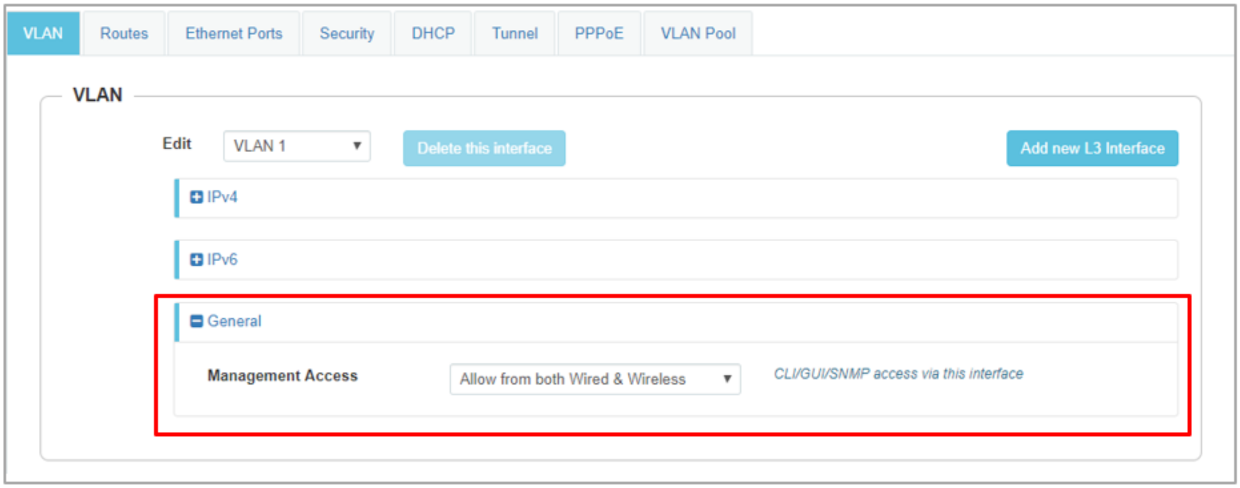
Table 29 :Configure: Network > VLAN > General parameters

Parameters	Description	Range	Default
Management Access	Provision to restrict the access of device in all modes CLI (Telnet, SSH), GUI (HTTP, HTTPs) and SNMP. User can configure restriction of device access as follows: • Block	—	Allow from both Wired and Wireless

Parameters	Description	Range	Default
	• Allow from Wired • Allow from both wired and wireless		

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

Figure 26 : *Configure: Network > VLAN > General parameters*



Edit: VLAN 1

Management Access: Allow from both Wired & Wireless

DHCP

Table 30 :Configure: Network > DHCP parameters

Parameters	Description	Range	Default
Edit	Provision to select DHCP Pool if multiple Pools are defined on Enterprise Wi-Fi AP device.	—	—
Address Range	User can configure start and end addresses for a DHCP Pool selected from the drop-down box.	—	—
Default Router	Provision to configure next hop for a DHCP pool selected from drop-down box.	—	—
Domain Name	Provision to configure domain name for a DHCP pool selected from drop-down box.	—	—
DNS Address	Provision to configure DNS server for a DHCP pool selected from drop-down box.	—	—
Network	Provision to configure Network ID for a DHCP pool selected from drop-down box.	—	—
Lease	Provision to configure lease for a DHCP pool selected from drop-down box.	—	—

Parameters	Description	Range	Default
Add Bind List			
	For every DHCP pool configured, user can bind MAC and IP from the address pool defined, so that wireless station gets same IP address every time they connect. Following parameters are required to bind IP address: • MAC Address • IP Address	—	—

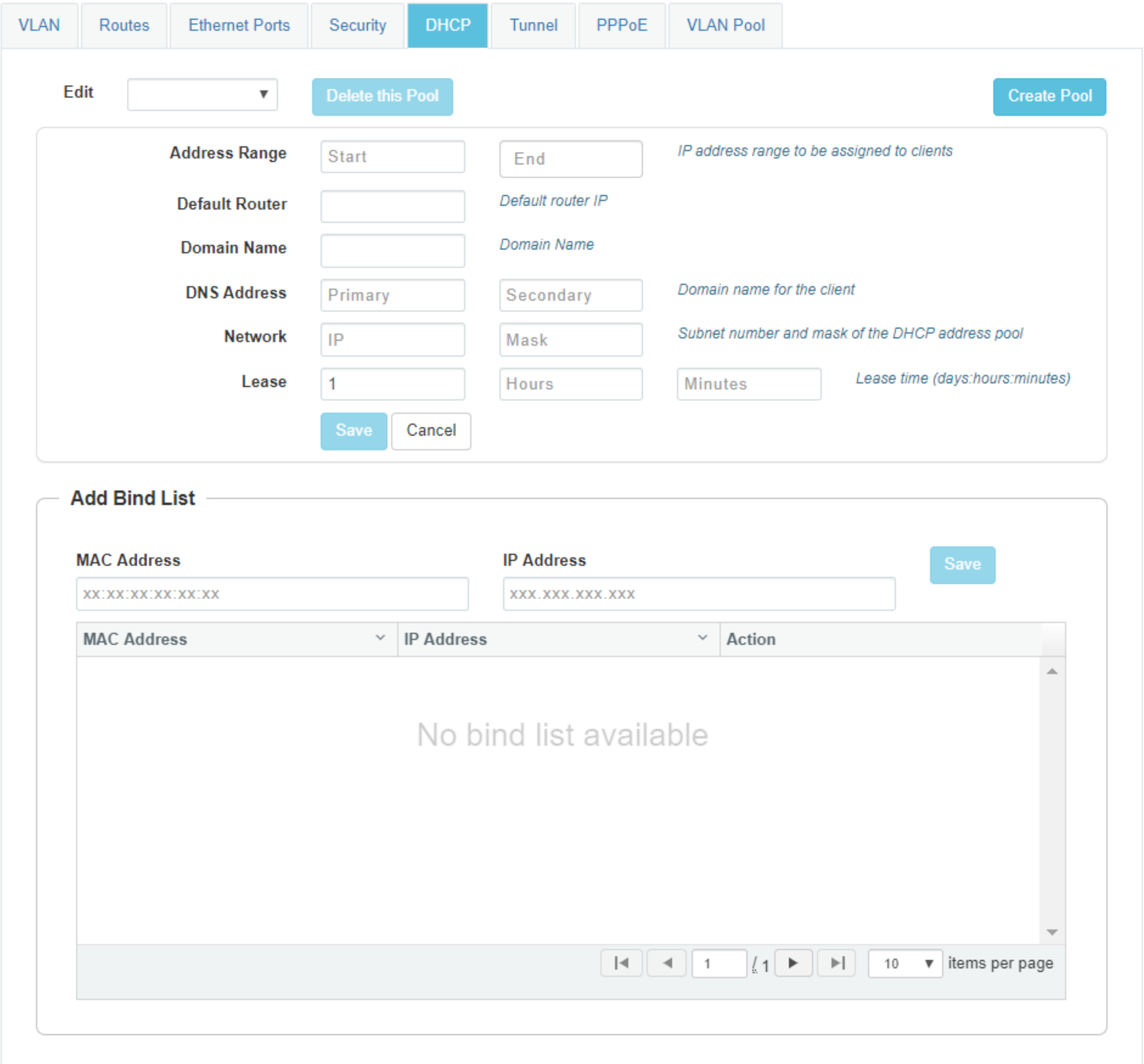
To configure the above parameter, navigate to the Configure > Network > DHCP tab and provide the details as given below:

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

To configure Add Bind List:

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

Figure 27 : *Configure: Network > DHCP parameters*



Edit ▼

Address Range	Start	End	*IP address range to be assigned to clients*	
Default Router		*Default router IP*		
Domain Name		*Domain Name*		
DNS Address	Primary	Secondary	*Domain name for the client*	
Network	IP	Mask	*Subnet number and mask of the DHCP address pool*	
Lease	1	Hours	Minutes	*Lease time (days:hours:minutes)*

Add Bind List

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

IP Address: xxx.xxx.xxx.xxx

MAC Address	IP Address	Action

No bind list available

1 / 1 10 ▼ items per page

Chapter 10 : Configuration - Services

This chapter describes the following topics:

- Overview
- Configuring Services

Overview

This chapter gives an overview of Enterprise Wi-Fi AP configurable parameters related to LDAP, NAT Logging, Location API and Speed Test.

Configuring Services

This section provides information on how to configure the following services on Enterprise Wi-Fi AP.

- LDAP
- APIs
- Location API
- Speed Test

LDAP

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

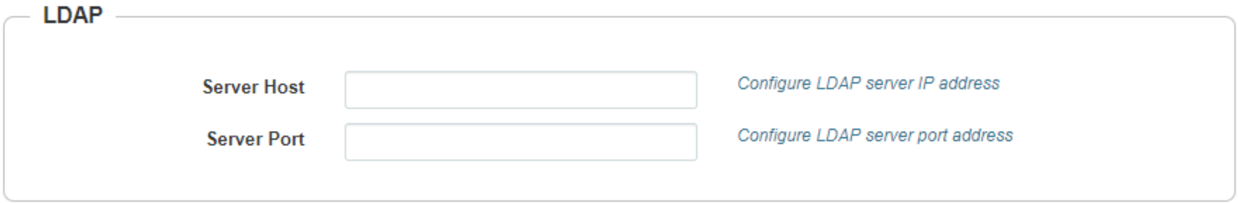
Table 31 :Configure: Services > LDAP parameters

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

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

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

Figure 28 : *Configure: Services > LDAP parameters*



LDAP

Server Host — Configure LDAP server IP address

Server Port — Configure LDAP server port address

APIs

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

NAT Logging

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

Table 32 :PDU type code: 0x82

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

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

Table 33 :NAT Logging Packet Structure

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

Length	Description
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.

Below table lists the fields that are displayed in Configuration > Services > NAT Logging tab:

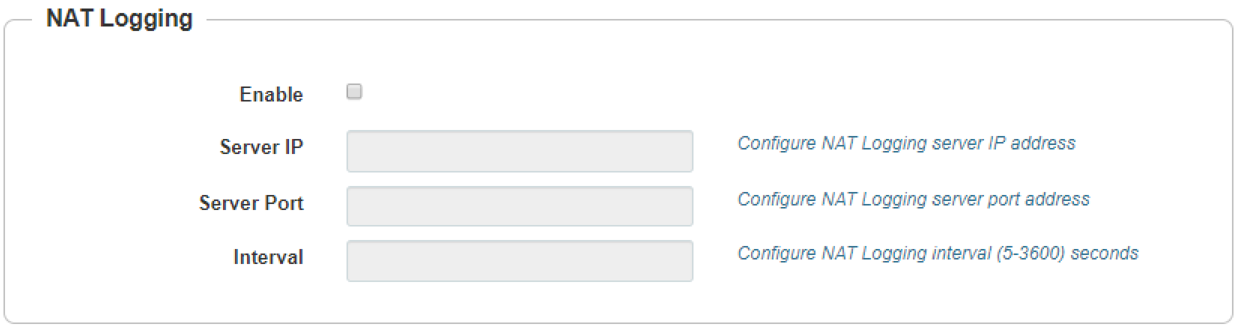
Table 34 :Configure: Services > NAT Logging parameters

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

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

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

Figure 29 : *Configure: Services > NAT Logging parameters*



NAT Logging

Enable □

Server IP — Configure NAT Logging server IP address

Server Port — Configure NAT Logging server port address

Interval — Configure NAT Logging interval (5-3600) seconds

Speed Test

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

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

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

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

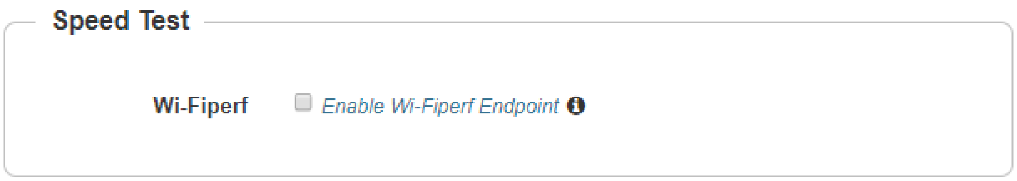
Table 35 lists the fields that are displayed in the Configuration > Services > Speed Test tab:

Table 35 :Configure: Services > Speed Test parameters

Parameters	Description	Range	Default
wifiperf	Provision to enable wifiperf functionality.	—	Disabled

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

Figure 30 : *Configure: Services > Speed Test parameters*



Speed Test

Wi-Fiperf □ *Enable Wi-Fiperf Endpoint* ℹ

User Group

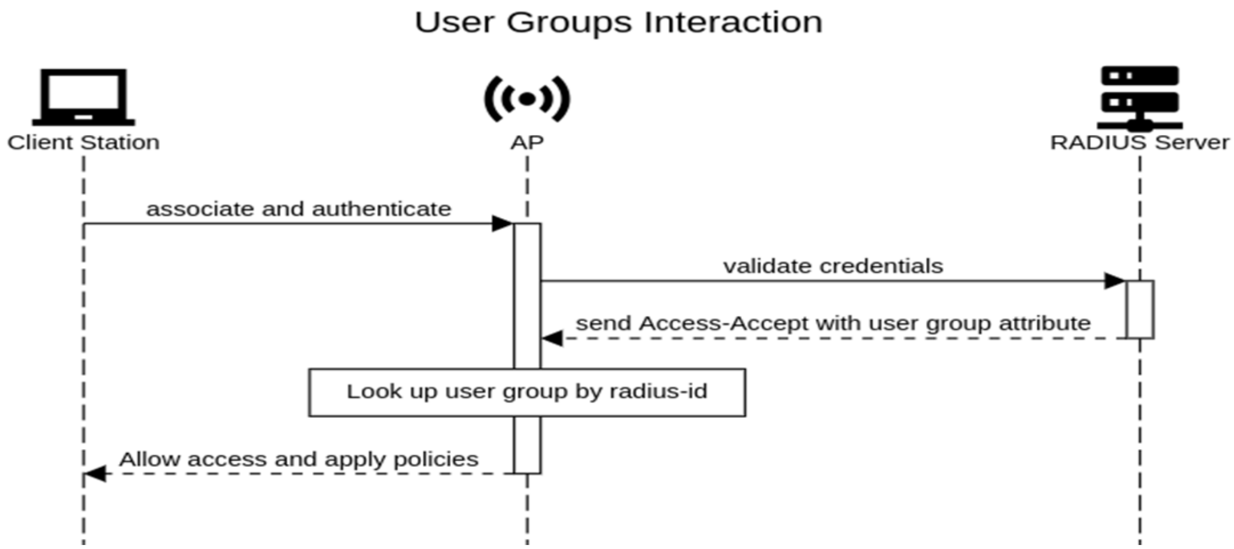
Some policies, like VLAN, require many RADIUS attributes to be sent by the RADIUS server and processed by the AP. Some wireless network administrators do not have administrative access to the RADIUS server, so making changes to wireless policies would require waiting for the RADIUS administrator to make changes.

To simplify wireless administration and streamline changes, a feature called User Groups is provided that allows the wireless administrator to apply a set of wireless policies to a user based on a single RADIUS attribute. This eliminates the need for administrative rights on the RADIUS server and simplifies applying complex policies to end-user stations.

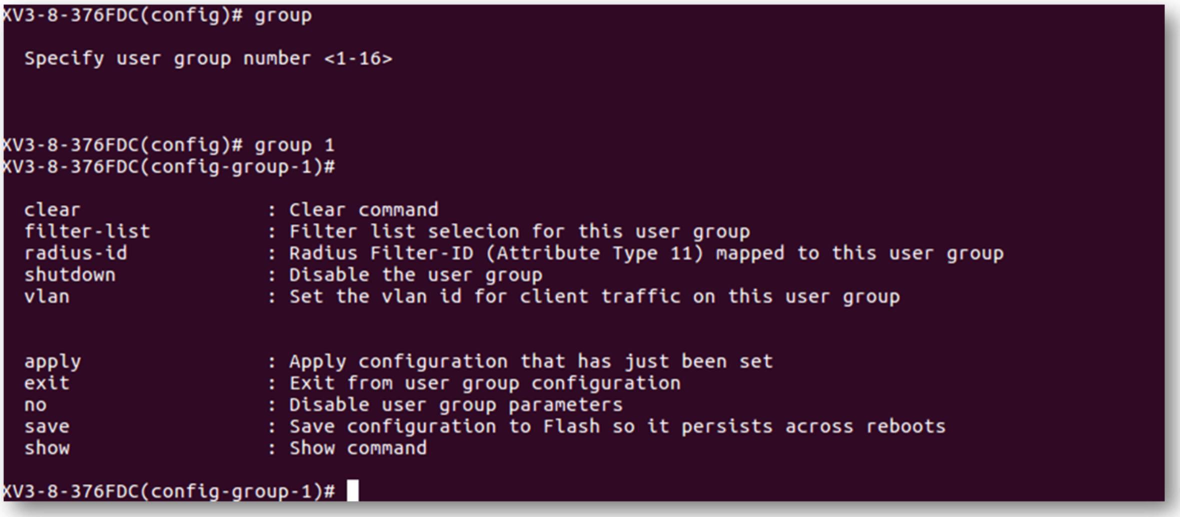
A user group can also be assigned to a station based on the device type. This approach is dependent on the accuracy and completeness of device identification functionality, which is not guaranteed to be accurate or exhaustive.

The User Group feature is natively supported by XMS Cloud.

Figure 31 : *User Groups interaction*

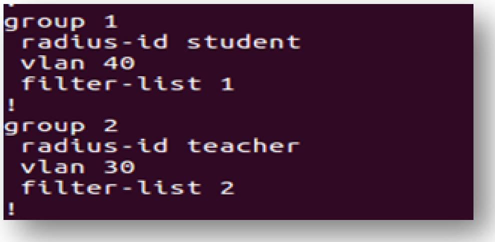

User Groups Interaction
Client Station
AP
RADIUS Server
associate and authenticate
validate credentials
send Access-Accept with user group attribute
Look up user group by radius-id
Allow access and apply policies

CLI Configuration:



```
XV3-8-376FDC(config)# group

  Specify user group number <1-16>


XV3-8-376FDC(config)# group 1
XV3-8-376FDC(config-group-1)#

  clear                   : Clear command
  filter-list             : Filter list selecion for this user group
  radius-id               : Radius Filter-ID (Attribute Type 11) mapped to this user group
  shutdown                : Disable the user group
  vlan                    : Set the vlan id for client traffic on this user group


  apply                   : Apply configuration that has just been set
  exit                    : Exit from user group configuration
  no                      : Disable user group parameters
  save                    : Save configuration to Flash so it persists across reboots
  show                    : Show command

XV3-8-376FDC(config-group-1)#
```

Example:



```
group 1
 radius-id student
 vlan 40
 filter-list 1
!
group 2
 radius-id teacher
 vlan 30
 filter-list 2
!
```

User group properties and actions

A user group supports the following properties and actions:

Command	Description
shutdown	Disable this User Group
radius-id	Radius Filter-ID (Attribute Type 11) mapped to this User Group
no shutdown	Enable this User Group
no group <index>	Delete User Group

User group policies

The policies available in a user group configuration are a subset of those for an SSID. The most commonly used policies are filter-list and VLAN.

Policy	Description
filter-list <index>	Filter List setting for this User Group
vlan	VLAN associated with this User Group

Chapter 11: Operations

This chapter describes the following topics:

- Overview
- Firmware update
- System
- Configuration

Overview

This chapter gives an overview of Enterprise Wi-Fi AP administrative functionalities such as Firmware update, System and Configuration.

Firmware update

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

Note

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

Table 36 lists the fields that are displayed in the Operations > Firmware update tab:

Table 36 :Configure: Operations > Firmware update parameters

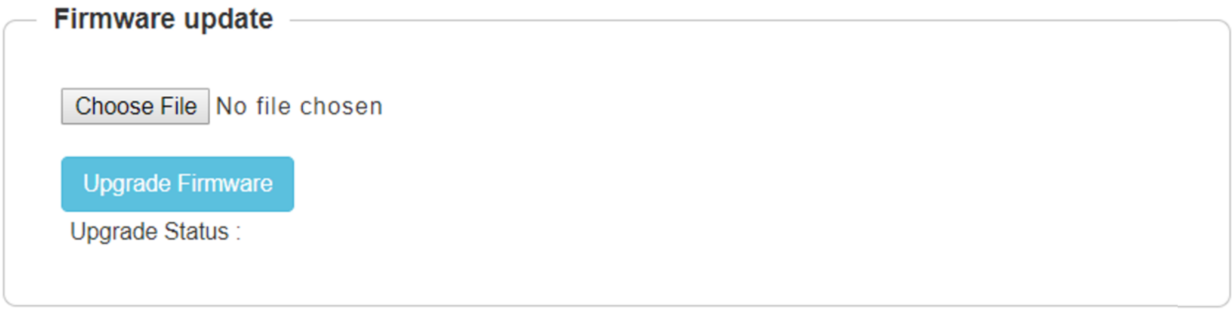
Parameters	Description	Range	Default
Choose File	Provisions to select upgrade file.	—	—
Upgrade Firmware	Provision to initiate upgrade once file is selected.	—	—

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

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

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

Figure 32 : *Configure: Operations > Firmware update parameters*


Firmware update

Choose File No file chosen

Upgrade Firmware

Upgrade Status :

System

This section provides multiple troubleshooting tools provided by Enterprise Wi-Fi AP.

Table 37 lists the fields that are displayed in the Operations > System tab:

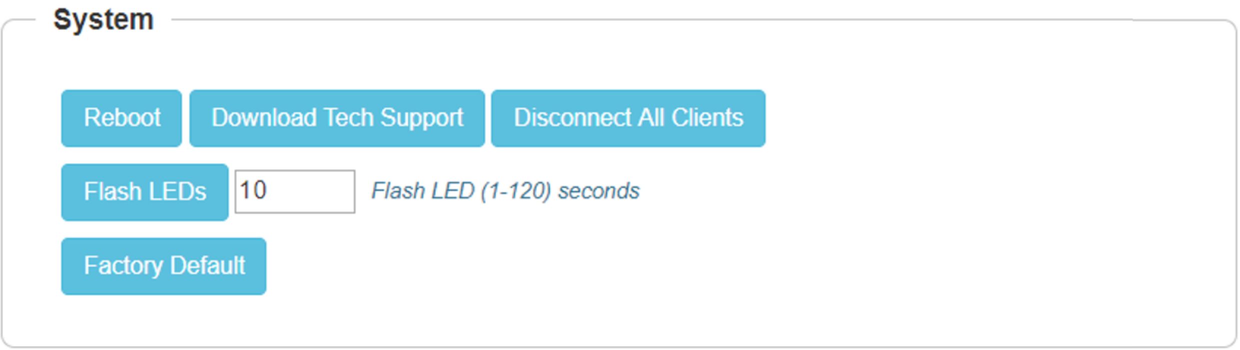
Table 37 :Configure: Operations > System parameters

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

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

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

Figure 33 : *Configure: Operations > System parameters*


System

Reboot | Download Tech Support | Disconnect All Clients

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

Factory Default

Configuration

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

Below table lists the fields that are displayed in the Operations > Configuration tab:

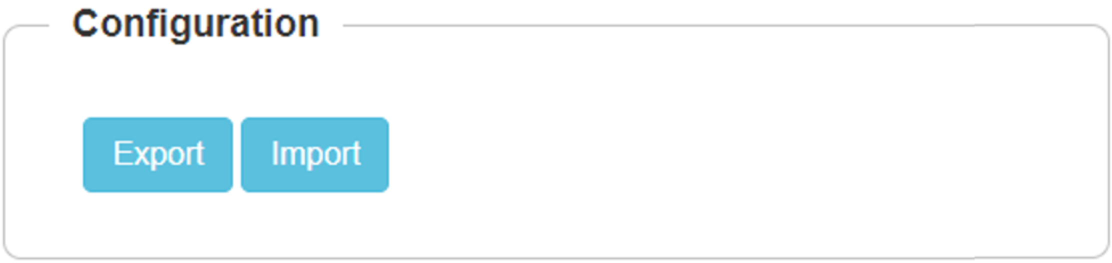
Figure 34 : *Configure: Operations > Configuration parameters*

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

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

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

Figure 35 : *Configure: Operations > Configuration parameters*



Chapter 12: Troubleshoot

This section provides detailed information about troubleshooting methods supported by Enterprise Wi-Fi APs. Troubleshooting methods supported by Enterprise Wi-Fi AP devices are categorized as below:

- Logging
  - Events
  - Debug Logs
- Radio Frequency
  - Wi-Fi Analyzer
- Packet capture
- Performance
  - Wi-Fi Perf Speed Test
  - Connectivity

Logging

Enterprise Wi-Fi AP devices supports multi-level logging, which will ease to debug issues.

Events

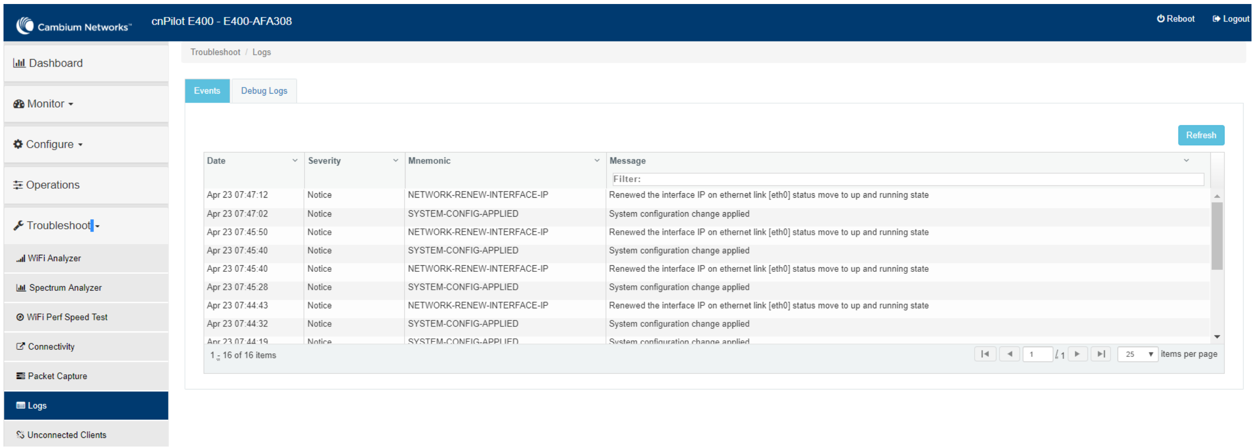
Enterprise Wi-Fi AP devices generates events that are necessary for troubleshooting across various modules. Below is the list of modules, Enterprise Wi-Fi AP device generates events for troubleshoot.

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

- Reboot
- Guest Access

Events are available at Troubleshoot > Logs > Events.

Figure 36 : *Troubleshoot > Logs > Events*



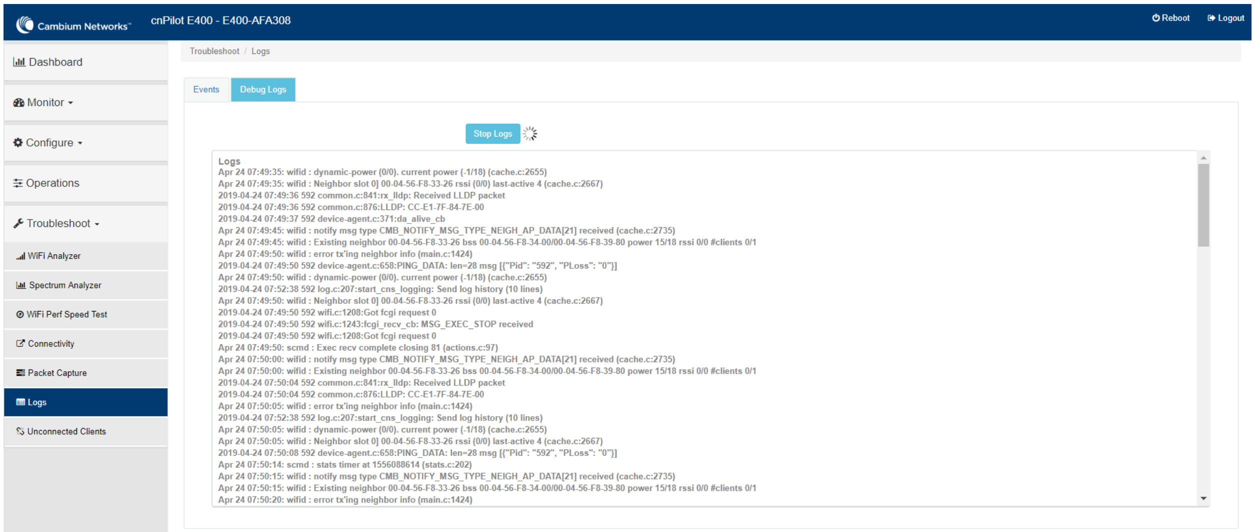
Date	Severity	Mnemonic	Message
Apr 23 07:47:12	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:47:02	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:45:50	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:45:40	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:45:40	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:45:28	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:44:43	Notice	NETWORK-RENEW-INTERFACE-IP	Renewed the interface IP on ethernet link [eth0] status move to up and running state
Apr 23 07:44:32	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied
Apr 23 07:44:19	Notice	SYSTEM-CONFIG-APPLIED	System configuration change applied

Debug Logs

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

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

Figure 37 : *Troubleshoot > Logs > Debug Logs*



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

Radio Frequency

Wi-Fi Analyzer

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

- Interference

This tool shares more information of each channel as below:

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

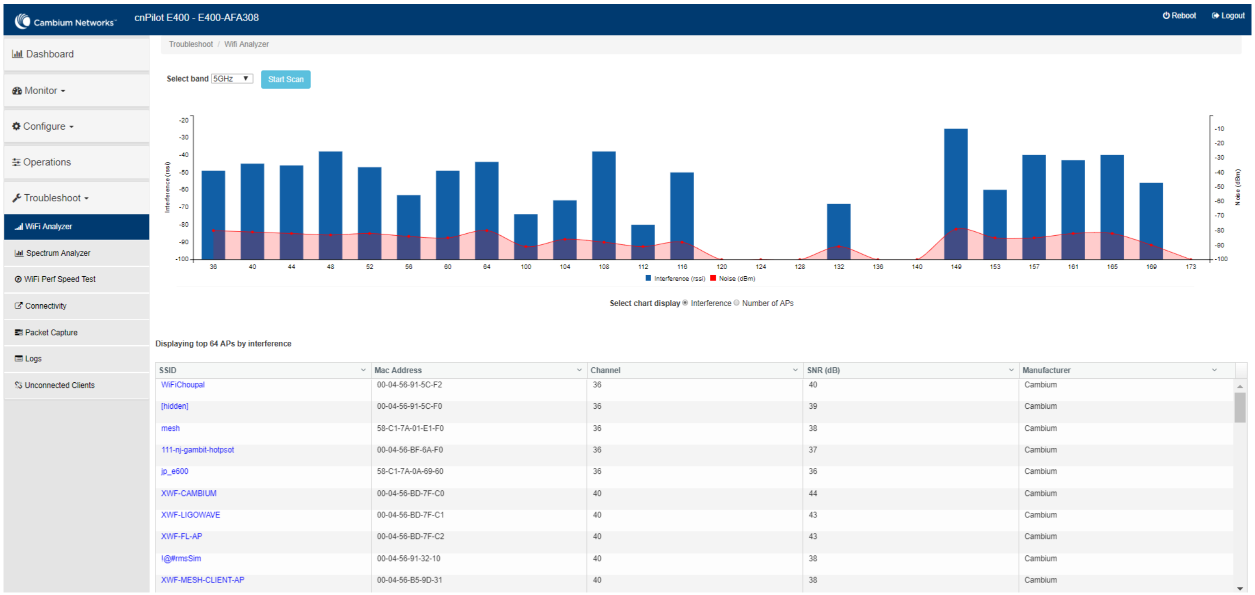
- Number of APs

This tool shares more information of each channel as below:

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

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

Figure 38 : *Troubleshoot > Wi-Fi Analyzer > Interference Mode*



Select band 5GHz

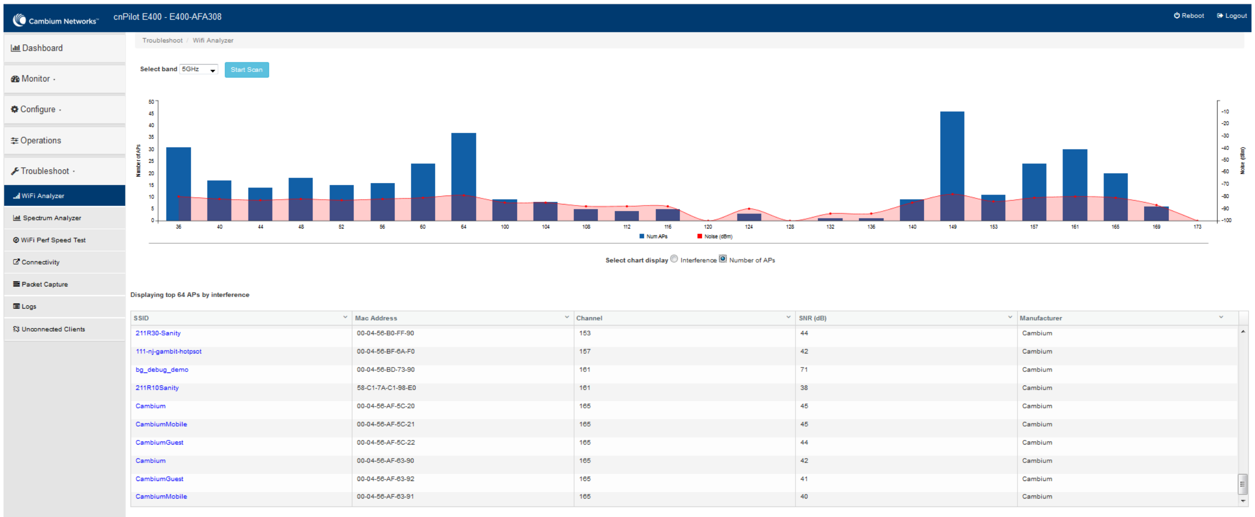
Select chart display ● Interference ○ Number of APs

Displaying top 64 APs by interference

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

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

Figure 39 : *Troubleshoot > Wi-Fi Analyzer > Number of APs Mode*



Select band 5GHz

Select chart display ○ Interference ● Number of APs

Displaying top 64 APs by interference

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

Packet capture

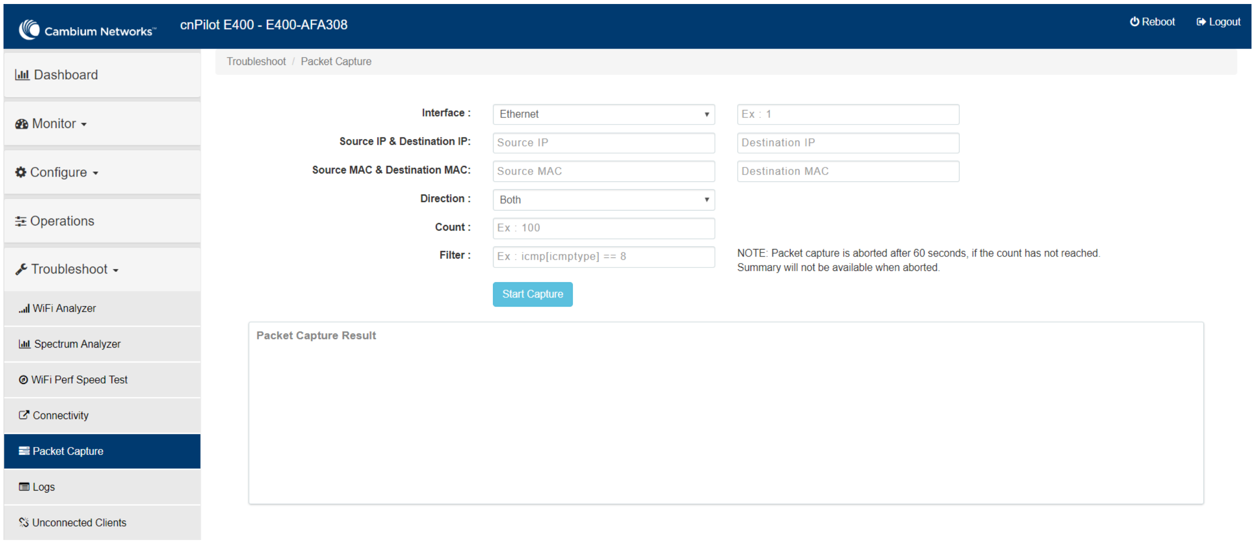
Allows the administrator to capture all packets on a specified interface. A decode of the packet indicating the network addresses, protocol types etc is displayed. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, port number etc. The number of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

Enterprise Wi-Fi AP device allows packet capture on following interfaces:

- WLAN
- Ethernet
- VLAN
- SSID

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

Figure 40 : *Troubleshoot > Packet Capture page*



Interface : Ethernet | Ex : 1

Source IP & Destination IP: Source IP | Destination IP

Source MAC & Destination MAC: Source MAC | Destination MAC

Direction : Both

Count : Ex : 100

Filter : Ex : icmp[icmptype] == 8

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

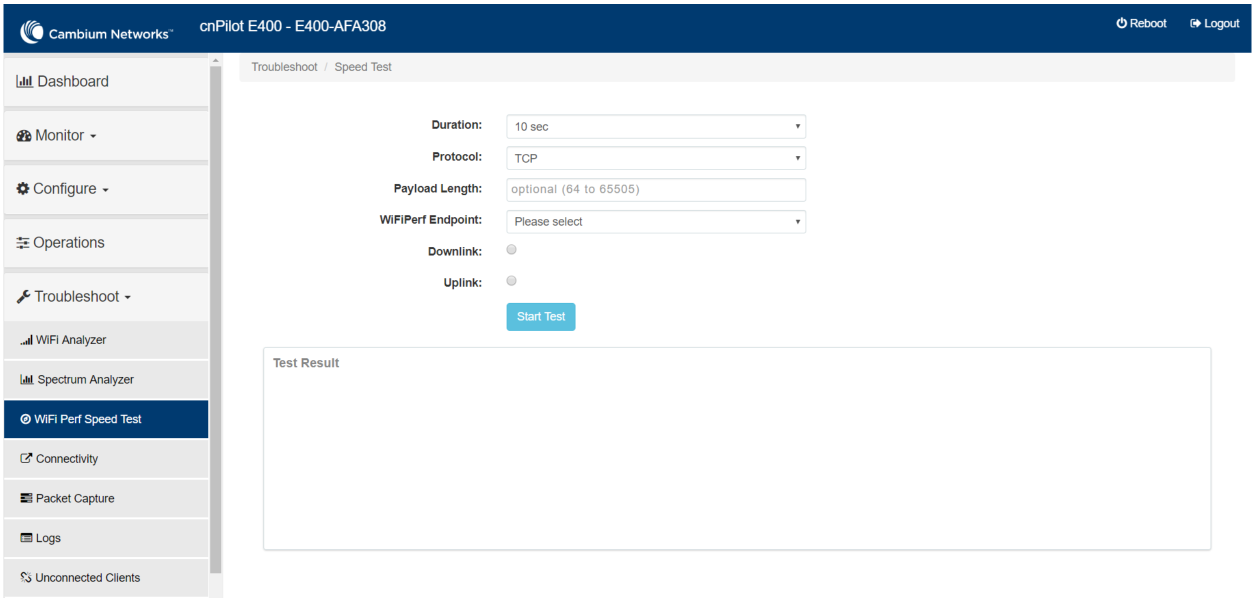
Performance

Wi-Fi Perf speed test

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

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

Figure 41 : *Troubleshoot > Wi-Fi Perf Speed Test*



Duration: 10 sec

Protocol: TCP

Payload Length: optional (64 to 65505)

WiFiPerf Endpoint: Please select

Downlink: ○

Uplink: ○

Start Test

Test Result

Connectivity

This tool helps to check the accessibility of remote hosts from Enterprise Wi-Fi AP device. Three types of tools are supported under this category:

- Ping
- DNS Lookup
- Traceroute

Table 38 :Troubleshoot: Connectivity

Parameters	Description	Range	Default
Ping			
IP Address or Hostname	Provide IPv4/IPv6 address or Hostname to validate the reachability of the destined Host.	-	-
Number of Packets	Provide number of request packets that are required to be transmitted to validate the reachability of destined Host.	1-10	3
Buffer Size	Configure ICMP packet size.	1-65507	56
Ping Result	Displays the ICMP results.	-	-
DNS Lookup			
Host Name	Provide Hostname whose IP must be resolved.	-	-
DNS Test Result	Displays the IP’s that are associated with configured Hostname.	-	-

Parameters	Description	Range	Default
Traceroute			
IP Address or Hostname	Provide IPv4/IPv6 address or Hostname to validate the reachability of the destined Host.	-	-
Fragmentation	Provision to allow or deny fragment packets.	-	Off
Trace Method	Provision to configure payload mechanism to check the reachability of destined IPv4/IPv6/Hostname.	-	ICMP Echo
Display TTL	Provision to customize TTL display.	-	On
Verbose	Provision to display the output of traceroute.	-	On
Traceroute Result	Displays the output of traceroute command.	-	-

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

To configure Ping:

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

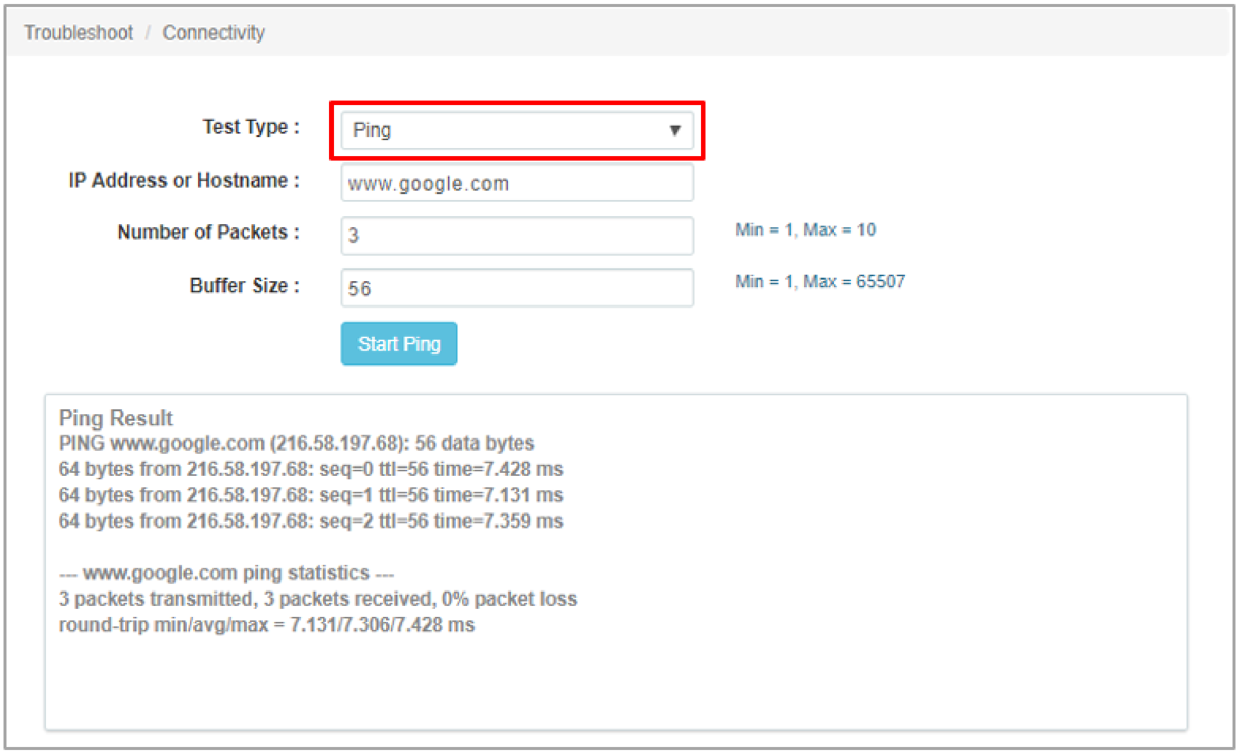
To configure DNS Lookup:

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

To configure Traceroute:

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

Figure 42 : *Troubleshoot > Connectivity > Ping*



Test Type : Ping

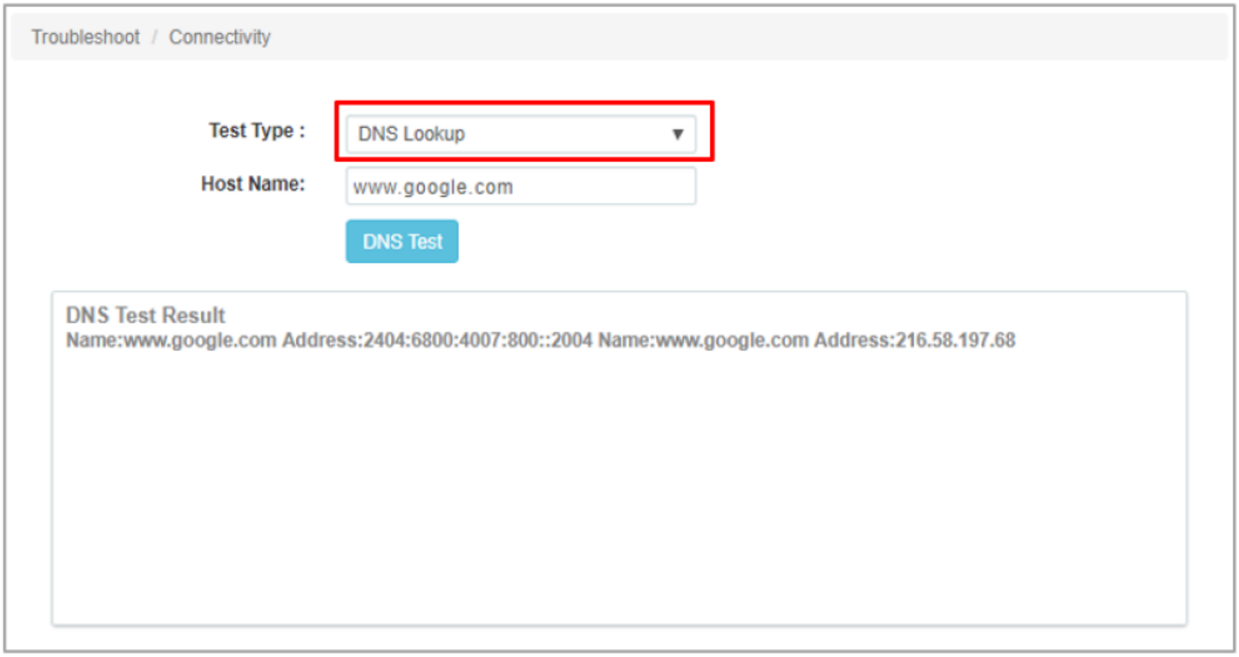
IP Address or Hostname : www.google.com

Number of Packets : 3 Min = 1, Max = 10

Buffer Size : 56 Min = 1, Max = 65507

```
Ping Result
PING www.google.com (216.58.197.68): 56 data bytes
64 bytes from 216.58.197.68: seq=0 ttl=56 time=7.428 ms
64 bytes from 216.58.197.68: seq=1 ttl=56 time=7.131 ms
64 bytes from 216.58.197.68: seq=2 ttl=56 time=7.359 ms

--- www.google.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 7.131/7.306/7.428 ms
```

Figure 43 : *Troubleshoot > Connectivity > DNS Lookup*

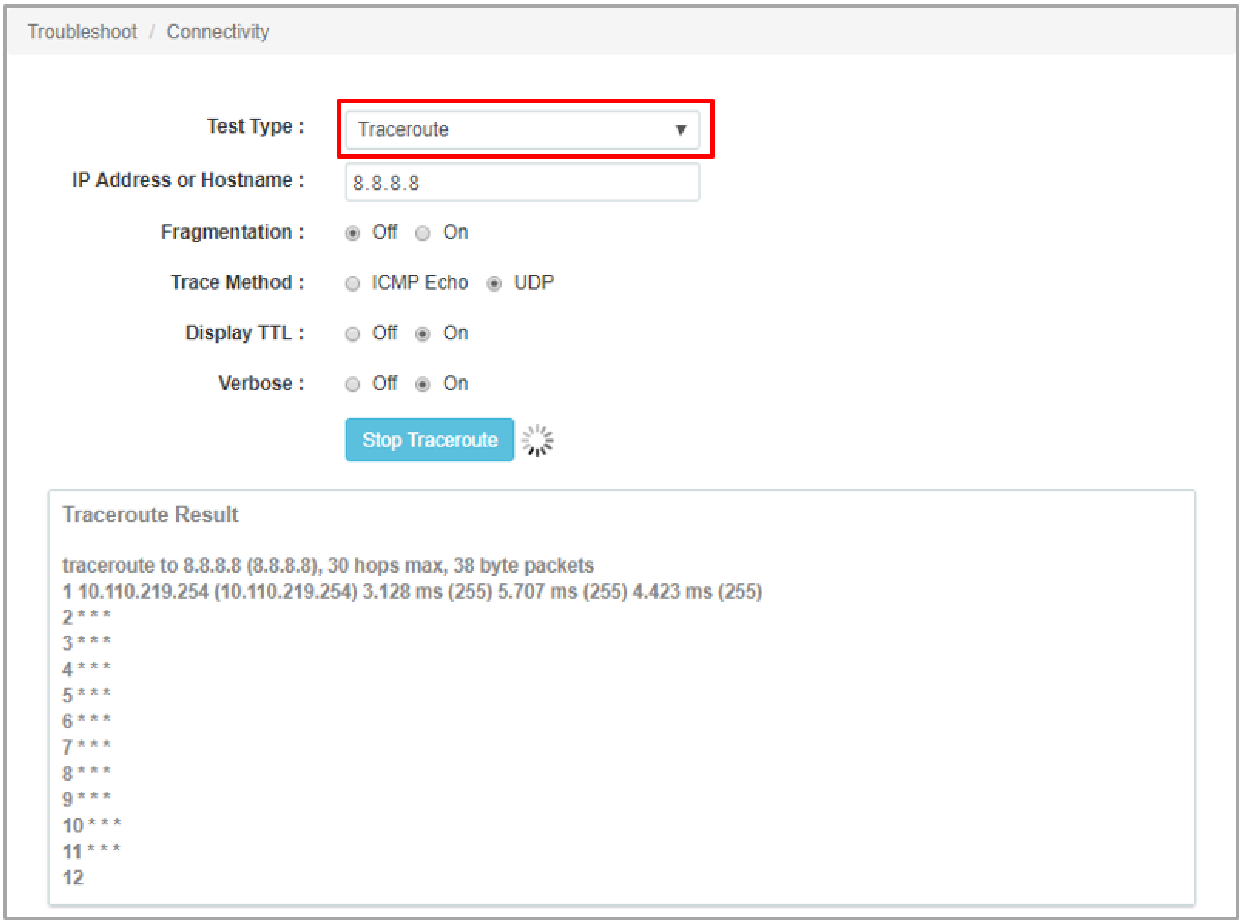


Test Type : DNS Lookup

Host Name: www.google.com

```
DNS Test Result
Name:www.google.com Address:2404:6800:4007:800::2004 Name:www.google.com Address:216.58.197.68
```

Figure 44 : *Troubleshoot: Connectivity > Traceroute*



Test Type : Traceroute ▼

IP Address or Hostname : 8.8.8.8

Fragmentation : ● Off ○ On

Trace Method : ○ ICMP Echo ● UDP

Display TTL : ○ Off ● On

Verbose : ○ Off ● On

Traceroute Result

```
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 38 byte packets
1 10.110.219.254 (10.110.219.254) 3.128 ms (255) 5.707 ms (255) 4.423 ms (255)
2 * * *
3 * * *
4 * * *
5 * * *
6 * * *
7 * * *
8 * * *
9 * * *
10 * * *
11 * * *
12
```

Chapter 13: Management Access

This chapter describes different methods of authenticating users to access device UI. Following are the authentication methods supported by Enterprise Wi-Fi AP devices:

- Local authentication
- SSH-Key authentication
- RADIUS authentication

Local authentication

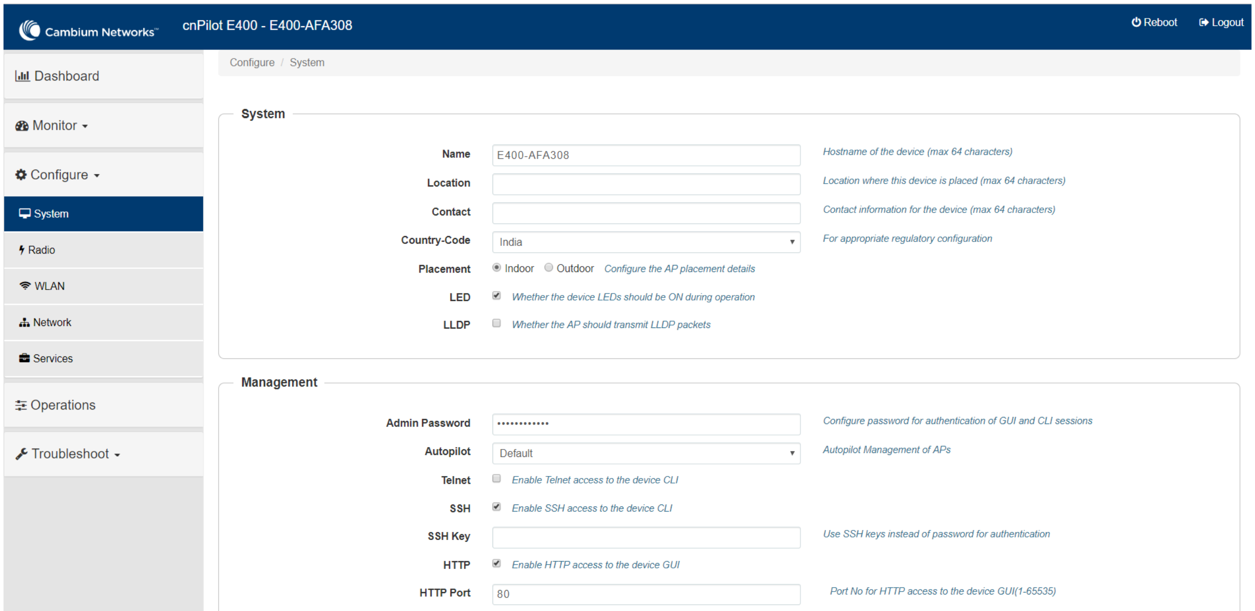
This is the default authentication mode enabled on device. Only one username is supported which is "admin". Default password for "admin" username is "admin". User has provision to configure/update password.

Device configuration

Below figure shows how to configure/update default password of admin user.

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

Figure 45 : *Configure/update default password of admin user*



System

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

Management

Admin Password	••••••••••••	Configure password for authentication of GUI and CLI sessions
Autopilot	Default	Autopilot Management of APs
Telnet	□	Enable Telnet access to the device CLI
SSH	☑	Enable SSH access to the device CLI
SSH Key		Use SSH keys instead of password for authentication
HTTP	☑	Enable HTTP access to the device GUI
HTTP Port	80	Port No for HTTP access to the device GUI(1-65535)

SSH-Key authentication

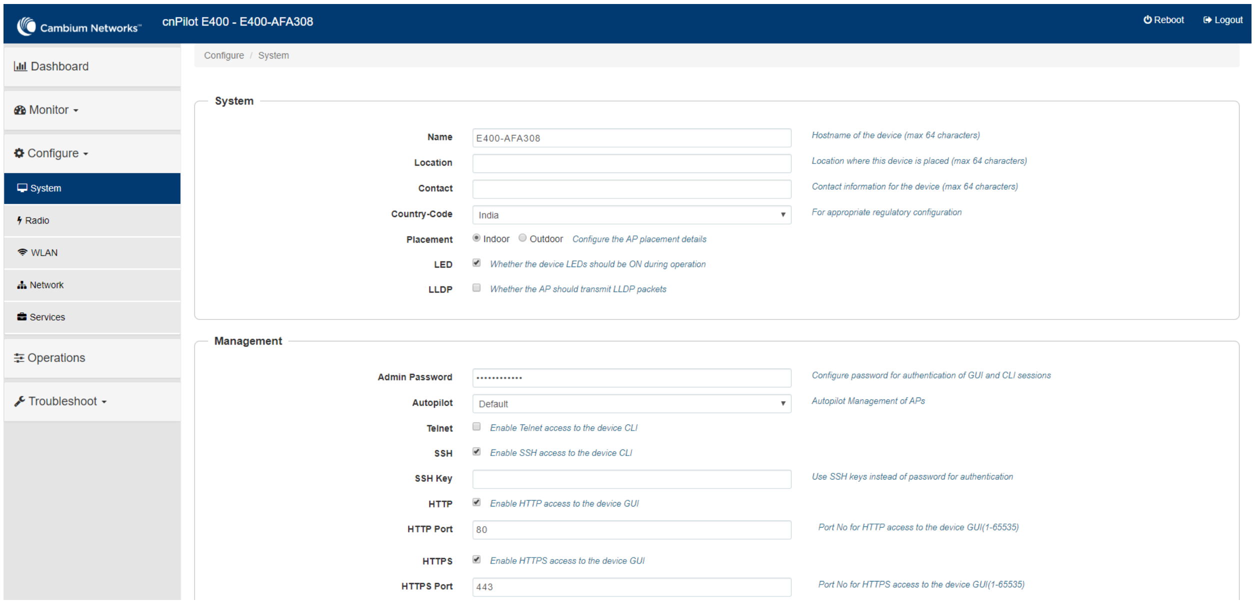
SSH keys are also used to connect remote machines securely. They are based on the SSH cryptographic network protocol, which is responsible for the encryption of the information stream between two machines. Ultimately, using SSH keys user can connect to remote devices without even entering a password and much more securely too. SSH works based on “public-key cryptography”. For simplicity, let us consider that SSH keys come in pairs. There is a private key, that is safely stored to the home machine of the user and a public key, which is stored to any remote machine (AP) the user wants to connect. So, whenever a user initiates an SSH connection with a remote machine, SSH first checks if the user has a private key that matches any of the public keys in the remote machine and if not, it prompts the user for password.

Device configuration

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

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

Figure 46 : *System > Management*



System

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

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

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

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

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

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

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

Management

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

Autopilot: Default — *Autopilot Management of APs*

Telnet: □ *Enable Telnet access to the device CLI*

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

SSH Key: — *Use SSH keys instead of password for authentication*

HTTP: ☑ *Enable HTTP access to the device GUI*

HTTP Port: 80 — *Port No for HTTP access to the device GUI(1-65535)*

HTTPS: ☑ *Enable HTTPS access to the device GUI*

HTTPS Port: 443 — *Port No for HTTPS access to the device GUI(1-65535)*

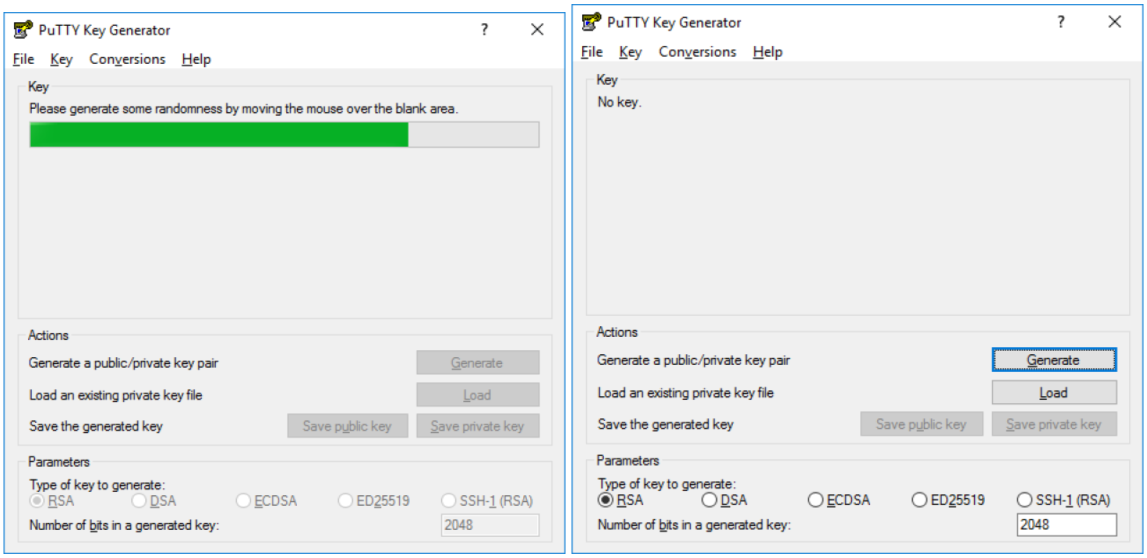
SSH Key Generation

Windows

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

1. Generate a key pair in PUTTY Key Generator (Figure 47) and save private and public key as shown in Figure 48.

Figure 47 : *Generating public/private Key*



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

Number of bits in a generated key: 2048

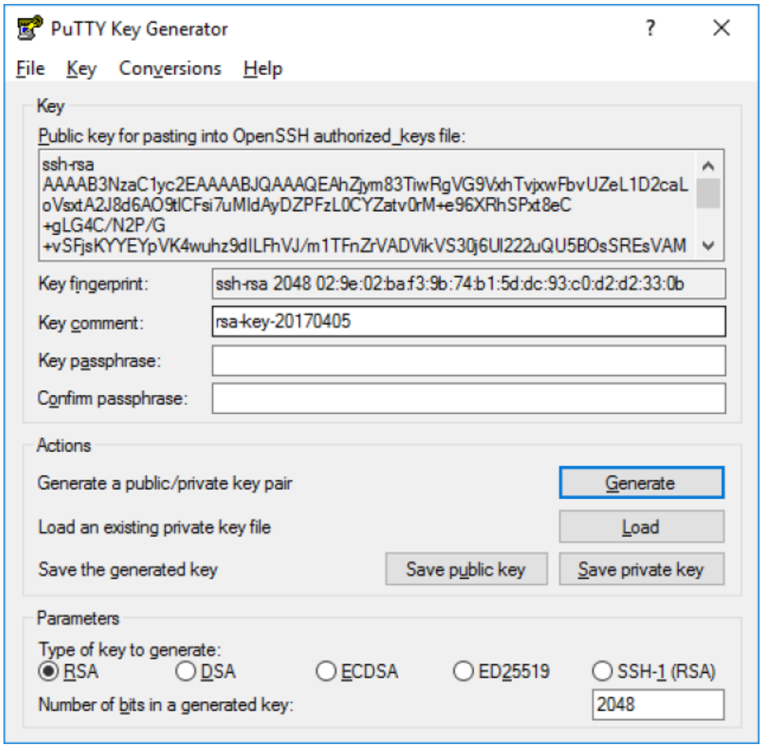
No key.

Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

2. Save the Public key and Private key once key pair is generated as shown in Figure 48.

Figure 48 : *Public and Private Key*



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAhZjym83TiwRgVG9VxhTvjxwFbvUZeL1D2caL
oVsxtA2J8d6AO9tlCFsi7uMIdAyDZPFzL0CYZatv0rM+e96XRhSPxt8eC
+gLG4C/N2P/G
+vSFjsKYYEYpVK4wuhz9dILFhVJ/m1TFnZrVADVikVS30j6UI222uQU5BOsSREsVAM
```

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

Key comment: rsa-key-20170405

Key passphrase:

Confirm passphrase:

Type of key to generate: ● RSA ○ DSA ○ ECDSA ○ ED25519 ○ SSH-1 (RSA)

Number of bits in a generated key: 2048

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

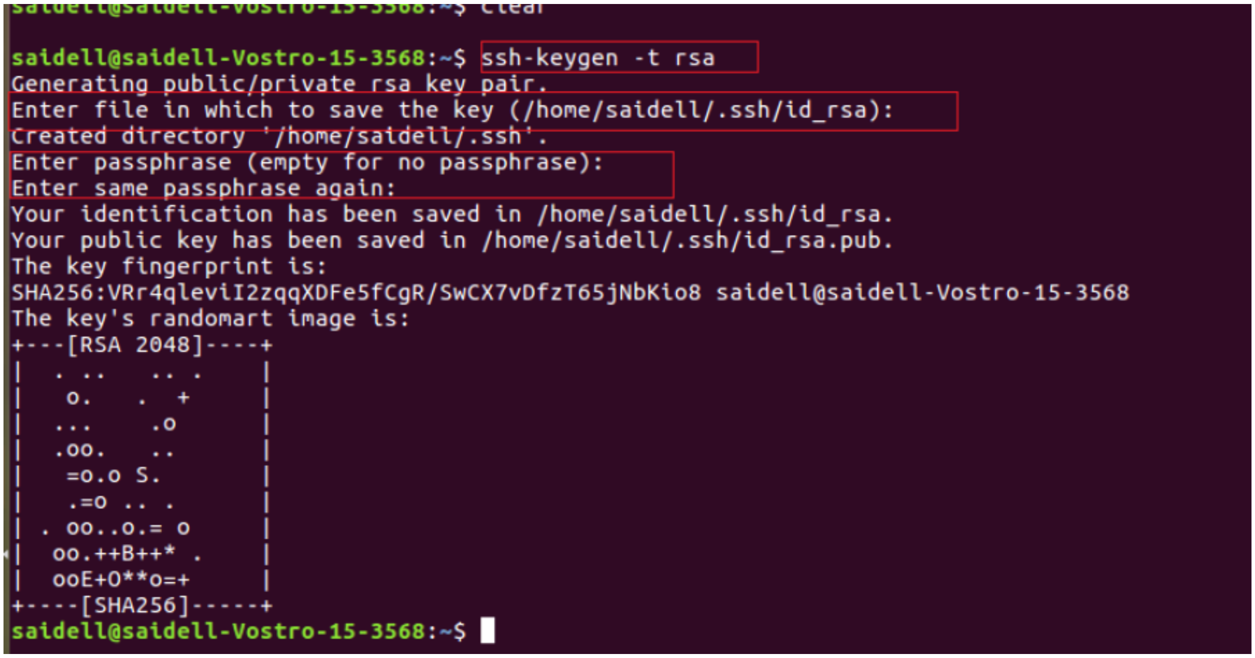
4. Login to device using Private key generated above with username as “admin”.

Linux

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

1. Generate key pair executing below command on Linux console as shown in Figure 49.

Figure 49 : *Public Key location path*



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

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

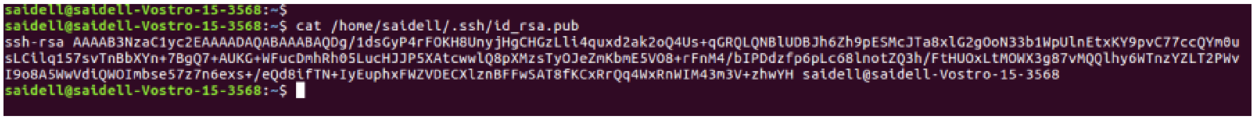
2. The Public key is now located in PATH mentioned in Figure 49.

- PATH = "Enter the file to which to save the key"

3. The private key (identification) is now saved in PATH as mentioned in Figure 50.

- PATH = "Your identification has saved in <>"

Figure 50 : *Private Key saved path*



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

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

5. Login to device using Private key generated above with username as "admin".

RADIUS authentication

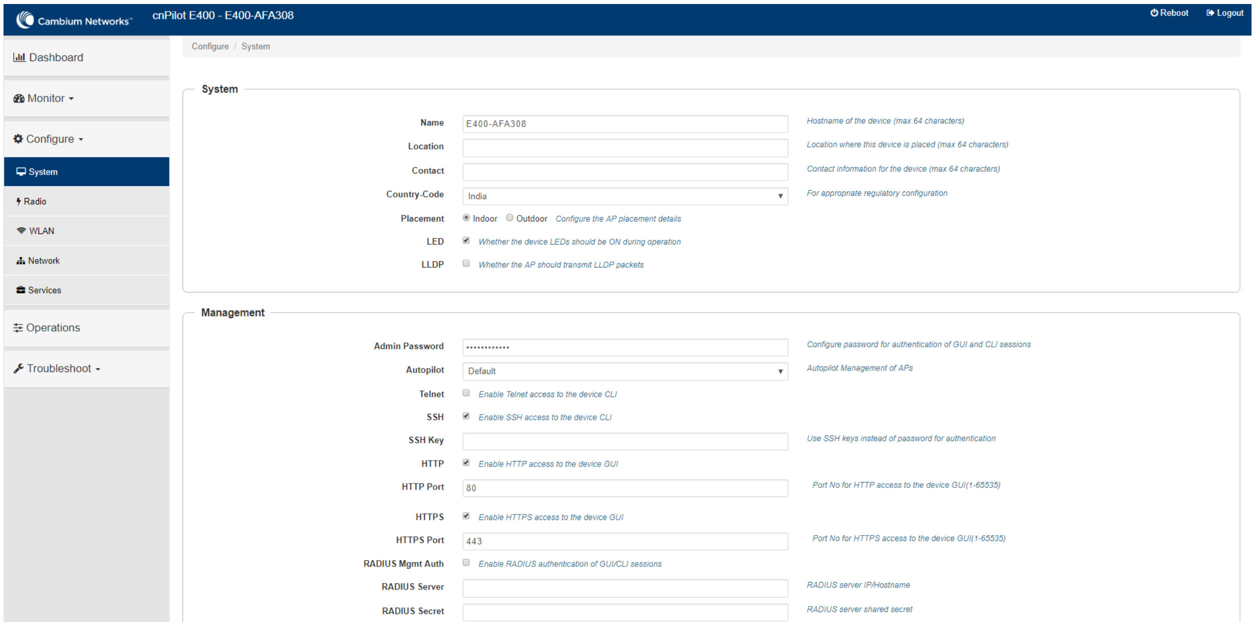
Device management access using RADIUS authentication allows multiple users to access using unique credentials and is secured.

Device configuration

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

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

Figure 51 : *System > Management: RADIUS Server and RADIUS Secret parameters*



System

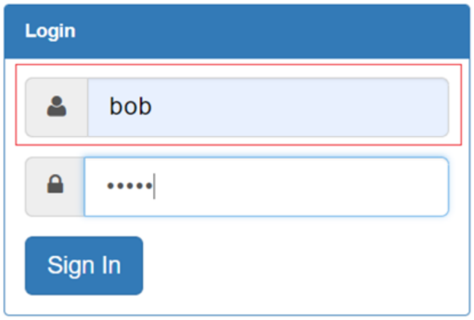
Name	E400-AFA308	Hostname of the device (max 64 characters)
Location		Location where this device is placed (max 64 characters)
Contact		Contact information for the device (max 64 characters)
Country-Code	India	For appropriate regulatory configuration
Placement	● Indoor ○ Outdoor	Configure the AP placement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

Management

Admin Password	············	Configure password for authentication of GUI and CLI sessions
Autopilot	Default	Autopilot Management of APs
Telnet	□	Enable Telnet access to the device CLI
SSH	☑	Enable SSH access to the device CLI
SSH Key		Use SSH keys instead of password for authentication
HTTP	☑	Enable HTTP access to the device GUI
HTTP Port	80	Port No for HTTP access to the device GUI(1-65535)
HTTPS	☑	Enable HTTPS access to the device GUI
HTTPS Port	443	Port No for HTTPS access to the device GUI(1-65535)
RADIUS Mgmt Auth	□	Enable RADIUS authentication of GUI/CLI sessions
RADIUS Server		RADIUS server IP/Hostname
RADIUS Secret		RADIUS server shared secret

4. Login to device using appropriate credentials as shown in below figure.

Figure 52 : *UI Login page*



bob

•••••

Chapter 14: Guest Access Portal- INTERNAL

Introduction

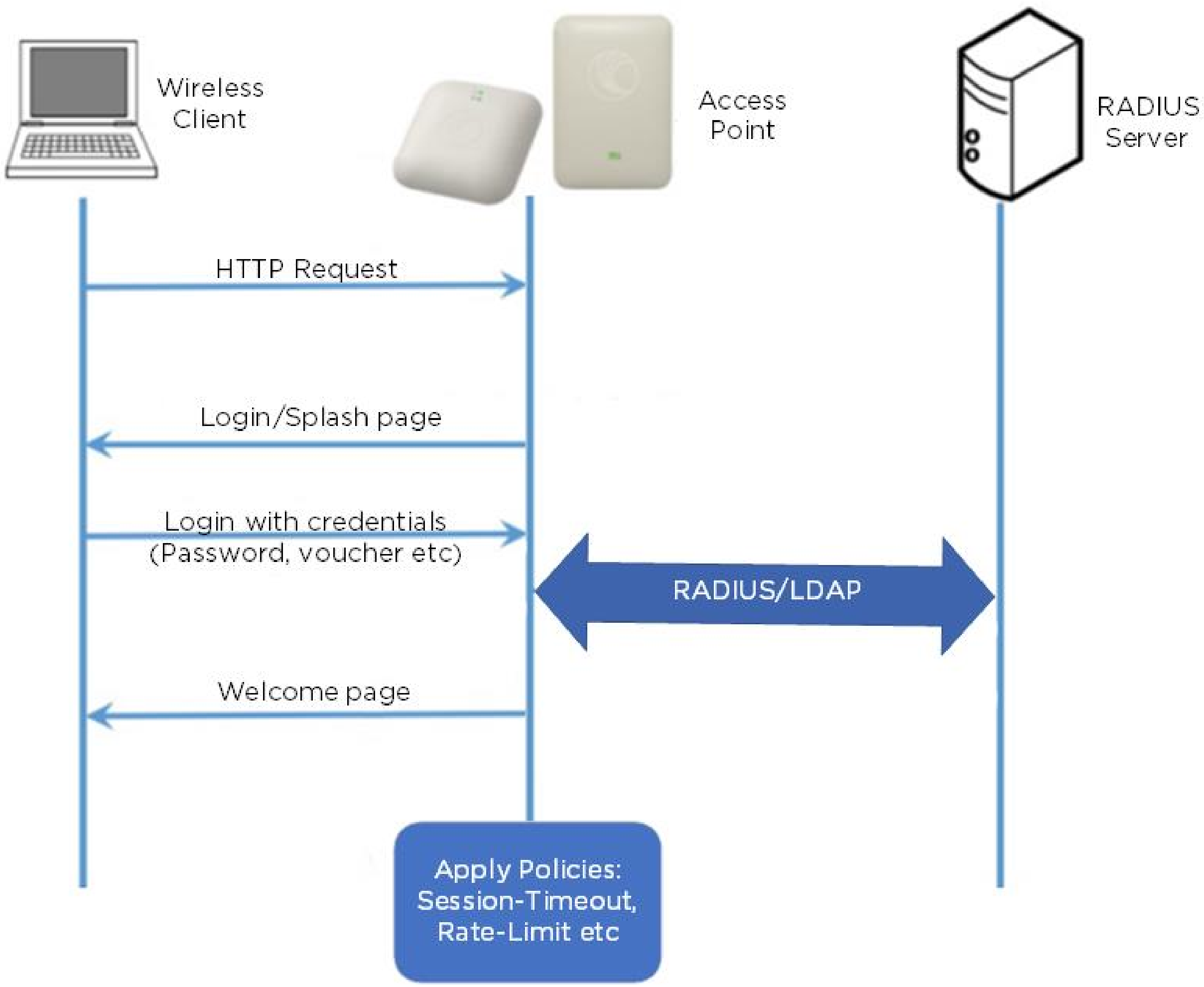
Guest Access Portal services offers a simple way to provide secure access to internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browsers session to a captive portal login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

Modes of Captive Portal Services supported by Enterprise Wi-Fi AP devices:

- **Internal Access**: Captive Portal server is hosted on access point and is local to access point.
- **External Access**: Enterprise Wi-Fi AP is integrated with multiple third-party Captive Portal services vendor. Based on the vendor, device needs to be configured. More details on this Guest Access Portal method is described in Chapter 17.
- **cnMaestro**: Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login and Paid login is supported. More details on this Guest Access Portal method is described in Chapter 18.
- **EasyPass**: EasyPass Access Services enable you to easily provide secure and controlled access to users and visitors on your Wi-Fi network.

Here in this chapter we will brief about Internal Captive Portal services supported by Enterprise Wi-Fi APs. Below figure displays the basic topology of testing Internal Captive Portal Service.

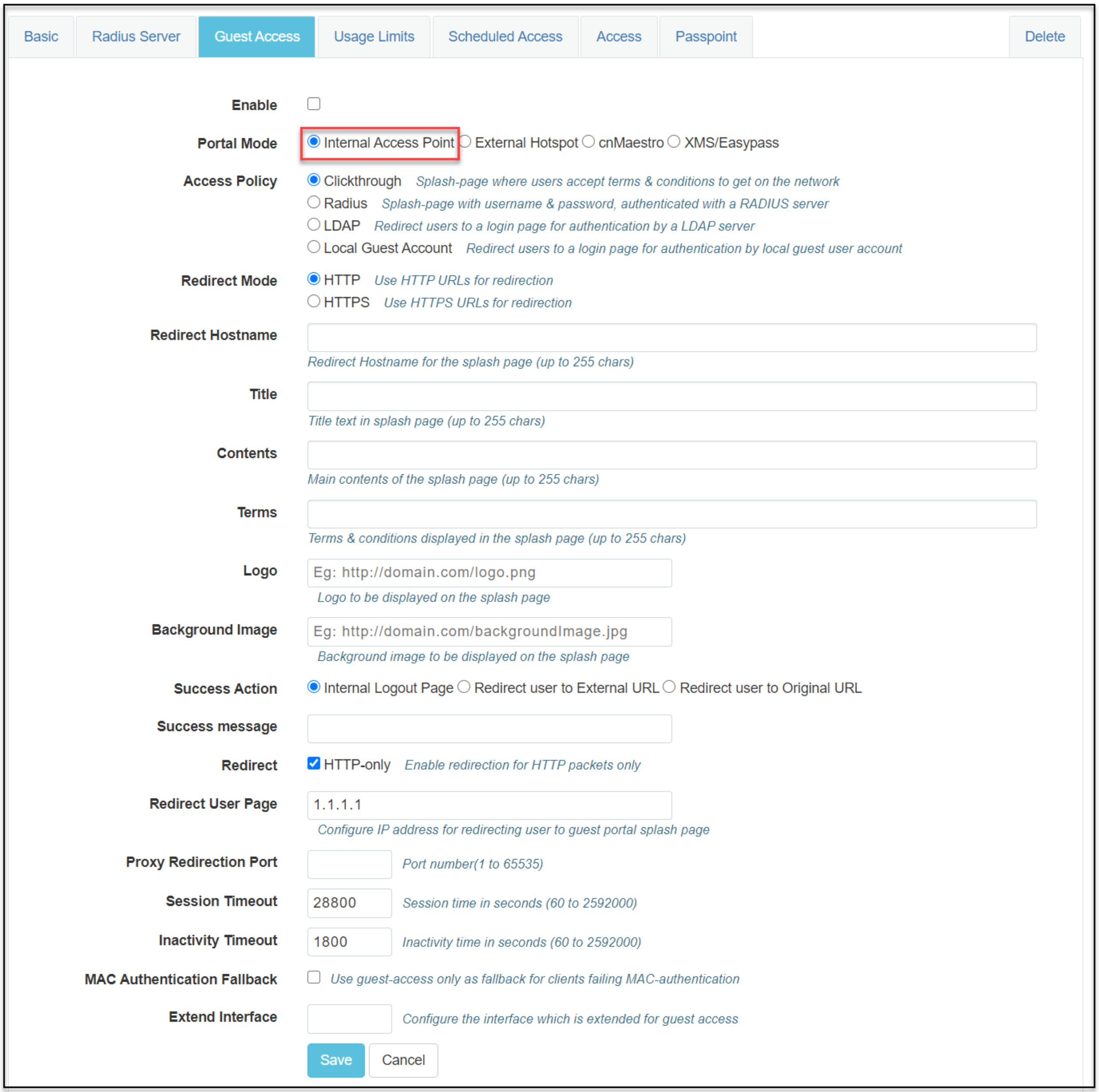
Figure 53 : *Topology*


Wireless Client
Access Point
RADIUS Server
HTTP Request
Login/Splash page
Login with credentials (Password, voucher etc)
RADIUS/LDAP
Welcome page
Apply Policies: Session-Timeout, Rate-Limit etc

Configurable Parameters

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

Figure 54 : *Configure: WLAN > Guest Access > Internal Access Point parameter*



Enable	□
Portal Mode	● Internal Access Point ○ External Hotspot ○ cnMaestro ○ XMS/Easypass
Access Policy	● Clickthrough *Splash-page where users accept terms & conditions to get on the network* ○ Radius *Splash-page with username & password, authenticated with a RADIUS server* ○ LDAP *Redirect users to a login page for authentication by a LDAP server* ○ Local Guest Account *Redirect users to a login page for authentication by local guest user account*
Redirect Mode	● HTTP *Use HTTP URLs for redirection* ○ HTTPS *Use HTTPS URLs for redirection*
Redirect Hostname	*Redirect Hostname for the splash page (up to 255 chars)*
Title	*Title text in splash page (up to 255 chars)*
Contents	*Main contents of the splash page (up to 255 chars)*
Terms	*Terms & conditions displayed in the splash page (up to 255 chars)*
Logo	Eg: http://domain.com/logo.png *Logo to be displayed on the splash page*
Background Image	Eg: http://domain.com/backgroundImage.jpg *Background image to be displayed on the splash page*
Success Action	● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL
Success message	
Redirect	☑ HTTP-only *Enable redirection for HTTP packets only*
Redirect User Page	1.1.1.1 *Configure IP address for redirecting user to guest portal splash page*
Proxy Redirection Port	*Port number(1 to 65535)*
Session Timeout	28800 *Session time in seconds (60 to 2592000)*
Inactivity Timeout	1800 *Inactivity time in seconds (60 to 2592000)*
MAC Authentication Fallback	□ *Use guest-access only as fallback for clients failing MAC-authentication*
Extend Interface	*Configure the interface which is extended for guest access*

Access policy

- Click through

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

Splash page

Title

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

Contents

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

Terms and conditions

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

Logo

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

Background image

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

Redirect Parameters

Redirect hostname

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

Success action

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

- Internal logout Page

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

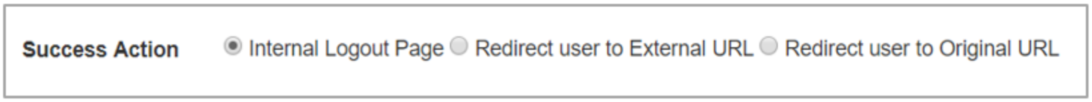
- Redirect users to external URL

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

- Redirect users to Original URL

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

  Figure 55 : *Success action*

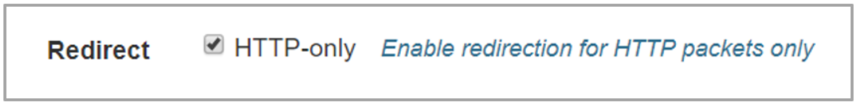


Success Action ● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL

Redirect

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

Figure 56 : *Redirect*



Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

Redirect Mode

There are two redirect modes available:

- **HTTP Mode**

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

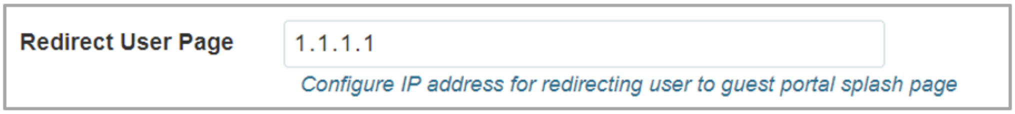
- **HTTP(s) Mode**

  When enabled, AP sends HTTPS POST URL to the client

Redirect user page

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

Figure 57 : *Redirect user page*



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

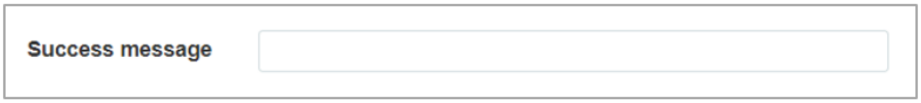
Logout re-direction URLs are as follows:

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

Success Message

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

Figure 58 : *Success Message*



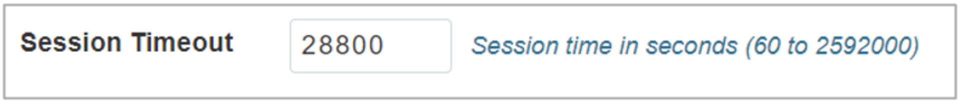
Success message

Timeout

Session

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

Figure 59 : *Configure: WLAN > Guest Access > Session timeout*

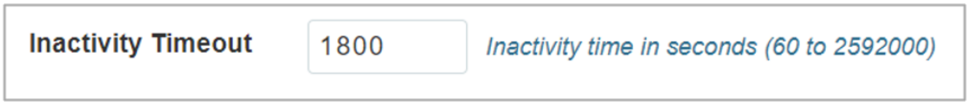


Session Timeout 28800 *Session time in seconds (60 to 2592000)*

Inactivity

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

Figure 60 : *Configure: WLAN > Guest Access > Inactivity timeout*

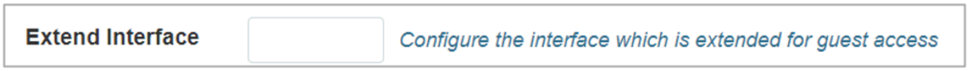


Inactivity Timeout 1800 *Inactivity time in seconds (60 to 2592000)*

Extended interface

Provision to support Guest Access on Ethernet interface.

Figure 61 : *Configure: WLAN > Guest Access > Extended interface*



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

Whitelist

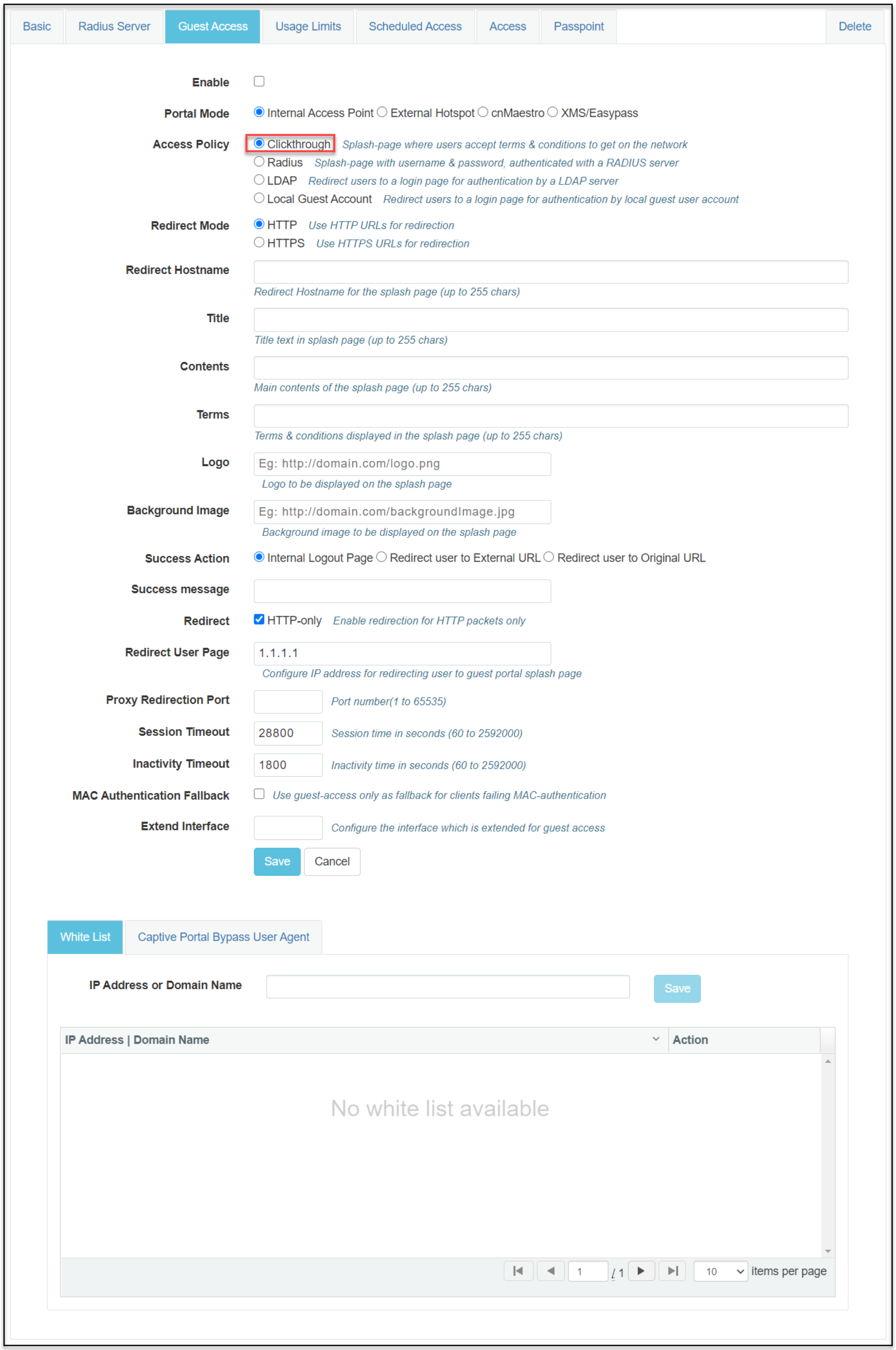
Provision to configure either Ips or URLs to bypass traffic, therefor user can access those Ips or URLs without Guest Access authentication.

Configuration examples

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

Access Policy – Clickthrough

Configuration

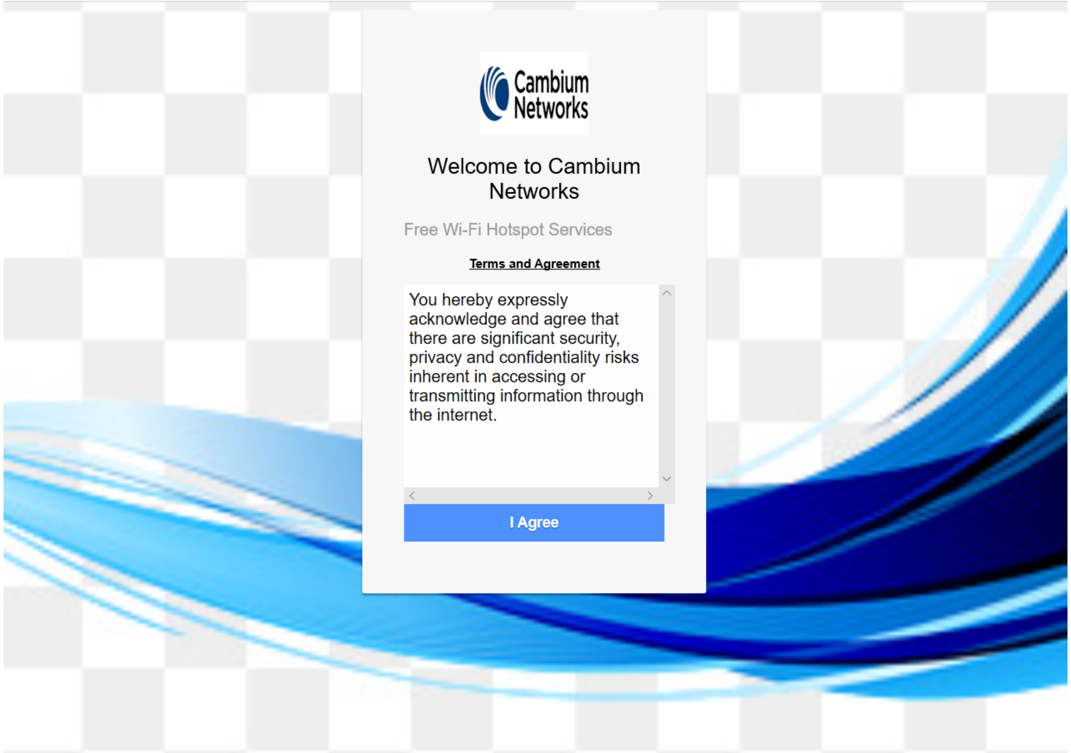


Enable	□
Portal Mode	● Internal Access Point ○ External Hotspot ○ cnMaestro ○ XMS/Easypass
Access Policy	● Clickthrough *Splash-page where users accept terms & conditions to get on the network* ○ Radius *Splash-page with username & password, authenticated with a RADIUS server* ○ LDAP *Redirect users to a login page for authentication by a LDAP server* ○ Local Guest Account *Redirect users to a login page for authentication by local guest user account*
Redirect Mode	● HTTP *Use HTTP URLs for redirection* ○ HTTPS *Use HTTPS URLs for redirection*
Redirect Hostname	*Redirect Hostname for the splash page (up to 255 chars)*
Title	*Title text in splash page (up to 255 chars)*
Contents	*Main contents of the splash page (up to 255 chars)*
Terms	*Terms & conditions displayed in the splash page (up to 255 chars)*
Logo	Eg: http://domain.com/logo.png *Logo to be displayed on the splash page*
Background Image	Eg: http://domain.com/backgroundImage.jpg *Background image to be displayed on the splash page*
Success Action	● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL
Success message	
Redirect	☑ HTTP-only *Enable redirection for HTTP packets only*
Redirect User Page	1.1.1.1 *Configure IP address for redirecting user to guest portal splash page*
Proxy Redirection Port	*Port number(1 to 65535)*
Session Timeout	28800 *Session time in seconds (60 to 2592000)*
Inactivity Timeout	1800 *Inactivity time in seconds (60 to 2592000)*
MAC Authentication Fallback	□ *Use guest-access only as fallback for clients failing MAC-authentication*
Extend Interface	*Configure the interface which is extended for guest access*

IP Address | Domain Name	Action

No white list available

Authentication – Redirected Splash Page



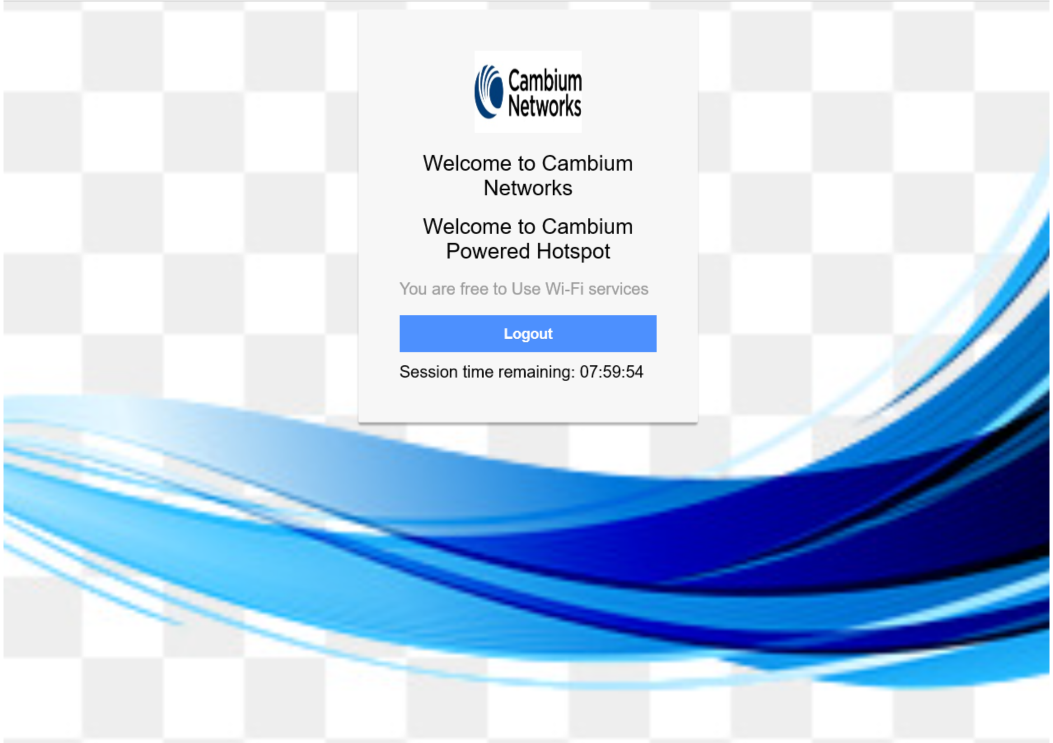
Welcome to Cambium Networks

Free Wi-Fi Hotspot Services

Terms and Agreement

You hereby expressly acknowledge and agree that there are significant security, privacy and confidentiality risks inherent in accessing or transmitting information through the internet.

Successful Login – Redirected Splash Page



Welcome to Cambium Networks

Welcome to Cambium Powered Hotspot

You are free to Use Wi-Fi services

Session time remaining: 07:59:54

Chapter 15: Guest Access Portal-EXTERNAL

Introduction

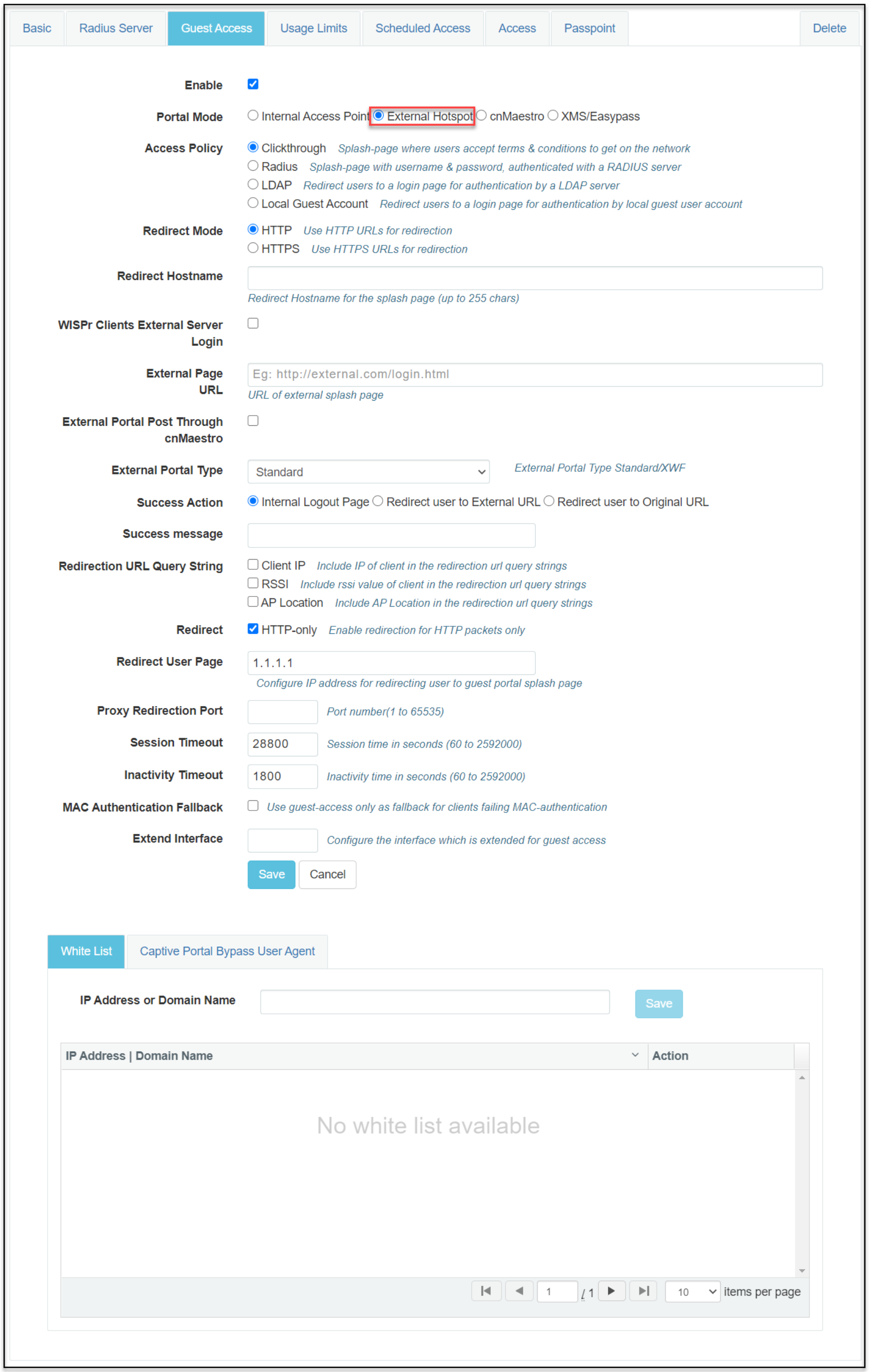
Guest access WLAN is designed specifically for BYOD (Bring your own device) setup, where large organizations have both staff and guests running on same WLAN or similar WLANs. Cambium Networks provides different options to the customers to achieve this based on where the captive portal page is hosted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

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

Configurable Parameters

Figure 62 displays multiple configurable parameters supported for External Guest Access hosted on AP.

Figure 62 : *Configure: WLAN > Guest Access > External Access Point parameter*



Enable ☑

Portal Mode ○ Internal Access Point ● External Hotspot ○ cnMaestro ○ XMS/Easypass

Access Policy
● Clickthrough *Splash-page where users accept terms & conditions to get on the network*
○ Radius *Splash-page with username & password, authenticated with a RADIUS server*
○ LDAP *Redirect users to a login page for authentication by a LDAP server*
○ Local Guest Account *Redirect users to a login page for authentication by local guest user account*

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

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

WISPr Clients External Server Login □

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

External Portal Post Through cnMaestro □

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

Success Action ● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL

Success message

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

Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

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

Proxy Redirection Port *Port number(1 to 65535)*

Session Timeout 28800 *Session time in seconds (60 to 2592000)*

Inactivity Timeout 1800 *Inactivity time in seconds (60 to 2592000)*

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

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

Save Cancel

White List | Captive Portal Bypass User Agent

IP Address or Domain Name Save

IP Address | Domain Name	Action

No white list available

1 / 1 10 items per page

Access policy

Click through:

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

WISPr

WISPr Clients External Server Login

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

External Portal Post Through cnMaestro

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

External Portal Type

Two modes of portal types are supported by Enterprise Wi-Fi AP products.

Standard

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

Redirect Parameters

Success action

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

- Internal logout Page

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

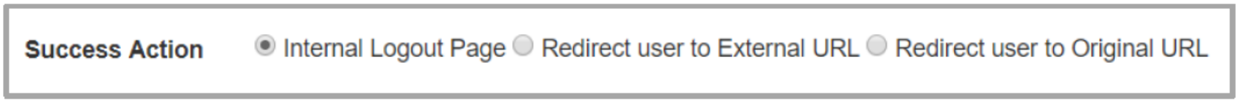
- Redirect users to external URL

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

- Redirect users to Original URL

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

Figure 63 : *Success action*

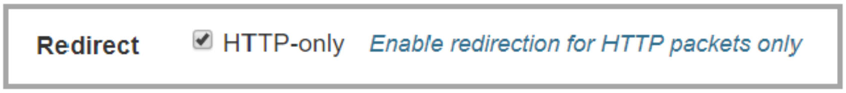


Success Action ● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL

Redirect

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

Figure 64 : *Redirect*



Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

Redirect Mode

There are two redirect modes available:

- HTTP Mode

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

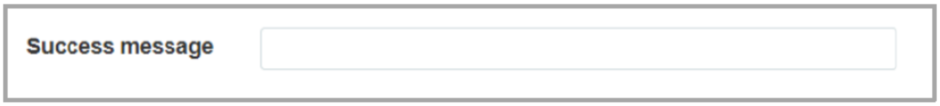
- HTTP(s) Mode

  When enabled, AP sends HTTPS POST URL to the client

Success Message

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

Figure 65 : *Success Message*



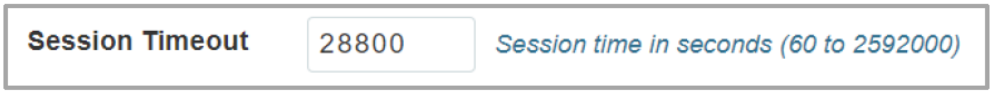
Success message

Timeout

Session

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

Figure 66 : *Configure: WLAN > Guest Access > Session timeout*

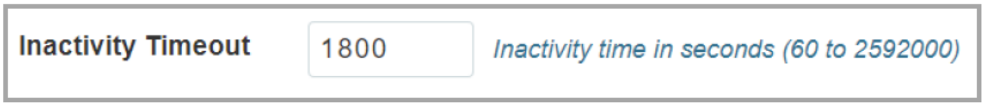


Session Timeout 28800 *Session time in seconds (60 to 2592000)*

Inactivity

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

Figure 67 : *Configure: WLAN > Guest Access > Inactivity timeout*



Inactivity Timeout 1800 *Inactivity time in seconds (60 to 2592000)*

Whitelist

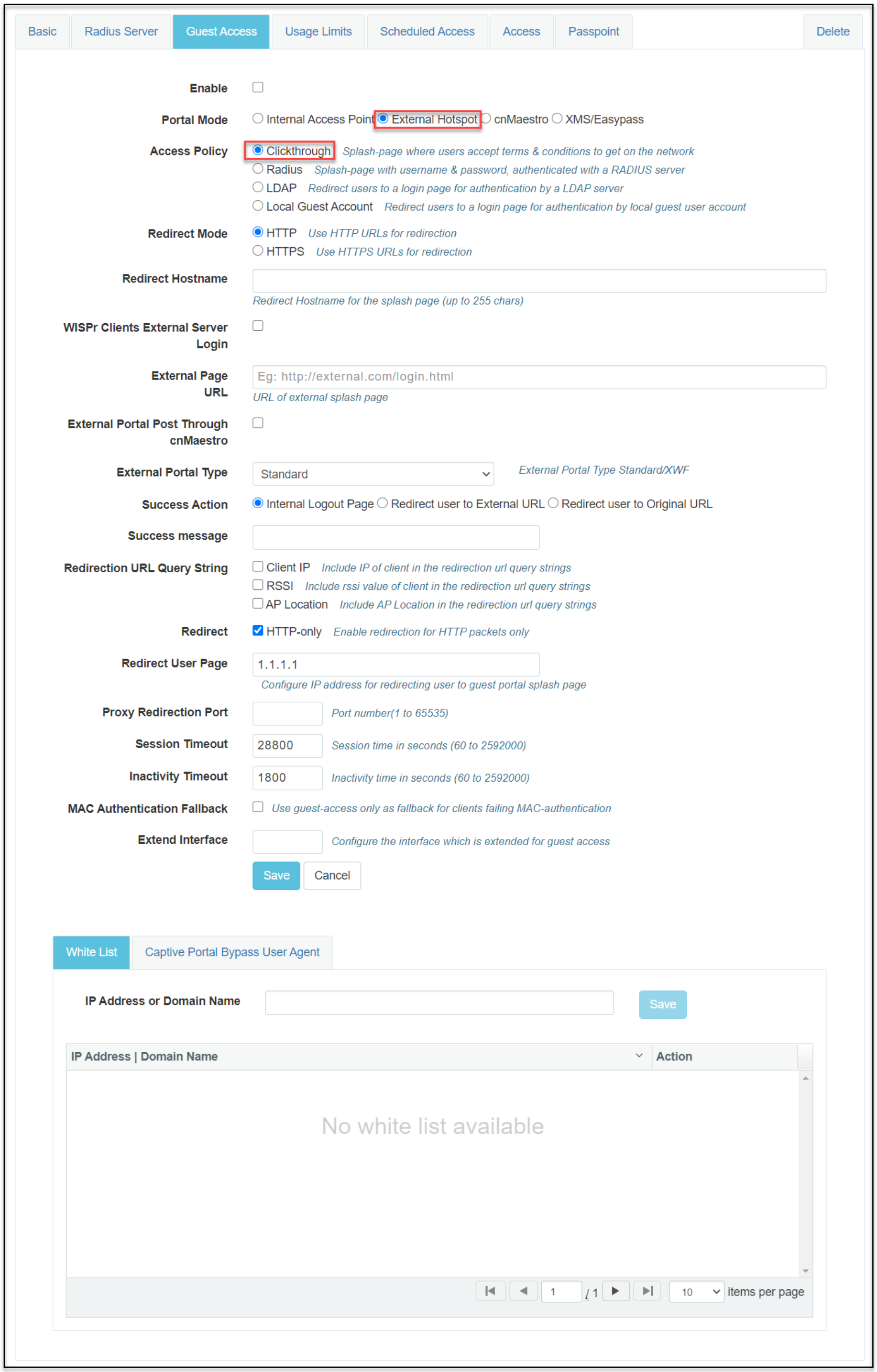
Provision to configure either Ips or URLs to bypass traffic, therefor user can access those Ips or URLs without Guest Access authentication.

Configuration examples

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

Access Policy – Clickthrough

Configuration



Enable □

Portal Mode ○ Internal Access Point ● External Hotspot ○ cnMaestro ○ XMS/Easypass

Access Policy ● Clickthrough *Splash-page where users accept terms & conditions to get on the network*
○ Radius *Splash-page with username & password, authenticated with a RADIUS server*
○ LDAP *Redirect users to a login page for authentication by a LDAP server*
○ Local Guest Account *Redirect users to a login page for authentication by local guest user account*

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

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

WISPr Clients External Server Login □

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

External Portal Post Through cnMaestro □

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

Success Action ● Internal Logout Page ○ Redirect user to External URL ○ Redirect user to Original URL

Success message

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

Redirect ☑ HTTP-only *Enable redirection for HTTP packets only*

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

Proxy Redirection Port *Port number(1 to 65535)*

Session Timeout 28800 *Session time in seconds (60 to 2592000)*

Inactivity Timeout 1800 *Inactivity time in seconds (60 to 2592000)*

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

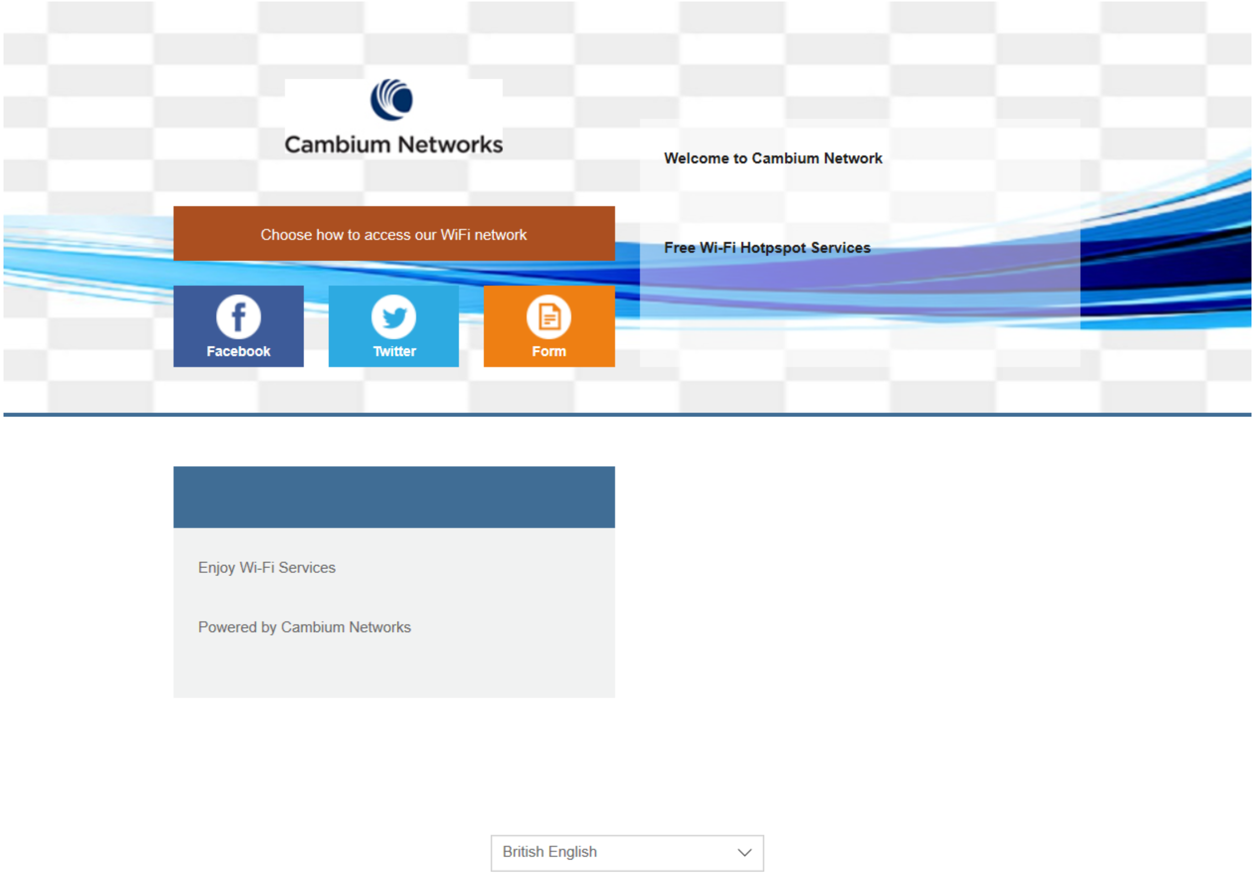
Extend Interface *Configure the interface which is extended for guest access*

IP Address or Domain Name

IP Address | Domain Name	Action

No white list available

Authentication – Redirected Splash Page

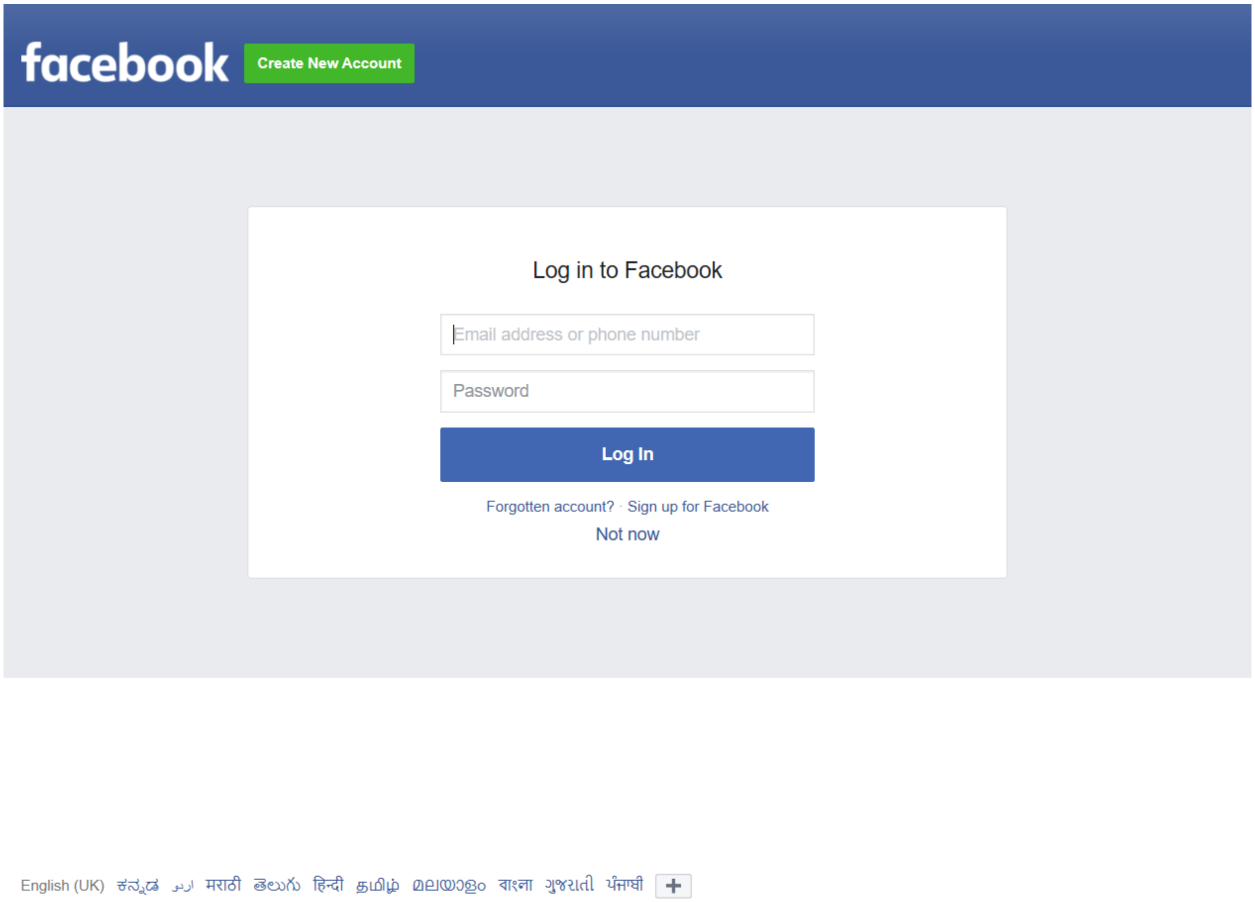


Cambium Networks
Welcome to Cambium Network
Choose how to access our WiFi network
Free Wi-Fi Hotspot Services
Facebook
Twitter
Form
British English

Enjoy Wi-Fi Services

Powered by Cambium Networks

Successful Login – Redirected Splash Page


facebook
Create New Account
Log in to Facebook
Email address or phone number
Password
Log In
Forgotten account? · Sign up for Facebook
Not now
English (UK) ಕನ್ನಡ اردو मराठी తెలుగు हिन्दी தமிழ் മലയാളം বাংলা ગુજરાતી ਪੰਜਾਬੀ +

Chapter 16: Guest Access – cnMaestro

Cambium supports end-to-end Guest Access Portal services with combination of Enterprise Wi-Fi AP and cnMaestro. cnMaestro supports various types of authentication mechanism for wireless clients to obtain Internet access. For further information about Guest Access Portal:

- For On-premises, go to: https://support.cambiumnetworks.com/files/cnmaestro/ and download cnMaestro On-Premises 2.4.0 User Guide.
- For cnMaestro Cloud, go to:

  https://docs.cloud.cambiumnetworks.com/help/2.4.0/index.htm#UG_files/WiFi/Guest%20Access.htm%3FTocPath%3DServices%253A%2520cnPilot%2520Guest%2520Access%2520%7C_____0

Chapter 17: Device Recovery Methods

Factory reset via ‘RESET’ button

Table 39 :Factory reset via RESET button

Access Point	Procedure	LED Indication
XV3-8	Press and hold Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2	Press and hold Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber

Factory reset via power cycle

Table 40 :Factory reset via power cycle

Access Point	Procedure
XV3-8	Not Applicable
XV2-2	Not Applicable

Boot partition change via power cycle

Table 41 :Boot partition change via power cycle

Access Point	Procedure
XV3-8	Follow power ON and off for 9 times with interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2	Follow power ON and off for 9 times with interval of 120 Sec (ON) and 5 Sec (OFF)

Glossary

Term	Definition
AP	Access Point Module. One module that distributes network or Internet services to subscriber modules.
API	Application Program Interface
ARP	Address Resolution Protocol. A protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host.
BHM	Backhaul Timing Master (BHM)- a module that is used in a point to point link. This module controls the air protocol and configurations for the link.
BHS	Backhaul Timing Slave (BHS)- a module that is used in a point to point link. This module accepts configuration and timing from the master module.
BT	Bluetooth
DFS	See Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus, DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
FCC	Federal Communications Commission of the U.S.A.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
UI	User interface.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure
HT	High Throughput
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
LUID	Logical Unit ID. The final octet of the 4-octet IP address of the module.
LLDP	Link Layer Discovery Protocol
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.

Term	Definition
Maximum Information Rate (MIR)	The cap applied to the bandwidth of an SM or specified group of SMs. In the Cambium implementation, this is controlled by the Sustained Uplink Data Rate, Uplink Burst Allocation, Sustained Downlink Data Rate, and Downlink Burst Allocation parameters.
MIB	Management Information Base. Space that allows a program (agent) in the network to relay information to a network monitor about the status of defined variables (objects).
MIR	See Maximum Information Rate.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer, which has an IP address that is not unique or not registered.
SLA	Service Level Agreement
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	Virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes is possible. SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.
VHT	Very High Throughput