Cambium Networks™

USER GUIDE

Enterprise Wi-Fi Access Point

Release 6.6.0.2

Reservation of Rights

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

This product is not restricted 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

About This User Guide

This section describes the following topics:

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 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 of related documents for Enterprise Wi-Fi AP.

Table 1: Related documents

Document Name	Location
Enterprise Wi-Fi AP product details	https://www.cambiumnetworks.com/products/wifi/
Enterprise Wi-Fi 6 AP Hardware and Installation Guide	https://support.cambiumnetworks.com/files
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/

Document Name	Location
Support	https://www.cambiumnetworks.com/support/contact-support/
Warranty	https://www.cambiumnetworks.com/support/warranty/
Feedback	For feedback, e-mail to support@cambiumnetworks.com/

Existing hardware platforms

Table 2 lists the existing hardware platforms in Enterprise Wi-Fi Access Points:

Warning

Release 6.x is no longer supported on Wi-Fi 5 APs. It was provided for the Wi-Fi 5 APs as a BETA release only. Any issues on these APs running release 6.x will not be supported by the Cambium Support team.

Table 2: Existing hardware platforms

Hardware Platform	Description
XE3-4	4x4:4; 2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Tri-Radio Indoor Wi-Fi 6e Access Point with BLE IoT radio
XE3-4TN	4x4:4, 2x2:2, 2x2:2 802.11b/g/n/ac wave 2/ax Tri-Radio Outdoor Wi-Fi 6e Access point with BLE IoT radio
XE5-8	8x8:8, 4x4:4, 4x4:4, 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Band AP with multi-radio SDR with BLE IoT radio
XV2-2	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Access Point
XV2-2T0	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Access Point, Omni antenna, PoE out with BLE IoT radio
XV2-2T1	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Access Point, Sector antenna, PoE out with BLE IoT radio
XV2-21X	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Wi-Fi 6 Access Point
XV2-22H	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Wi-Fi 6 Wall-Plate Access Point with BLE/Zigbee IoT radio
XV2-23T	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Wi-Fi 6 Access Point
XV3-8	8x8:8, 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Radio Indoor Access Point with BLE IoT radio

Premium feature list

Release 6.0 and later releases of Enterprise Wi-Fi AP firmware support certain advanced features that are available only through a paid subscription to cnMaestro X or XMS-Cloud management. These features are identified with the label **Premium feature** in the documentation. With Release 6.5 and later releases, end users can access these features without a management subscription on a free trial basis and for a limited

time. As Cambium Networks releases new versions, restrictions will be enforced on the use of these premium features only in conjunction with a current cnMaestro X or XMS-Cloud subscription. If the user does not have a current subscription at that time, the APs will stop enabling configurations, including these premium features.

Table 3: Premium feature list

Feature Name	Release Details
Wireless Intrusion Detection Systems (WIDS)	Release 6.4.2
RADIUS-based ePSK	Release 6.4
ePSK scale (more than 300 keys)	Release 6.3
Stanley AeroScout Location Engine	Release 6.3
User Groups	Release 6.2
Advanced Filters (QoS, DSCP, Schedule, and Rate limit)	Release 6.0
Application Control	Release 6.0

Chapter 1: Quick Start – Device Access

This chapter describes the following topics:

Powering up the device

This section includes the following topics:

Enterprise Wi-Fi AP product family can be powered using an Ethernet PoE Switch or a PoE midspan injector. Note that some APs can be powered by 802.3af, while others may require 802.3at or 802.3bt. Additionally, some APs can be powered with an external power supply. Refer to the related product datasheet to determine the options available.

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

Enterprise Wi-Fi APs negotiate the power via the LLDP mechanism. Figure 1 represents the Enterprise Wi-Fi AP Eth1 port connecting to a switch (PoE PSE Port).

Figure 1: *Installation of Enterprise Wi-Fi AP to PSE port*

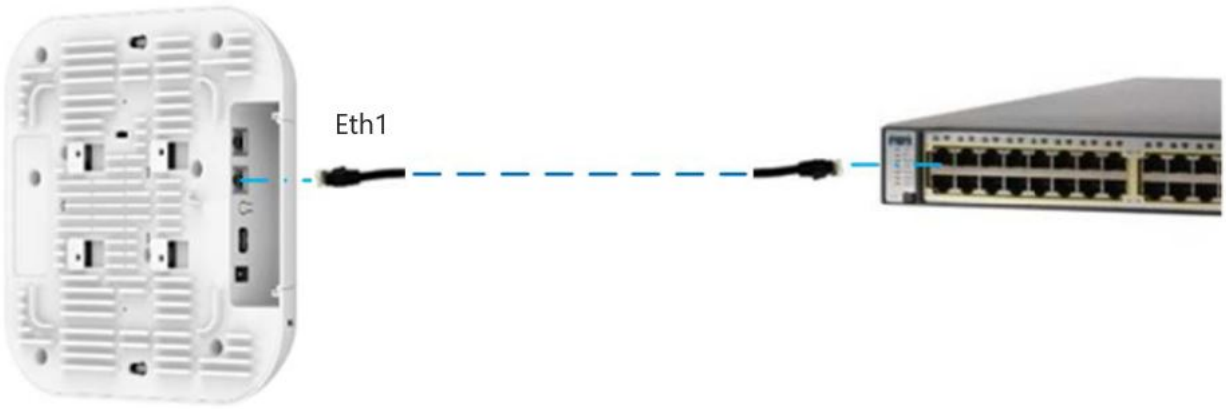


Table 4 provides detailed information on the AP modules that are enabled based on power negotiated via LLDP.

Table 4: Power management policy

Platform	IEEE 802.3af (12.95W @ PD)	IEEE 802.3at (25.5W @ PD)	IEEE 802.3bt Class - 0/1/2/3/4 (40W @ PD)	IEEE 802.3b Class - 5/6 (51W @ PD)	IEEE 802.3b Class - 7/8 (64W @ PD)
XV3-8	✓	✓	✓		
XV2-2	✓	✓			
XV2-2T0	✓	✓	✓	✓	
XV2-2T1	✓	✓	✓	✓	
XE5-8		✓	✓	✓	✓
XE3-4	✓	✓	✓		
XV2-21X	✓	✓			
XV2-23T	✓	✓			
XV2-22H	✓	✓			
XE3-4TN	✓	✓	✓	✓	✓

PoE adapter

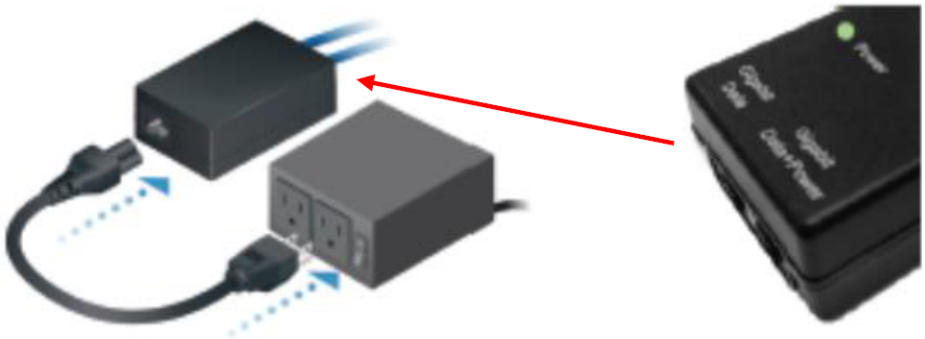
To power up the device using a PoE adapter, perform the following steps:

1. Connect the Ethernet cable from the Eth1/PoE-IN port of the device to the 5 Gigabit Data + Power port of the PoE adapter.
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 a PoE adapter*

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

Figure 3: *Connecting PoE adapter to a power outlet*



DC power supply

The Enterprise Wi-Fi AP XV3-8 has an option to power via a DC power adapter through the barrel connector. If the device is connected to both the DC power adapter and the PoE adapter, then the DC power adapter takes precedence.

Accessing the device

This section includes the following topics:

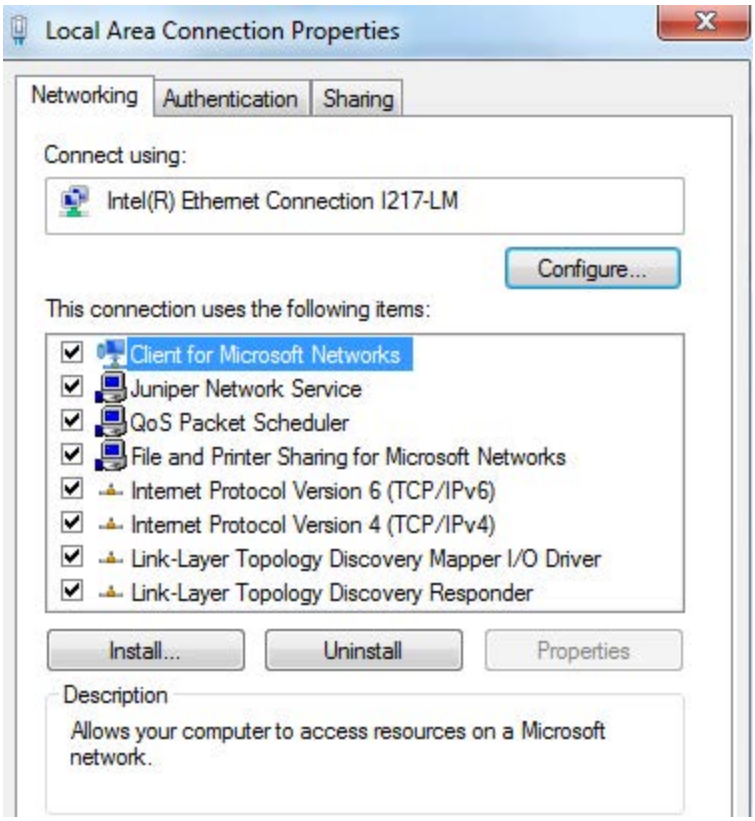
- Device access using default/fallback IP
- Device access using zeroconf IP
- Device access using DHCP IP address

Once the device is powered up ensure the device is up and running before you try to access it based on LED status. The 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 or fallback IP

To configure the computer to access the device using the default or fallback IP, perform the following steps:

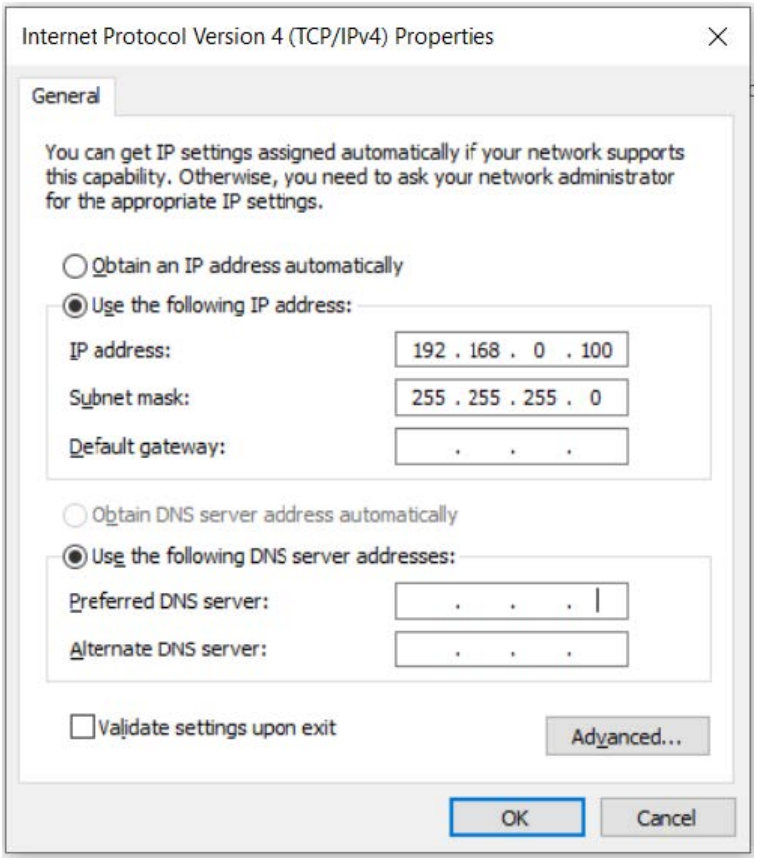
1. Open **Local Area Connection Properties** by performing one of the following steps:
    - In computers running the Windows 7 operating system, go to **Control Panel > Network and Internet > Network Connections > Local Area Connection > Properties** (in the **Local Area Connection Status** window).
    - In computers running the Windows 10 operating system, go to **Control Panel > Network and Internet > Network and Sharing Center > Local Area Connection > Properties** (in the **Local Area Connection Status** window).



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

2. Select **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.

    The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box appears, as shown below.:

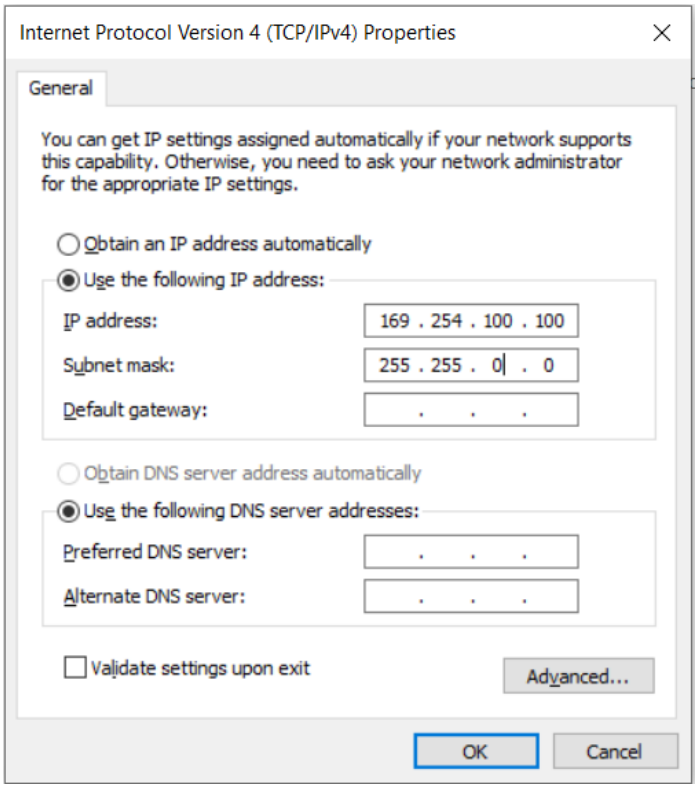


3. In the **Use the following IP address** section, ensure that an appropriate IP address and a subnet address are provided.
4. Click OK.
5. Ensure that your computer is set up to communicate with the required range of IP addresses.
6. Open a web browser and type the URL - http://192.168.0.1 - to access the device UI. The Sign In page appears.
7. Type an appropriate username and password.
    - Default username: admin
    - Default password: admin
8. Click **Sign In**.

Device access using zeroconf IP

To configure the computer to access the device using the zeroconf IP, complete the following steps:

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. Zeroconf IP of the device with ESN 58:C1:CC:DD:AA:BB is 169.254.170.187.
2. Configure Management PC with 169.254.100.100/16, as described below:



3. 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

To access the device using DHCP IP address, follow the below steps:

1. Plugin the device to the network.
2. Obtain the IP address of the device from the system administrator.
3. Access the device UI using http://<IP address> and default credentials, as listed below:
    - Username: admin
    - Password: admin

LED status

The Enterprise Wi-Fi AP has a single-color LED. The power LED glows amber as the AP boots up and turns Green once it has booted up successfully. The network or status LED glows green if the connection to XMS or cnMaestro controller or manager is down and turns blue once the AP is connected successfully to XMS or cnMaestro.

Table 5: Enterprise Wi-Fi AP LED status

LED Color	Status Indication
	The device is booting up.  **Note:** If these LEDs remain amber for more than five minutes, this indicates that the device has failed to boot.
	• The device is successfully up and accessible. • Wi-Fi services are up, if configured.
	XMS or cnMaestro connection is successful.

Chapter 2: Onboarding the Device

This chapter describes the following topics:

Overview

By default, support is available for all the devices at 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 the devices to connect to the cnMaestro server using DHCP options or static URL configuration. For more information, refer to the *cnMaestro On-Premises User Guide.*

Device onboarding and provisioning

Enterprise Wi-Fi APs support the following onboarding methods:

cnMaestro

cnMaestro is a simple next-generation network management system for Cambium Networks wireless and wired solutions.

For onboarding devices to cnMaestro, refer to the *cnMaestro User Guide*.

Supported devices and minimum version

The following table lists the minimum release version of every Enterprise Wi-Fi APs that is required to be managed by cnMaestro Cloud and On-Premises. It also lists the minimum version of cnMaestro On-Premises required to manage the respective APs.

Note

The AP version is the minimum version required to manage them using cnMaestro Cloud and On-Premises.

Similarly, the cnMaestro On-Premises version is the minimum version required to manage the APs.

Table 6: Supported minimum AP and cnMaestro versions

AP Model	Supported Minimum AP Version		Supported Minimum cnMaestro On-Premises Version
	For cnMaestro Cloud	For cnMaestro On-Premises	
XE3-4	6.4	6.4	3.1.0

AP Model	Supported Minimum AP Version		Supported Minimum cnMaestro On-Premises Version
	For cnMaestro Cloud	For cnMaestro On-Premises	
XE3-4TN	6.5.1	6.5.1	3.2.0
XE5-8	6.4.1	6.4.1	3.1.1
XV2-2	6.1	6.1	2.4.1
XV2-2T0	6.4	6.4	3.1.0
XV2-2T1	6.4.1	6.4.1	3.1.1
XV2-21X	6.5	6.5	3.1.1
XV2-22H	6.5	6.5	3.1.1
XV2-23T	6.5	6.5	3.1.1
XV3-8	6.0	6.0	2.4.1

XMS-Cloud

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

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

Chapter 3: Using the UI

You can manage Enterprise Wi-Fi AP devices using the on-device user interface (UI), which is accessible from any network device. This chapter explains how to access the UI.

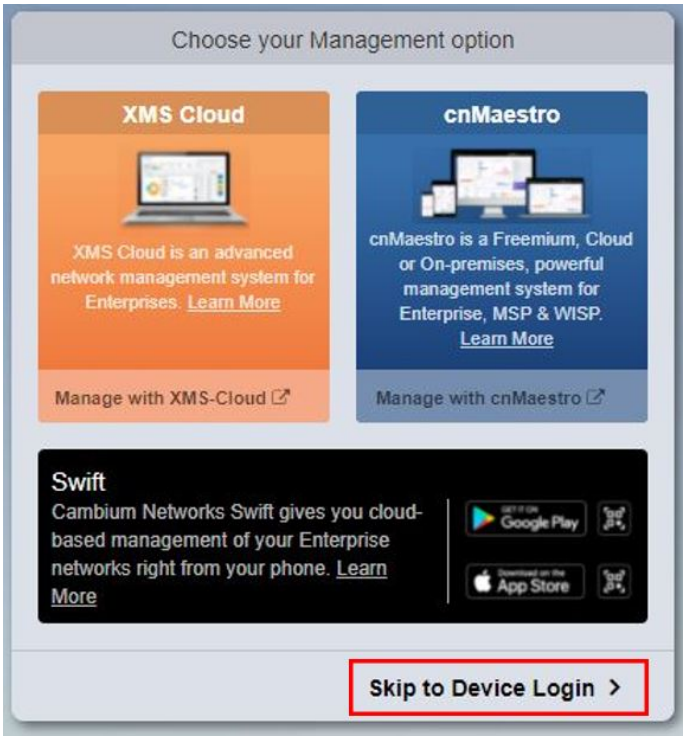
This chapter describes the following topics:

Logging into the UI

You can manage the devices using either of the management options (Figure 4) or directly using the device login (Chapter 3).

- To manage the device, select one of the following management options, as shown in Figure 4:
  - **XMS-Cloud**
  - **cnMaestro**

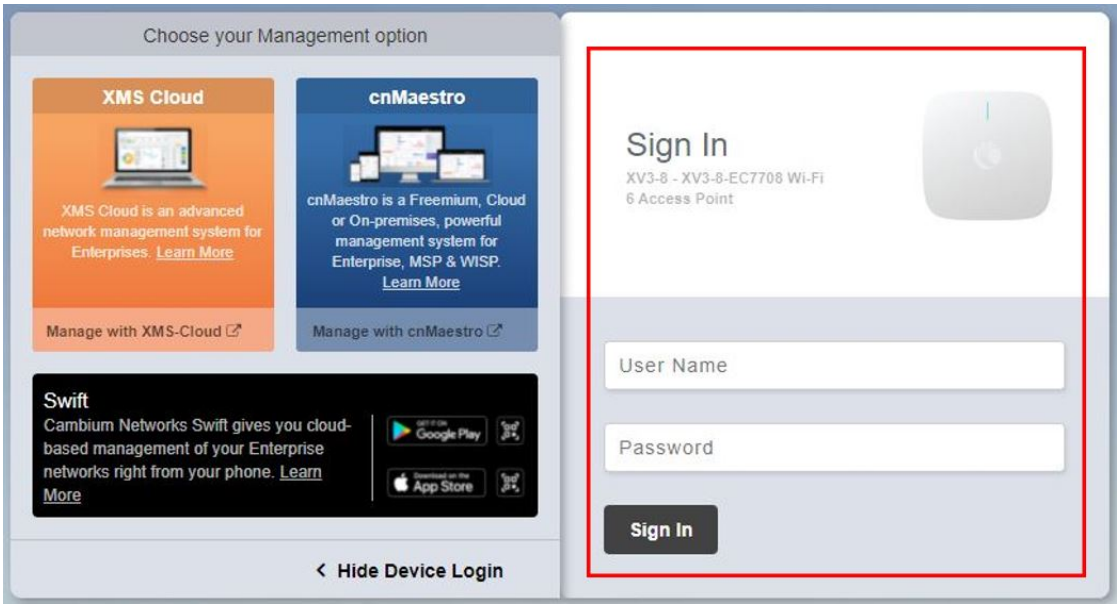
  Figure 4: *The Management option page*



- To login to the device login page, click **Skip to Device Login.**

  The **Sign In** tab appears, as shown in Chapter 3.

Figure 5: *The device login page*



Enter the following credentials:

- User Name: admin
- Password: admin

Viewing the home page (dashboard)

On logging into the Enterprise Wi-Fi AP login page, the home page (dashboard) is displayed. Figure 6 shows the elements that are displayed on the Enterprise Wi-Fi AP home page.

Figure 6: *The Enterprise Wi-Fi AP home page (dashboard)*

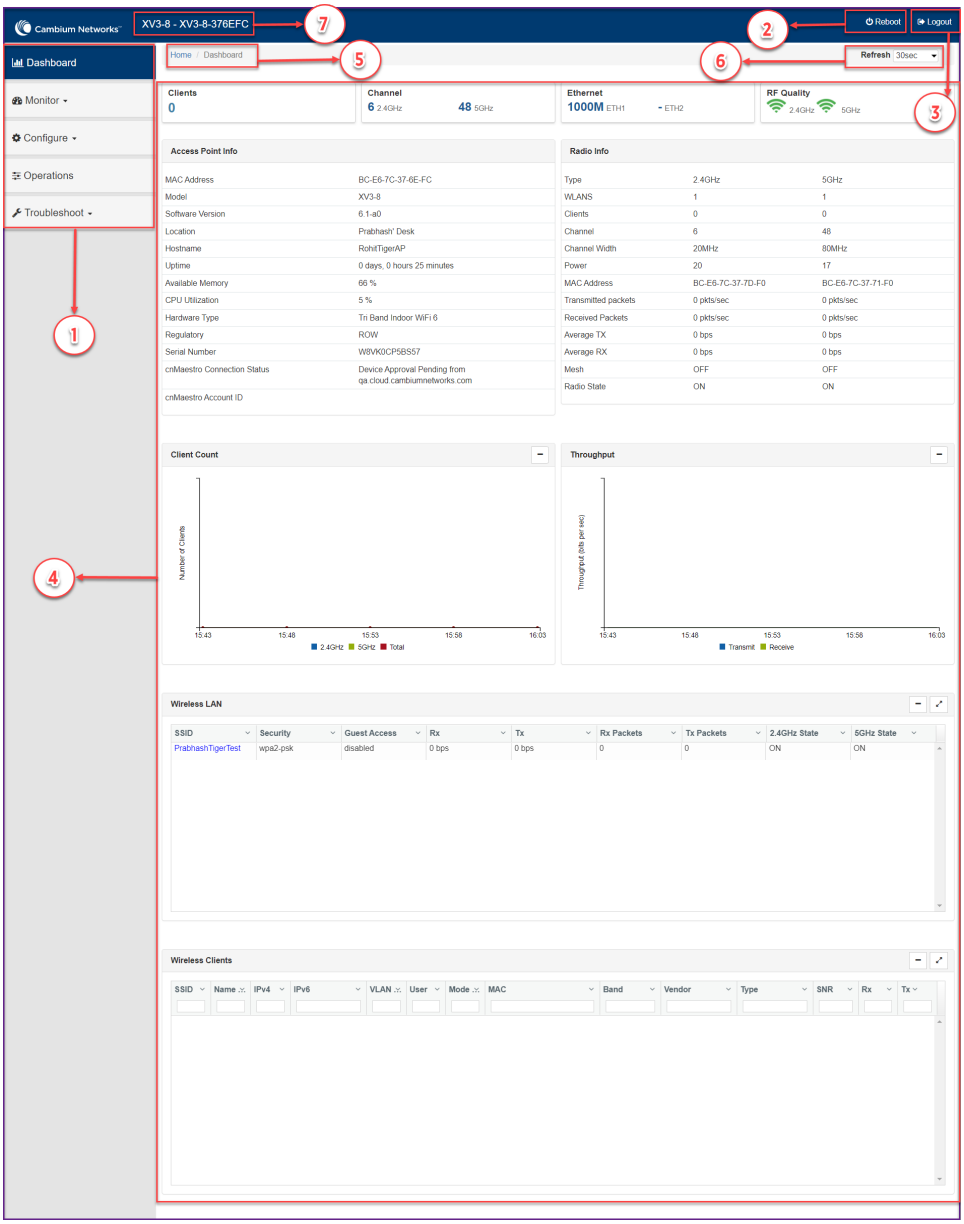


Table 7: Elements in the Enterprise Wi-Fi AP dashboard

Number	Element	Sub-Element	Description
1	Menu	-	Contains multiple tabs that help the user to configure, monitor, and troubleshoot the Enterprise Wi-Fi AP device. The menu consists of the following options: • Monitor • Configure

Number	Element	Sub-Element	Description
			• Operations • Troubleshoot
2	Reboot	-	Restarts the Enterprise Wi-Fi AP device ().
3	Logout	-	Sign out user from the Enterprise Wi-Fi AP device ().
4	Content	-	Contains details of configuration, statistics, or provision to configure Enterprise Wi-Fi AP device. Information displayed here varies based on the tab selected in the **Menu** section.
		RF Quality	Displays the device radio RF Quality Index that provides an indication of the RF link quality of wireless clients, or mesh clients, or both as seen by the AP's radio. It is the average of all the wireless clients and or mesh clients SNR. Following are the interpretation of the bars in the image: • Aggregate SNR is more than 45: RF Quality Index is displayed as **Excellent** • Aggregate SNR is more than 35 but less than 45: RF Quality Index is displayed as **Good** • Aggregate SNR is more than 25 but less than 35: RF Quality Index is displayed as **Average** • Aggregate SNR is less than 25: RF Quality Index is displayed as **Poor**
5	UI path	-	Provides UI navigation path information to the user.
6	UI refresh interval	-	Provision to reload updated statistics at regular intervals.
7	Model number	-	Displays the model number of the AP and the configured hostname.

Monitor

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

- **System:** Provides information related to Enterprise Wi-Fi AP device such as software image, hostname, and country code.

- **Radio**: Provides information such as RF statistics, neighbour list, and current radio configuration of the device.
- **WLAN**: Provides information on WLANs.
- **Network**: Provides information related to interfaces such as default route and interface statistics.
- **Services**: Provides information related to entities that support Bonjour.

Configure

This section allows users to configure various parameters on the Enterprise Wi-Fi AP devices based on deployment requirements. The **Configure** tab contains the following sections:

- **System**: Provision to configure system UI parameters.
- **Radio**: Provision to configure radio settings (2.4 GHz/5 GHz).
- **WLAN**: Provision to configure WLAN parameters as per the end user requirements and type of wireless station.
- **Network**: Provides information related to VLAN, routes, and Ethernet ports.
- **Services**: Provides information related to network and Bonjour gateway.

Operations

This section allows users to perform the following maintenance tasks on devices:

- **Firmware update**: Provision to upgrade software for the Enterprise Wi-Fi AP devices.
- **System**: Provides different methods of debugging field issues and recovering devices.
- **Configuration**: Provision to modify the configurations of a device.

Troubleshoot

This section allows users to debug and troubleshoot the devices remotely. The **Troubleshoot** tab contains the following sections:

- **Wi-Fi Analyzer**: Provides information related to air quality.
- **Connectivity**: Provides different modes of network reachability for the Enterprise Wi-Fi AP device.
- **Packet Capture**: Provides feasibility for the user to capture packets on operational interfaces.
- **Logs**: Supports the feasibility to check logs for different modules of Enterprise Wi-Fi AP devices. These logs help the customer to debug an issue.

Chapter 4: Configuring the System

This chapter describes the following topics:

Basic

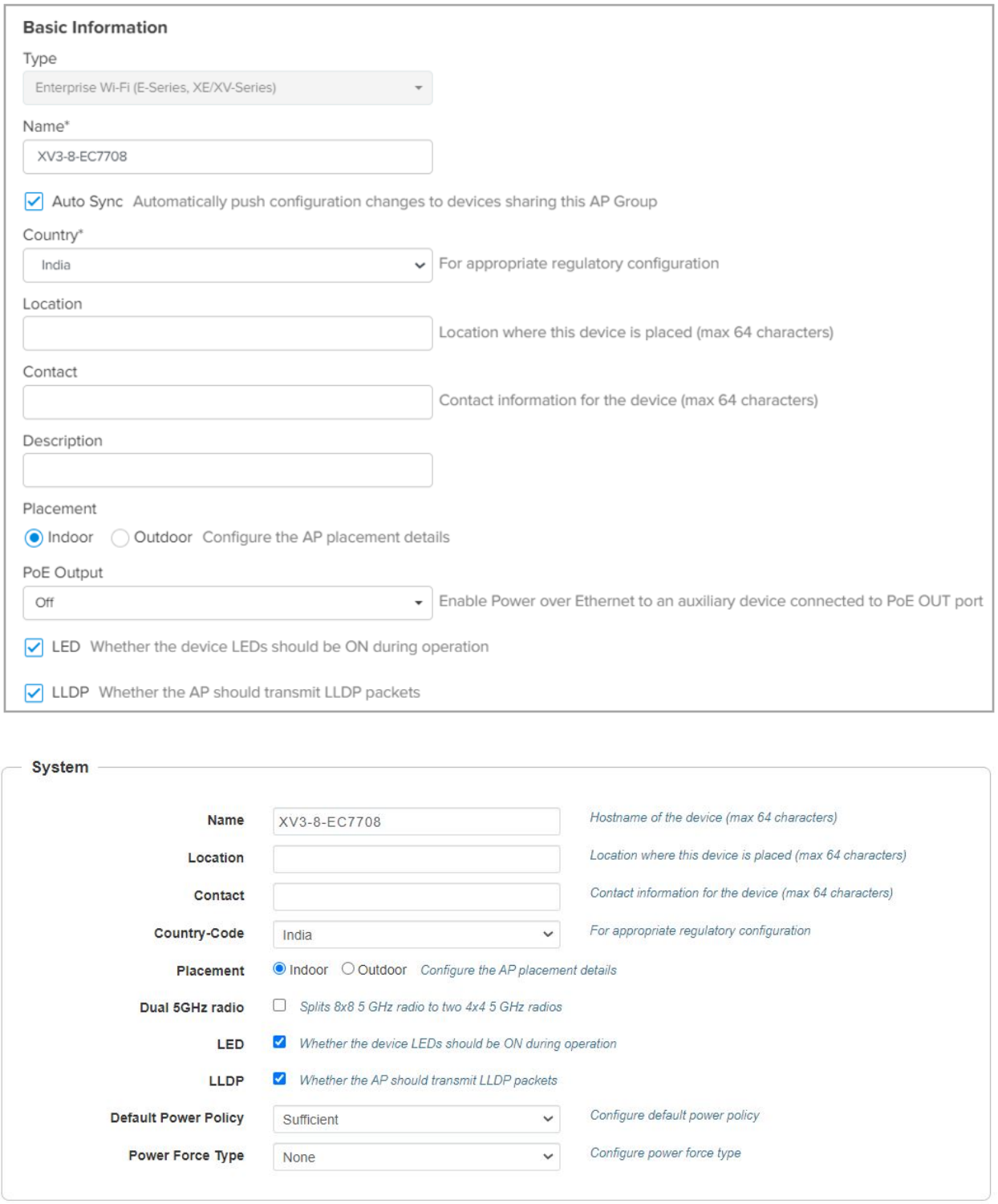
Table 8 lists configurable system parameters that are available under **Configuration > Basic** tab in the cnMaestro UI:

Table 8: Basic parameters

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

Parameter	Description	Range	Default
PoE Output	Enable power over Ethernet to an auxiliary device connected to PoE OUT port.	-	Off
Dual 5 GHz radio	Enable Dual 5 GHz radio. This parameter provides the flexibility of splitting 8x8 5 GHz radio into two 4x4 5 GHz radios.	-	Disabled
LED	When enabled, turns on the device LEDs during operation.	-	Enabled
LLDP	Advertises device capabilities and information in the L2 network.	-	Enabled
Channels Distribution	Allows unique distribution of channels across radios when multiple radios are configured with same frequency band. **Note**: This option is available only as a CLI-based configuration. Use the `channels-distribution` command.	-	Enabled
Default Power Policy	Provision to configure current power policy.	-	Sufficient
Power Force Type	Provision to configure power force type.	-	None

Figure 7: *The System page*



To configure the above parameters, navigate to the **Configuration > Basic** 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 the **Placement** checkbox parameter Indoor or Outdoor to configure the AP placement details.
6. Enable **Dual 5 GHz radio** checkbox.
7. Enable the **LED** checkbox.
8. Enable the **LLDP** checkbox.
9. Select **Default Power Policy** from the drop-down list.
10. Select **Power Force Type** from the drop-down list.
11. Click **Save**.

Power over Ethernet (PoE) in

Enterprise Wi-Fi APs first attempt to detect the type and classification of the Power Source (PS) they are being powered by using standard hardware handshake and control logic. Some PS devices are the passive type, like the Cambium PoE power injectors, and therefore the AP cannot detect the type or classification of the PS they are being powered by. For this reason, Enterprise Wi-Fi APs also use LLDP power negotiation to request a specific amount of PoE power from the PS. This feature in the Enterprise Wi-Fi APs is called LLDP power request and it is enabled by default.

The following table lists the PoE power requirements for the Enterprise Wi-Fi APs:

Caution

Although APs may operate in accordance with the power requirements mentioned in the **Hardware Power Requirement** column, caution is advised as the results may be unexpected.

Table 9: PoE power requirements for APs

Device	PoE Out	Hardware Power Requirement	Maximum Power Draw (Watts)	Minimum Power Required to boot (Watts)
XE3-4TN	Yes (Max 30W)	802.3at	64	15
XV2-2	No	802.3at	21	7.6
XV2-2T0	Yes (Max 30W)	802.3at	51	13.3
XV2-2T1	Yes (Max 30W)	802.3at	51	13.3

Device	PoE Out	Hardware Power Requirement	Maximum Power Draw (Watts)	Minimum Power Required to boot (Watts)
XV2-21X	No	802.3af	12.95	8
XV2-22H	Yes (Max 10W)	802.3af	22.95	8
XV2-23T	No	802.3af	12.95	8
XV3-8	No	802.3bt	35	22.9
XE3-4	No	802.3bt	32	15.6
XE5-8	No	802.3bt	60	32.9

Note

Accurate time on the AP is critical for features such as WLAN Scheduled Access, and Syslogs.

Figure 8: *Power policy configuration*

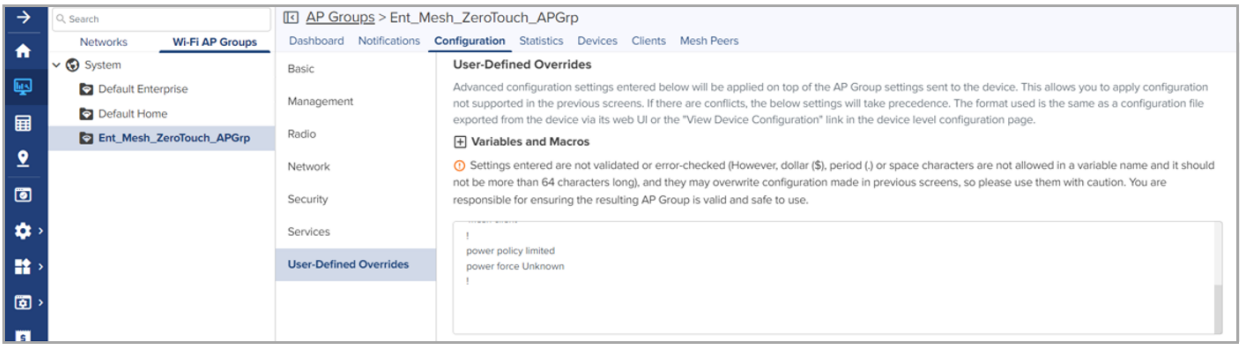


Table 10 lists the Cambium PoE injectors and cnMatrix models supported on the APs.

Table 10: Supported Cambium PoE Injectors and cnMatrix models

AP Model	Cambium PoE Injector	cnMatrix Recommended Model
XE3-4TN	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-2	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-2T0	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-2T1	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XV2-21X	N000000L142A / N000000L034B / N000900L017A	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P
XV2-22H	N000000L142A / N000000L034B	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P

AP Model	Cambium PoE Injector	cnMatrix Recommended Model
XV2-23T	N000000L142A / N000000L034B / N000900L017A	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P
XV3-8	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XE3-4	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P
XE5-8	N000000L142A	EX3028R-P / EX3052R-P / EX2016M-P

Attention

Configure Power policy and power force type based on the input power source.

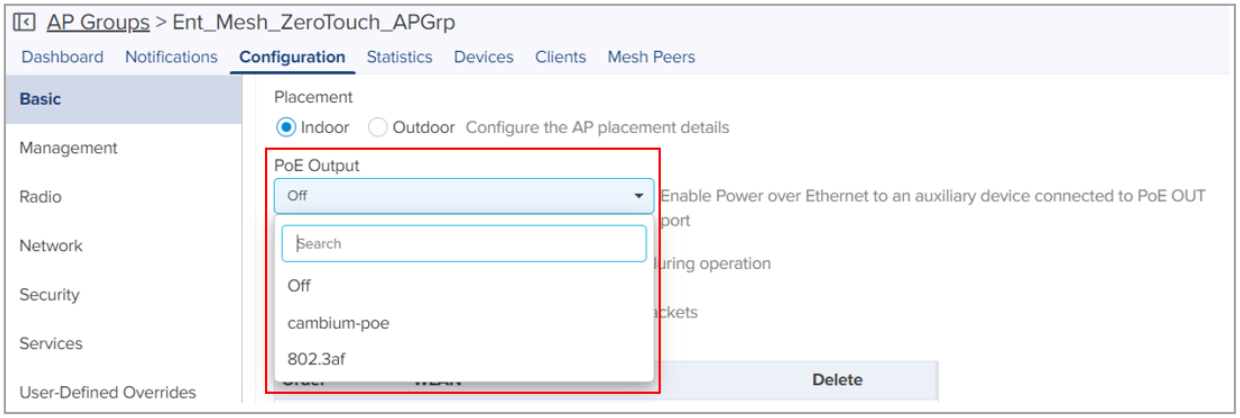
Power over Ethernet (PoE) Out port

PoE out provision is provided to power on devices that are compatible with IEEE802.3af/at PoE IN as per power consumption or Cambium 30v POE as shown in the below table.

Table 11: PoE-out capabilities

AP Model	10W	48V @ 15W	48V @ 30W	30V @ 30W	Default State
XV2-2T0		✓	✓	✓	Disabled
XV2-2T1		✓	✓	✓	Disabled
XV2-22H	✓				Disabled
XE3-4TN		✓	✓	✓	Disabled

Figure 9: *PoE Output cnMaestro configuration*



Link Layer Discovery Protocol (LLDP)

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

LLDP settings are enabled by default on AP. This implies power negotiation is also enabled over LLDP when an AP is powered by a Power over Ethernet (PoE) PSE switch port.

This window allows you to establish your LLDP settings. Use the **Save** button if you want to save the settings.

Power negotiation

LLDP discovers a device port (connected to a PoE PSE switch, for example) that supplies power to this AP. The AP checks that the port can supply the maximum power that is required by this AP model. AP sends the required maximum power (in watts) via LLDP frames to the PoE source and expects the PoE source to reply with the amount of power that can be allocated.

- If the AP receives a response confirming that the power allocated by the PoE PSE source is equal to or greater than the maximum power requested then the AP enables radios and other Model Specific peripherals (USB port, Bluetooth etc.).
- If the AP receives power allocation less than the maximum but more than the minimum to keep the radios operational then AP issues a Syslog message and shuts down the other peripherals (USB port, Bluetooth etc.).
- If the AP receives lesser than the minimum power for radios to operate in that case the radios are shut down for five minutes and power LLDP power negotiation continues to monitor available power to be minimum for AP radios to function.
- Click to check power status: `show power`

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.

CLI Configuration

Consider the following tasks to configure the CLI:

To enable:

```
XV3-8-EC7708(config)# lldp
XV3-8-EC7708(config)#
```

To disable:

```
XV3-8-EC7708(config)# no lldp
XV3-8-EC7708(config)#
```

To list LLDP configuration:

```
show lldp configuration
show lldp interfaces
```

Request power

To enable/disable power negotiation via LLDP:

```
XV3-8-EC7708(config)# lldp

request-power : Enable power negotiation (default:enabled)

tx-hold : Set transmit hold multiplier (default:4, used to calculate the time-to-live
(tx-interval * tx-hold))

tx-interval : Set LLDP packet transmit delay (in Sec, default:30 sec)

XV3-8-EC7708(config)# lldp request-power

<ENTER>

XV3-8-EC7708(config)# lldp request-power
```

Transmit hold

It is used to compute the Time To Live (TTL) value. This is the time during which the receiving device maintains information before the validity of information expires.

```
XV3-8-EC7708(config)# lldp

request-power : Enable power negotiation (default:enabled)

tx-hold : Set transmit hold multiplier (default:4, used to calculate the time-to-live
(tx-interval * tx-hold))

tx-interval : Set LLDP packet transmit delay (in Sec, default:30 sec)

XV3-8-EC7708(config)# lldp tx-hold

Specify transmit hold multiplier value (max 65535)
```

Transmit interval

It is the time interval between two regular LLDP packets transmissions. The AP sends out LLDP announcements, advertising its presence at this interval. The default value is 120 seconds.

```
XV3-8-EC7708(config)# lldp

request-power : Enable power negotiation (default:enabled)

tx-hold : Set transmit hold multiplier (default:4, used to calculate the time-to-live
(tx-interval * tx-hold))

tx-interval : Set LLDP packet transmit delay (in Sec, default:30 sec)

XV3-8-EC7708(config)# lldp tx-interval

Specify LLDP transmit delay in sec (max 65535)
```

Management

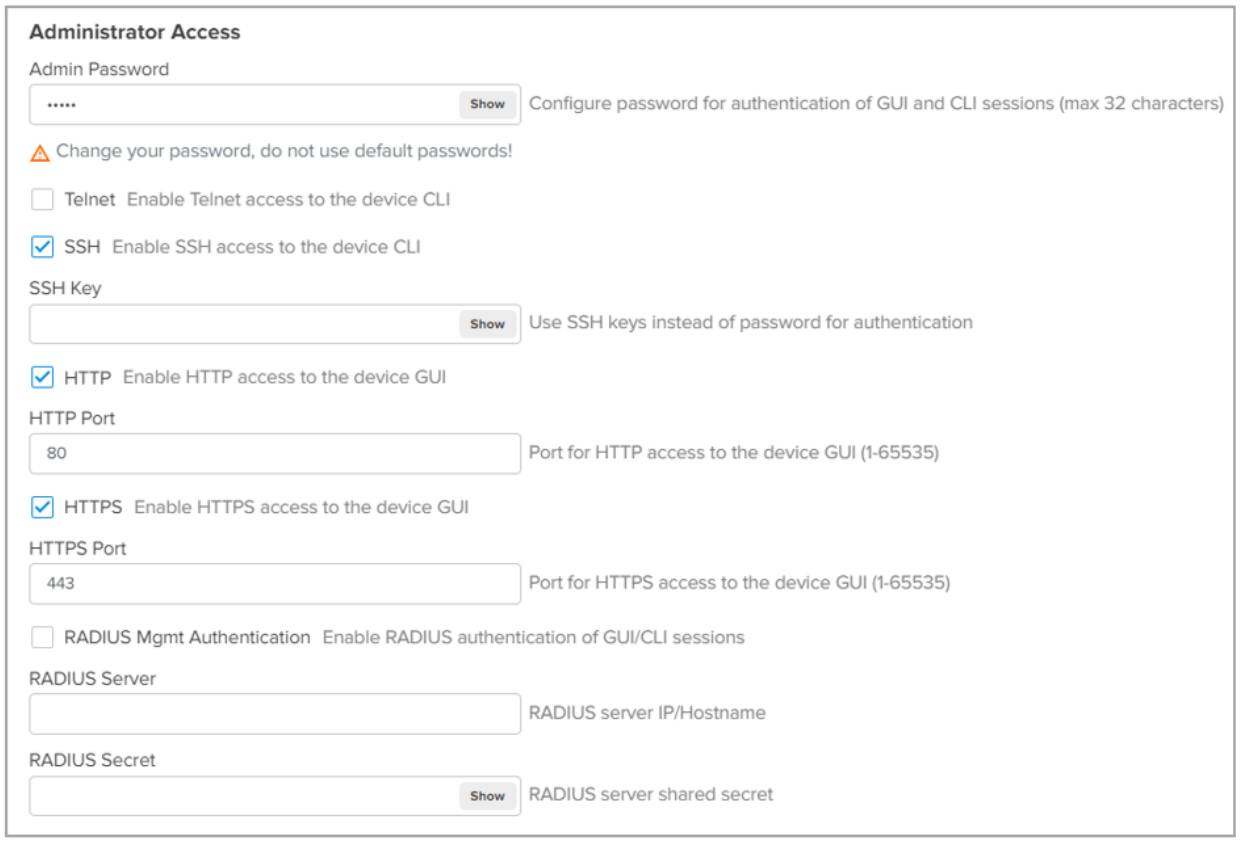
Administrator Access

Table 12 lists configurable fields that are displayed in the **Configuration > System > Management > Administrator Access** tab:

Table 12: Administrator Accessparameters

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. The user needs to add Public Key in this section. If configured, the 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 is provided by the user undergo RADIUS authentication. If successful, allowed to login to UI of the device. 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 URL.	-	-
Cambium ID	Cambium ID is used for provisioning cnMaestro (Cambium Remote Management) of this device.	-	-
Onboarding Key	Password used for onboarding the device to cnMaestro.	-	-

Figure 10: *Administrator Access page*



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.

   If certificate-based login is required, enter SSH Key in the textbox else select
4. Enable the **HTTP** checkbox to enable HTTP access to the device UI.
5. If a custom port other than the default is required, enter the **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 a custom port other than the default is required, enter the **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 the **RADIUS Server** parameter in the textbox.

b. Enter the **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.

HTTPS Proxy server configuration

The proxy management service is established in the AP to proxy management of traffic for remote management services originating from the AP.

For zero-touch configuration, refer to DHCP Option 43 - Zero-touch onboarding.

CLI Configuration:

```
XV3-8-EC7708(config)# management proxy
https : Enable HTTPS proxy support
XV3-8-EC7708(config)# management proxy https
host : Configure HTTPS proxy host
password : Configure HTTPS proxy password
port : Configure HTTPS proxy port
username : Configure HTTPS proxy username
```

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 resets to default and resyncs the time as the Enterprise Wi-Fi AP does not have battery backup. The servers can be specified as IPv4 address or as a hostname (Example: pool.ntp.org). If NTP is not configured on the device, the device synchronizes time with cnMaestro if onboarded.

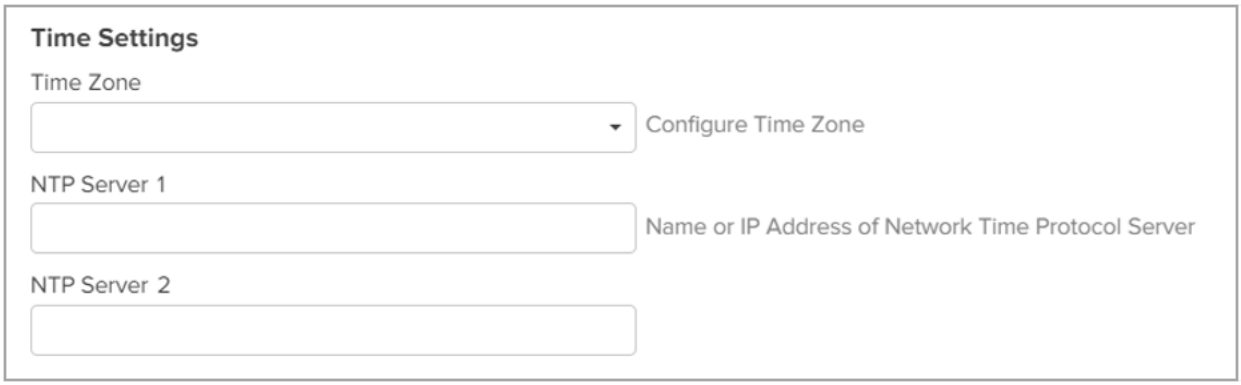
Table 13 lists the fields that are displayed in the **Configuration > Management > Time Settings** section.

Table 13: Time Setting parameters

Parameter	Description	Range	Default
Time zone	The time zone can be set according to the location where the AP is installed. Selecting the appropriate time zone from the drop-down list, ensures that the device clock is synced with the wall clock time.	-	-

Parameter	Description	Range	Default
	Note Accurate time on the AP is critical for features such as WLAN Scheduled Access, and Syslogs.		
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.	-	-

Figure 11: *Time setting page*



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

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

Event logging

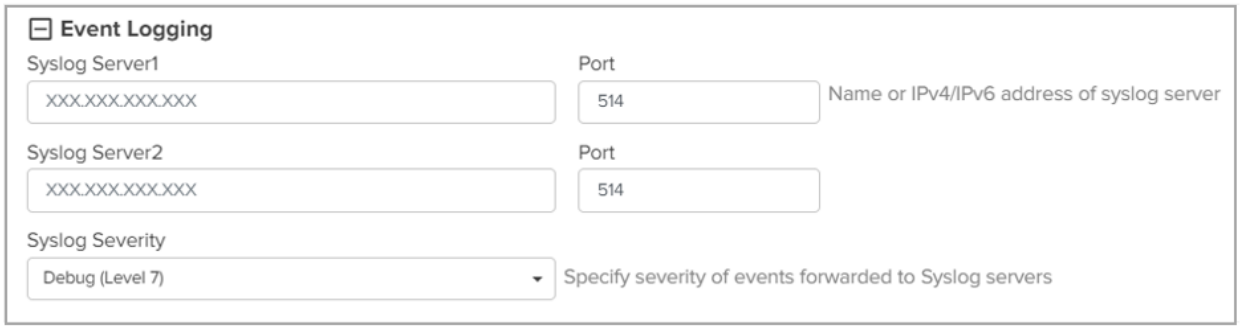
The Enterprise Wi-Fi AP devices support multiple troubleshooting methods. Event logging or Syslog is one of the standard troubleshooting processes. If you have a Syslog server in your network, you can enable it on an Enterprise Wi-Fi AP device.

Table 14 lists the fields that are displayed in the **Configuration > System > Event Logging** section.

Table 14: Event logging parameters

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

Figure 12: *Event logging page*



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

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

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

SNMP

Table 14 lists the fields that are displayed in the **Configuration > Management > SNMP** section.

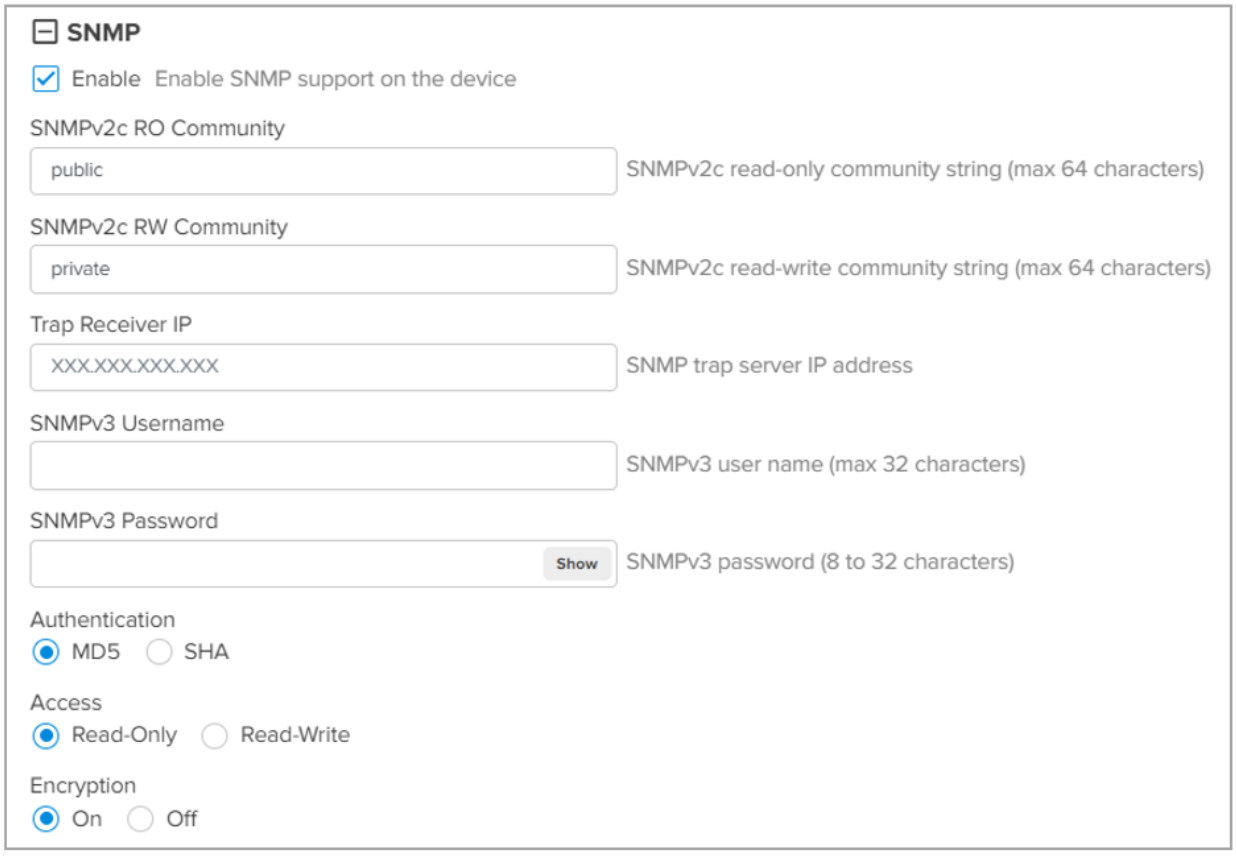
Table 15: SNMP parameters

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

Note

The AP uses the AES algorithm for encryption and SNMPv3 password configuration parameter is used for encryption and authentication.

Figure 13: *SNMP parameters*



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

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 supports 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** checkbox.
8. Select **Read-Only** or **Read-Write** from the **Access** checkbox.

9. Select ON or OFF from the **Encryption** checkbox.
10. Click **Save**.

Chapter 5: Configuring the Radio

This chapter describes the following topics:

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 5 GHz radio into two independently configurable and operational radios. In DBS mode, 5 GHz radio operates as single radio with an 8x8 configuration. In SBS mode, 5 GHz Radio operates as split radio with each 4x4 configuration. Configurable parameters under the **Radio** profile are listed below:

Basic

The following table lists configurable fields that are displayed in the **Configuration > Radio > Basic** tab:

Table 16: Configure Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables the operation of radio.	-	Enabled
Band	If any radio supports multiple bands then the user can select one of the bands.	-	-
Channel	The user can select the channel from the drop-down list. Channels in the drop-down list are populated based on the Country selected in **Configuration > System** UI.	• 2.4 GHz: 1 - 14 • 5 GHz: 36 - 173 • 6 GHz: 1 - 233	Auto

Parameter	Description	Range	Default
Channel Width	The user can select the following channel widths for the operation: • For 2.4 GHz: Only 20 MHz channel width is supported. • For 5 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel width are supported. **Note**: Please refer Chapter 5 for 160 MHz support with 5 GHz. • For 6 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel width are supported.	-	20 MHz
Transmit Power	The 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. The 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 are available at https://www.cambiumnetworks.com/products/wifi/. Transmit power drop-down box varies as per the country selected in Configuration > System UI. The default value is AUTO, which means radio transmit power is configured to the maximum as per the county configured selected in the **Configuration > System** UI.	• 2.4 GHz: 4 - 30 • 5 GHz: 4 - 30 • 6 GHz: 4 - 30	Auto
Beacon Interval	The user can configure time duration between two consecutive Beacons. 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, the lesser the range. The user can configure this value based on SLA in deployment. The drop-down list contains all values that are advertised by Enterprise Wi-Fi AP devices which include legacy, HT, and VHT rates.	Standard 802.11b and 802.11g data rates	1Mbps
Candidate Channels	Enterprise Wi-Fi AP provides the user to configure selective channels based on their requirement. Options vary based on a band of operation and are as follows: • **For 2.4 GHz:** ◦ All ◦ Specific • **For 5 GHz:**	• 2.4 GHz: 1 - 14 • 5 GHz: 36 - 173 • 6 GHz: 1 - 233	All

Parameter	Description	Range	Default
	◦ All ◦ Specific ◦ Prefer Non-DFS ◦ Prefer DFS • **For 6 GHz:** ◦ All ◦ Specific		
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.	• 2.4 GHz: b/g/n/ax • 5 GHz: a/n/ac/ ax	All mode
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 a device to capture neighbor clients and APs.	-	-
Dwell-time	Configure the time period to spend scanning of Wi-Fi devices on a channel.	50-300	50ms
Auto-RF (Dynamic-power)			
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 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 automatic cell logic.	1-10	2
Cellsize Overlap Threshold	Cell overlap will be allowed when the AP is determining automatic cell sizes.	0-100%	50%

Parameter	Description	Range	Default
Auto-RF (Dynamic Channel)			
acceptance-per-threshold	Provision to configure acceptance Packet Error Rate (PER) threshold.	-	-
channel-hold-time	Channel hold time specifies how much time AP needs to hold the channel.	0-1800	-
channel-load-weightage	Provision to configure the channel load parameter weightage used in ACS algorithm.	-	-
congestion-channel-switch	Provision to enable/disable congestion based channel switch.	-	Enabled
congestion-threshold	Provision to configure congestion threshold.	-	-
efficiency-weightage	Provision to configure the efficiency parameter weightage used in ACS algorithm.	-	-
interval	Configure periodic ACS interval in minutes; Set '0' to disable.	-	-
per-channel-switch samples	Provision to enable/disable PER based channel switch.	-	Enabled
samples	Configure the minimum number of samples required to run the channel selection.	-	-
allowed-wlan-modes	• access : Only access WLANs are allowed • mesh : Only mesh WLANs are allowed • default : Both mesh and access types of WLANs are allowed	-	default

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** check box 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 does not support 40 MHz, 80 MHz, and 160 MHz in 2.4 GHz.
4. Select radio transmits 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** check box.
9. Click **Save**.

To configure **Off Channel Scan**:

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

To configure **Auto-RF (Dynamic-power)**:

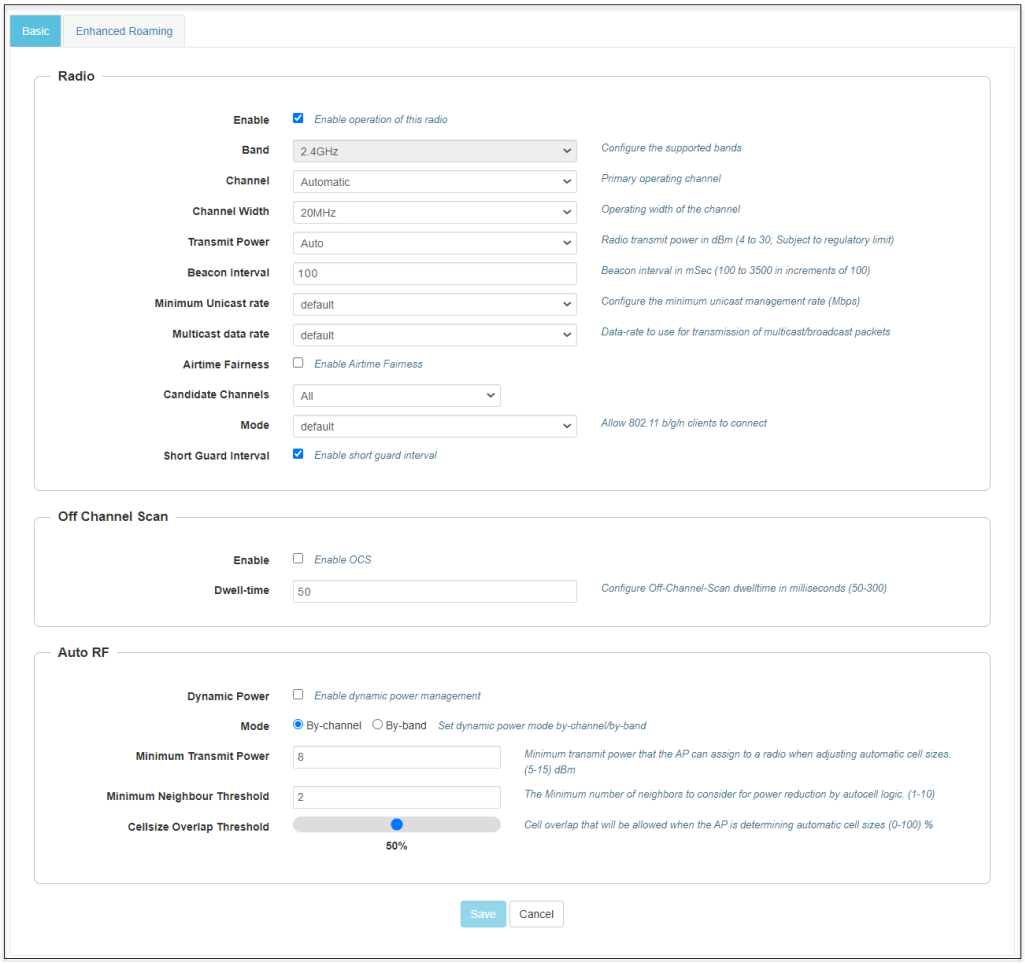
1. Select **Dynamic Power** check box to enable the operations of this radio.
2. Select the required dynamic power **Mode** as By-channel or By-hand.
3. Enter the **Minimum Transmit Power** in the text box.
4. Enter **Minimum Neighbour Threshold** parameter in the text box.
5. Click **Save**.

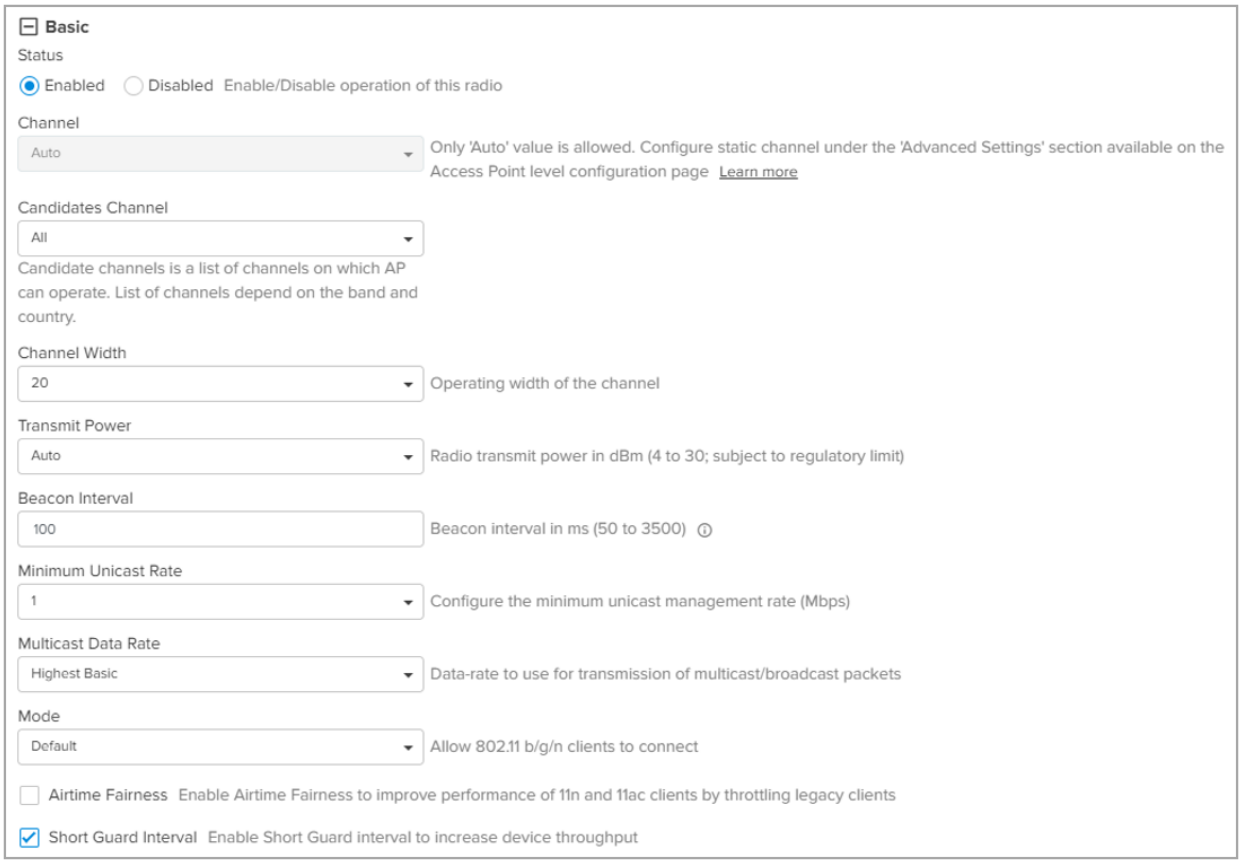
To configure **Auto-RF (Dynamic Channel)**:

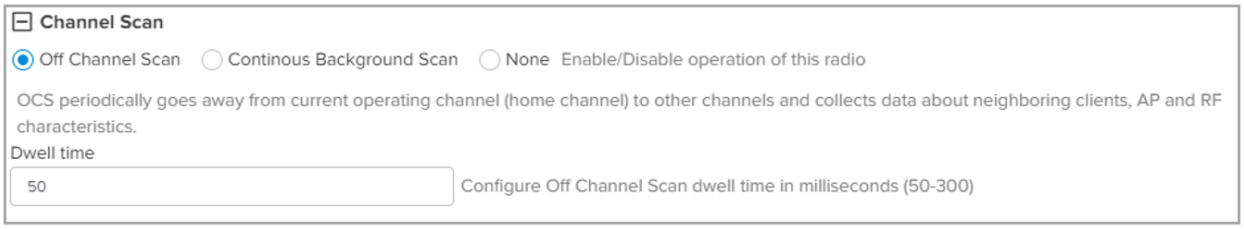
The following figure illustrates how to to configure **Auto-RF (Dynamic-channel)** using the CLI:

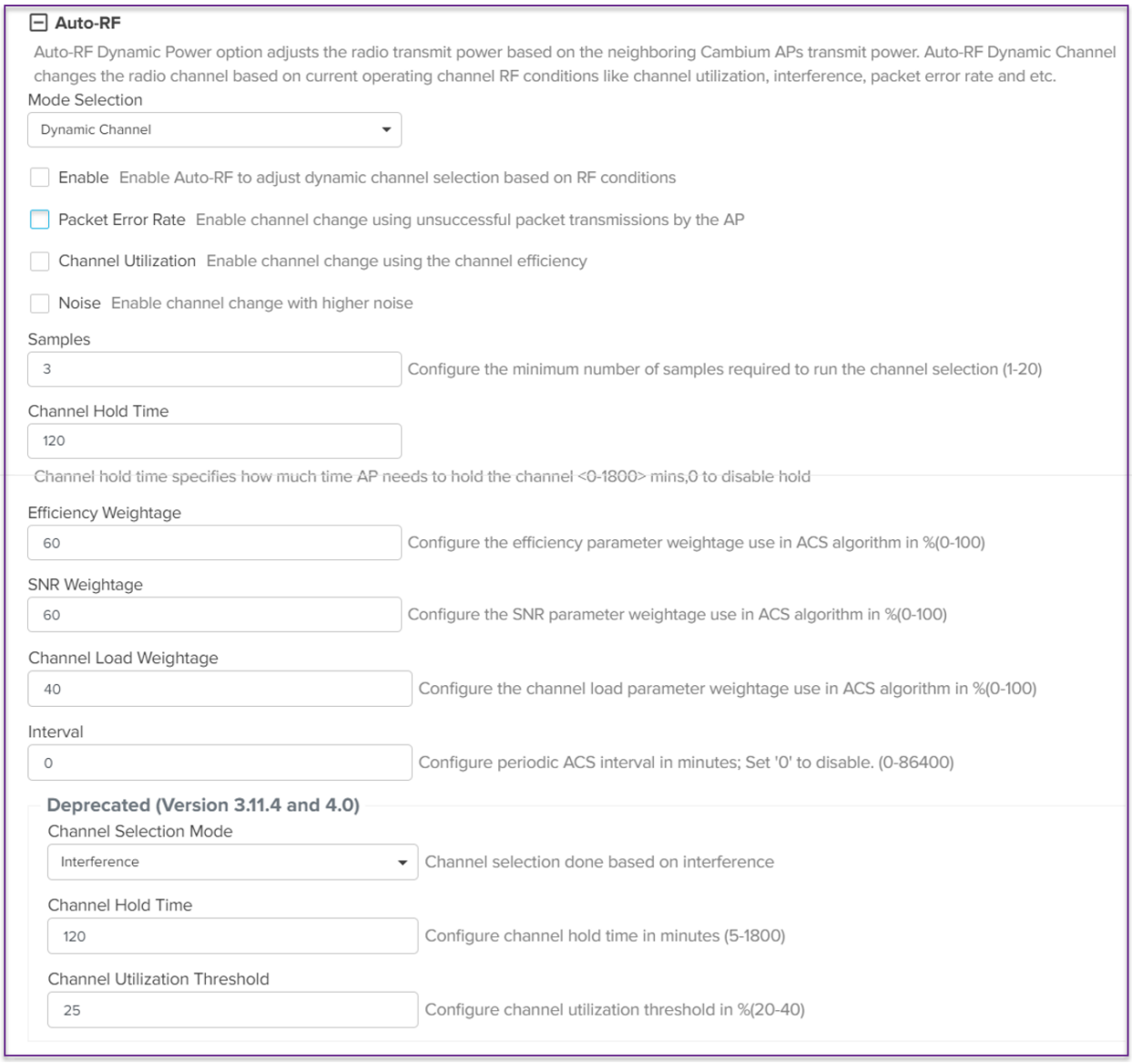
```
XV3-8-EC7708(config-radio-1)# auto-rf dynamic-channel

acceptance-per-threshold: Configure Acceptance Packet Error Rate (PER) threshold

channel-hold-time : channel hold time specifies how much time AP needs to hold the
channel <0-1800> mins,0 to disable hold

channel-load-weightage: Configure the channel load parameter weightage use in acs
algorithm

congestion-channel-switch: Enable / Disable Congestion based channel switch, enabled
by default

congestion-threshold: Configure Congestion threshold

efficiency-weightage: Configure the efficiency parameter weightage use in acs
algorithm

interval : Configure periodic ACS interval in minutes; Set '0' to disable

per-channel-switch : Enable / Disable PER based channel switch, enabled by default

samples : Configure the minimum number of samples required to run the channel
selection
```

Figure 14: *Radio parameters in the Basic page*




Basic
Status
Enabled
Disabled
Enable/Disable operation of this radio
Channel
Auto
Only 'Auto' value is allowed. Configure static channel under the 'Advanced Settings' section available on the Access Point level configuration page
Learn more
Candidates Channel
All
Candidate channels is a list of channels on which AP can operate. List of channels depend on the band and country.
Channel Width
20
Operating width of the channel
Transmit Power
Auto
Radio transmit power in dBm (4 to 30; subject to regulatory limit)
Beacon Interval
100
Beacon interval in ms (50 to 3500)
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
Mode
Default
Allow 802.11 b/g/n clients to connect
Airtime Fairness
Enable Airtime Fairness to improve performance of 11n and 11ac clients by throttling legacy clients
Short Guard Interval
Enable Short Guard interval to increase device throughput


Channel Scan
Off Channel Scan
Continous Background Scan
None
Enable/Disable operation of this radio
OCS periodically goes away from current operating channel (home channel) to other channels and collects data about neighboring clients, AP and RF characteristics.
Dwell time
50
Configure Off Channel Scan dwell time in milliseconds (50-300)



Software-Defined Radio (SDR) capabilities

Table 17: Supported radios

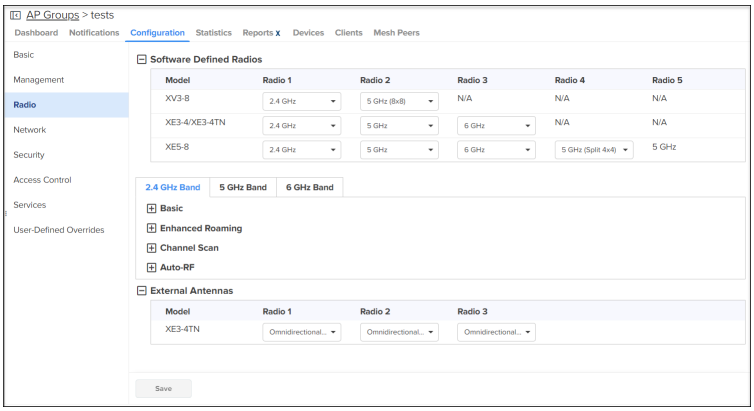
Access Point Model	Radio 1 (2.4 GHz)	Radio 2		Radio 3		Radio 4 (5 GHz)	Radio 5 (5 GHz)
		5 GHz	6 GHz	5 GHz	6 GHz		
XV3-8	✓	✓		✓			
XV2-2	✓	✓					
XV2-2T0	✓	✓					
XV2-2T1	✓	✓					

Access Point Model	Radio 1 (2.4 GHz)	Radio 2		Radio 3		Radio 4 (5 GHz)	Radio 5 (5 GHz)
		5 GHz	6 GHz	5 GHz	6 GHz		
XE3-4	✓	✓		✓	✓		
XE3-4TN	✓	✓		✓	✓		
XE5-8	✓	✓	✓	✓	✓	✓ (DBS)	✓ (SBS)
XV2-21X	✓	✓					
XV2-23T	✓	✓					
XV2-22H	✓	✓					

Table 18: Factory reset behavior of multi-radio APs

Access Point Model	Radio 1 (2.4 GHz)	Radio 2		Radio 3		Radio 4 (5 GHz)	Radio 5 (5 GHz)
		5 GHz	6 GHz	5 GHz	6 GHz		
XV3-8	ON	ON	NA	**OFF**	NA	-	-
XE3-4	ON	ON	NA	OFF	ON	-	-
XE3-4TN	ON	ON	NA	ON	OFF	-	-
XE5-8	ON	ON	OFF	OFF	ON	ON 4x4 SBS	ON 4x4 SBS

The **Radio** page allows the user to enable or disable the Software-Defined Radio (SDR) operations. It allows to configure **Software Defined Radios, Basic**, **Enhanced Roaming**, **Off Channel Scan**, **Auto-RF, and External Antennas**.



Note:

The software-defined radio creation and channel listing are populated based on the country-specific restrictions, device type, and release version.

Software-Defined Radio

Software-Defined Radio (SDR) allows you to configure radio parameters for XV3-8, XE3-4, and XE5-8 device models. By default these device models are configured for radio bands as shown in the above figure. The other radio bands for which the devices can be configured are as shown in Table 19.

Table 19: Supported Radio bands for Enterprise Wi-Fi Series (E-Series, XV-Series and XE-Series)

<table>
<tr><th rowspan="2">Models</th><th rowspan="2">Radios</th><th rowspan="2">Supported Radio Bands</th><th colspan="3">Channel Specification</th></tr>
<tr><th>Channel width</th><th>Default Channel width</th><th>Supported channel list</th></tr>
<tr><td rowspan="3">XV3-8</td><td>Radio 1</td><td>2.4 GHz</td><td>20/40</td><td>20</td><td colspan="2">1 to 13</td></tr>
<tr><td>Radio 2</td><td rowspan="2">5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)</td><td>20 / 40 / 80</td><td>40</td><td>100 to 165 in Split 4x4 dual radio</td><td>36 to 165 in 8x8 - single radio</td></tr>
<tr><td>Radio 3</td><td>20 / 40 / 80</td><td>40</td><td colspan="2">36 to 64 in Split 4x4 dual radio</td></tr>
<tr><td rowspan="3">XE3-4</td><td>Radio 1</td><td>2.4 GHz</td><td>20/40</td><td>20</td><td colspan="2">1 to 13</td></tr>
<tr><td>Radio 2</td><td>5 GHz</td><td>20 / 40 / 80</td><td>40</td><td colspan="2">36 to 64</td></tr>
<tr><td rowspan="2">Radio 3</td><td>5 GHz</td><td rowspan="2">20 / 40 / 80 / 160</td><td>40</td><td colspan="2">100 to 165</td></tr>
<tr><td>6 GHz</td><td>160</td><td colspan="2">Any 6 GHz channel</td></tr>
<tr><td rowspan="3">XE3-4TN</td><td>Radio 1</td><td>2.4 GHz</td><td>20/40</td><td>20</td><td colspan="2">1 to 13</td></tr>
<tr><td>Radio 2</td><td>5 GHz</td><td>20 / 40 / 80</td><td>40</td><td colspan="2">36 to 64</td></tr>
<tr><td rowspan="2">Radio 3</td><td>5 GHz</td><td rowspan="2">20 / 40 / 80 / 160</td><td>40</td><td colspan="2">100 to 165</td></tr>
<tr><td>6 GHz</td><td>160</td><td colspan="2">Any 6 GHz channel</td></tr>
<tr><td rowspan="6">XE5-8</td><td>Radio 1</td><td>2.4 GHz</td><td>20/40</td><td>20</td><td colspan="2">1 to 13</td></tr>
<tr><td>Radio 2</td><td>5 GHz or 6 GHz</td><td>20 / 40 / 80 / 160</td><td>20*/80**</td><td colspan="2" rowspan="4">Refer to Table 20 for Supported Channel list in 5 GHz and 6 GHz</td></tr>
<tr><td>Radio 3</td><td>5 GHz or 6 GHz</td><td>20 / 40 / 80 / 160</td><td>20*/80**</td></tr>
<tr><td>Radio 4</td><td rowspan="2">5 GHz (8x8 - single radio) or 5 GHz (Split 4x4 dual radio)</td><td>20 / 40 / 80</td><td rowspan="2">20</td></tr>
<tr><td>Radio 5</td><td>20 / 40 / 80</td></tr>
<tr><td colspan="7">* 5 GHz **6 GHz</td></tr>
</table>

Note:

- Split 4x4 is applicable only for 8x8 spatial streams supported devices. (Supported device models are XV3-8 and XE5-8).
- Dual 5 GHz Radio (Only supported for XV3-8 and XE5-8 Access Points) Splits 8x8 5 GHz radio into two 4x4 5 GHz radios.

Table 20: Supported Channel list 5 GHz or 6 GHz in XE5-8

Radio Index				Radio 1	Radio 2	Radio 3	Radio 4	Radio 5
8x8 mode of operation: Radio 4 & 5 as single radio with 8x8								
Radio 2	Radio 3	Radio 4 and 5						
5 GHz	5 GHz	5 GHz		NA	100 to 128	149 to 165	36 to 64	
6 GHz	5 GHz	5 GHz		NA	Any 6 GHz channel	100 to 165	36 to 64	
5 GHz	6 GHz	5 GHz		NA	100 to 165	Any 6 GHz channel	36 to 64	
6 GHz	6 GHz	5 GHz		NA	* 1 to 93	** 97 to 233 / 65 to 93	36 to 165	
Split 4x4 mode of operation: Radio 4 and 5 as individual radio with 4x4								
Radio 2	Radio 3	Radio 4	Radio 5					
5 GHz	5 GHz	5 GHz	5 GHz	NA	60 to 64	100 to 128	149 to 165	36 to 40
6 GHz	5 GHz	5 GHz	5 GHz	NA	Any 6 GHz channel	100 to 128	149 to 165	36 to 64
5 GHz	6 GHz	5 GHz	5 GHz	NA	100 to 128	Any 6 GHz channel	149 to 165	36 to 64
6 GHz	6 GHz	5 GHz	5 GHz	NA	* 1 to 93	** 97 to 233	100 to 165	36 to 64
Note: *FCC SKU 6GHz UNII-5 or 6 (1 - 93) EU SKU UNII-5 low (1 - 61) **FCC SKU 6GHz UNII-7 or 8 (97 - 233) EU SKU UNII-5 High (65 - 93)								

Note:

You can use no `channels-distribution global configuration` CLI command for all multi-radio platforms, such as XV3-8, XE3-4, and XE5-8 APs. When configured on device, default channel list can be overridden.

Off Channel Scan (OCS)

The following figure illustrates how to to configure **Off Channel Scan** using the CLI:

```
XV3-8-EC7708(config)# wireless radio 2
```

```
XV3-8-EC7708(config-radio-2)# off-channel-scan

dwell-time : Configure Off-Channel-Scan dwelltime
interval : Configure Off-Channel-Scan interval
type : Configure active/passive Off-Channel-Scan

XV3-8-EC7708(config-radio-2)# off-channel-scan type
active : active off channel scan
passive : passive off channel scan
```

Below table lists the fields that are required for configuring **Off Channel Scan**:

Table 21: Configuring Off Channel Scan

Parameter	Description	Range	Default
dwell time	Provision to configure Off Channel Scan dwell time. Needs to change 100 or more than 100+ ms for supporting passive scan method.	50-300	50ms
interval	AP Off Channel Scan interval time.	-	6 sec
type	Provision to configure Off Channel Scan types. • active AP Radio transmits a probe request and listens for a probe response from an AP. • passive AP Radio listens on each channel for beacons sent periodically by neighbor APs. Users are advised to use passive as scan type.	-	active

Enhanced Roaming

Below table lists configurable fields that are displayed in the **Configuration > Radio > Enhanced Roaming** tab:

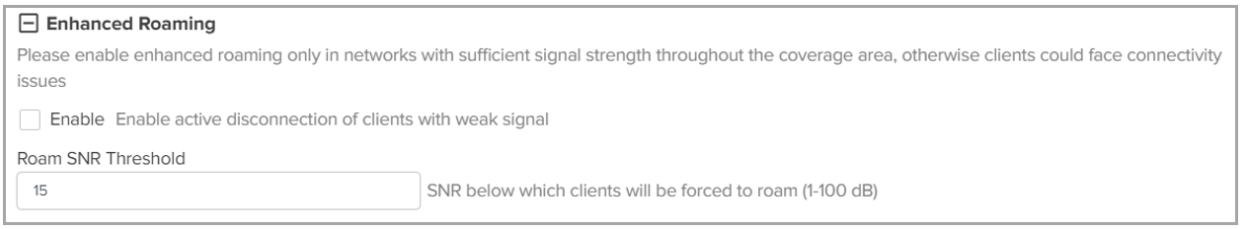
Table 22: Configure: Radio Enhanced Roaming parameters

Parameter	Description	Range	Default
Enhanced Roaming			
Enable	Provision to enable enhanced roaming on device.	-	Disabled
Roam SNR threshold	Enterprise Wi-Fi AP device triggers de-authentication of the wireless station when the wireless station is seen at configured SNR level or below.	1-100	15dB

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

1. Select the **Enable** check box to enable the operations of this radio.
2. Enter **Roam SNR threshold** parameter in the text box.
3. Click **Save**.

Figure 15: *The Enhanced Roaming parameters*



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 at 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 are enabled.

Receive sensitivity configuration

This feature enables users to configure the receiver sensitivity per radio. The configuration hooks are exposed from both CLI and XMS-Cloud. The cnMaestro does not expose any hooks for configuring receiver configuration. The receiver configuration is the signal power required at the receiver to achieve

the targeted or configured bit rate. Every RF receiver comes up with some default receiver sensitivity which may or may not be sufficient for achieving required RF performance in terms of meeting bit rate, hence reconfiguration of receiver sensitivity is suggested.

Multicast-snooping and Multicast-to-Unicast conversion

Multicast-to-Unicast conversion heavily depends on multicast (IGMP) snooping. With IGMP snooping enabled, the device monitors IGMP traffic on the network and forwards multicast traffic to only the downstream interfaces that are connected to interested receivers. The device conserves bandwidth by sending multicast traffic only to clients connected to devices that receive the traffic (instead of flooding the traffic to all the downstream clients in a VLAN).

The functionality to preserve both multicast and unicast MAC addresses during multicast enhancement implementation for packets in APs is introduced. The AP supports Directed Multicast Services (DMS) and Multicast Enhancement (ME). ME is a feature provided in APs that allows multicast frames to be sent as unicast frames to each member of the mentioned multicast group to improve the QoS of the transmission between the STA and the AP. The multicast frame is received at the host WLAN driver as an 802.3 (Ethernet) frame. This frame header contains the destination and source address, which are the multicast group address and client address, respectively. Iteratively, the Ethernet header is replaced with the unicast addresses of the clients present in the multicast group and sent out to the “air”. During this process, the multicast group address is completely lost from the frame.

CLI Configuration:

```
XV3-8-EC7708(config)# service show mcastsnoop br0 mdbtbl


----------------------------Bridge Snooping Hash Table -- IPv4----------------------------------
NUM    GROUP                                                FDB               PORT      AGE

IPv4 Router Ports:      None


----------------------------Bridge Snooping Hash Table -- IPv6----------------------------------
NUM    GROUP                                                FDB               PORT      AGE

IPv6 Router Ports:      None
XV3-8-EC7708(config)# service show mcastsnoop br0 acltbl

IGMP ACL TABLE:
        PATTEN 01:224.000.000.001/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- SYSTEM WIDE MANAGEMENT
        PATTEN 02:224.000.000.000/255.255.000.000 - 00:00:00:00:00:00/00:00:00:00:00:00 -- MANAGEMENT
        PATTEN 03:239.255.000.000/255.255.000.000 - 00:00:00:00:00:00/00:00:00:00:00:00 -- MANAGEMENT
        PATTEN 04:239.255.255.250/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- NON SNOOPING
        PATTEN 05:224.000.000.251/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- NON SNOOPING
        PATTEN 06:224.000.000.252/255.255.255.255 - 00:00:00:00:00:00/00:00:00:00:00:00 -- NON SNOOPING
        PATTEN 07:000.000.000.000/000.000.000.000 - 01:00:5e:00:00:00/ff:ff:ff:00:00:00 -- MULTICAST

MLD ACL TABLE:
        PATTEN 01:ff01:0000:0000:0000:0000:0000:0000:0001/ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff - 00:00:00:00:00:00/00:00:
00:00:00:00 -- SYSTEM WIDE MANAGEMENT
        PATTEN 02:ff02:0000:0000:0000:0000:0000:0000:0001/ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff - 00:00:00:00:00:00/00:00:
00:00:00:00 -- SYSTEM WIDE MANAGEMENT
        PATTEN 03:ff00:0000:0000:0000:0000:0000:0000:0000/fff0:0000:0000:0000:0000:0000:0000:0000 - 00:00:00:00:00:00/00:00:
00:00:00:00 -- MANAGEMENT
        PATTEN 04:0000:0000:0000:0000:0000:0000:0000:0000/0000:0000:0000:0000:0000:0000:0000:0000 - 33:33:00:00:00:00/ff:ff:
00:00:00:00 -- MULTICAST
```

```
XV3-8-EC7708(config)# multicast-snoop

XV3-8-EC7708(config)# no multicast-snoop

XV3-8-EC7708(config)# save

XV3-8-EC7708(config)# wireless radio 1

XV3-8-EC7708(config-radio-1)# multicast-to-unicast

XV3-8-EC7708(config-radio-1)# multicast-to-unicast mode 802.3

XV3-8-EC7708(config-radio-1)# multicast-to-unicast mode amsdu
```

```
XV3-8-EC7708(config-radio-1)# multicast-to-unicast exclude-list 224.0.0.1
XV3-8-EC7708(config-radio-1)# show wireless radios multicast-to-unicast
=========================================================================
RADIO BAND MC2UC MC2UC-MODE EXCLUDE-LIST
=========================================================================
radio1 2.4GHz NO amsdu
radio2 5GHz YES amsdu
XV3-8-EC7708(config-radio-1)#
```

Chapter 6: Configuring the Wireless LAN

This chapter describes the following topics:

Overview

Enterprise Wi-Fi AP devices support up to 16 unique WLANs. Each of these WLANs can be configured as per the customer requirement and type of wireless station.

Configuring the WLAN parameters

Configurable parameters under the WLAN profile are listed below:

Basic

Table 1 lists configurable fields that are displayed in the **Configuration > WLAN > Basic** tab.

Table 23: Basic parameters

Parameters	Description	Range	Default
WLAN > Basic			
Enable	Enables a WLAN profile. Once enabled, a Beacon is broadcasted with the SSID and the corresponding parameters configured in a WLAN profile.	-	-
Mesh	This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. This parameter supports the following options: • **Base** A WLAN profile configured with a mesh-base will operate as a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients. • **Client** A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-base AP to connect. • **Recovery** A WLAN profile configured as mesh-recovery will broadcast a pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on a mesh-base device. Meshclient will auto scan for mesh-recovery SSID upon failure of mesh link. • **Off** Mesh support disabled on WLAN profile.	-	OFF (Access Profile Mode)
VLAN	Segregates wireless station traffic from AP traffic in the network. Wireless stations obtain an IP address from the subnet configured in the VLAN field of the WLAN profile.	1-4094	1
Radios	Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options are available to configure transmit mode of SSID: • 2.4 GHz • 5 GHz • 6 GHz	-	all
SSID	Unique network name that wireless stations scan and associate.	-	-

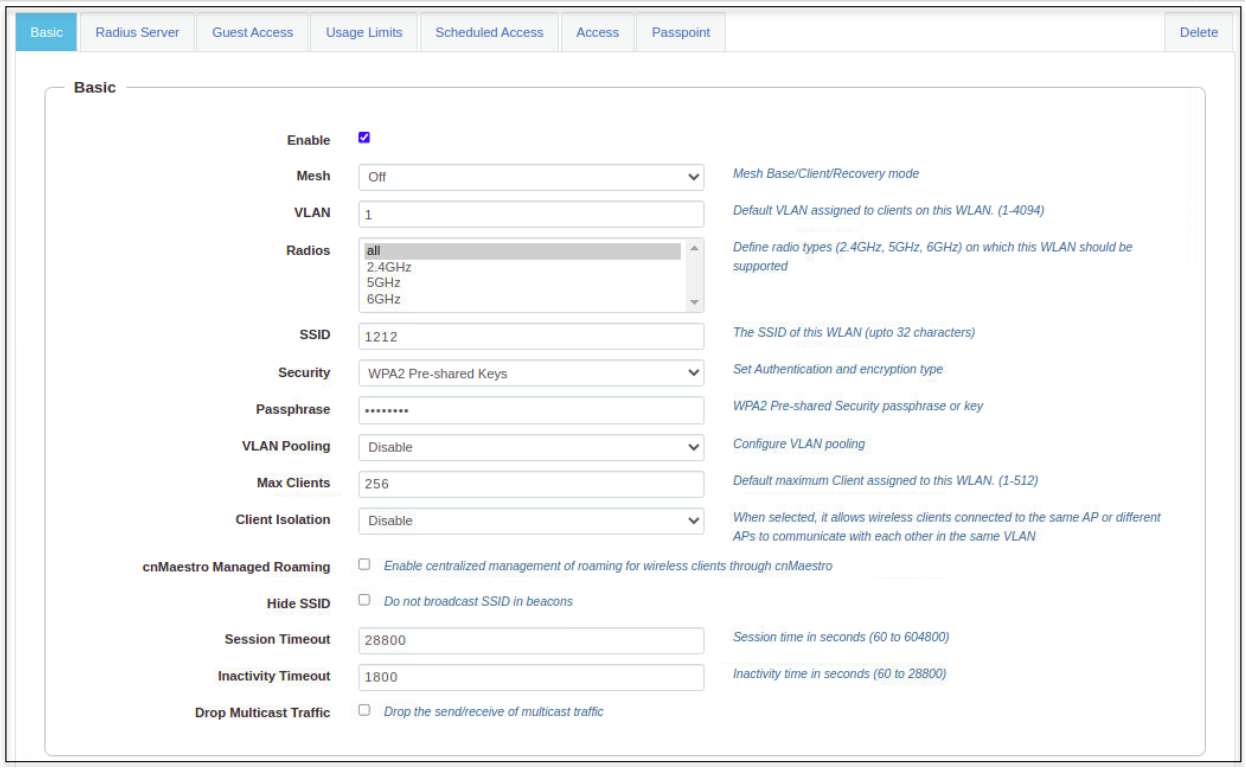
Parameters	Description	Range	Default
Security	Determines key values that are encrypted based on the selected algorithm. Following security methods are supported: • **Open** This method is preferred when Layer 2 authentication is built into the network. With this configured on an Enterprise Wi-Fi AP device, any wireless station will be able to connect. • **OWE** This method ensures the communication between each pair of endpoints is protected from other endpoints. • **Osen** This method is extensively used when Passpoint 2.0 is enabled on Enterprise Wi-Fi AP devices. If Passpoint 2.0 is disabled, this security plays no role in wireless station association. • **WPA2-Pre-Shared Keys** This mode is supported with AES and TKIP encryption. WPA-TKIP can be enabled from the CLI with the “allow-tkip” CLI option. • **WPA2 Enterprise** This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication methods. • **WPA2/WPA3 Pre-shared Keys** WPA3 comes with a transition mode where WPA2-only capable clients can connect to SSID. WPA2-only capable clients connect using the older PSK method while WPA3 capable clients connect using a more secure Simultaneous Authentication of Equals (SAE) method. • **WPA3 Pre-shared Keys** WPA3 replaces the Pre-Shared Key (PSK) exchange with SAE of Equals, which is more secure and provides forward-secrecy as well as resistance to offline dictionary attack. • **WPA3 Enterprise**	-	Open

Parameters	Description	Range	Default
	WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. • **WPA3 Enterprise CNSA** WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite and is commonly used in high-security Wi-Fi networks in government, defense, Finance, and industrial verticals. • **User Pre-shared keys** The U-PSK (User-PSK) Authentication settings are only used in conjunction with XMS Cloud's EasyPass Onboarding Portals. The Cloud automatically configures this setting for an WLAN when you create an Onboarding portal and you assign that WLAN to the portal. Thus, you should not normally change this setting manually. Note that the User- PSK settings are only available on the WLAN profile.		
Passphrase	The string that is a key value to generate keys based on the security method configured.	-	12345678
VLAN Pooling	This parameter is required when a 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 the deployment site. Modes supported are as follows: • **Disabled** This feature is disabled for this WLAN. • **Radius Based** The user is expected to configure WPA2 Enterprise for this mode to support. During the association phase, AP obtains pool name from RADIUS transaction and based on the 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. • **Static**	–	Disabled

Parameters	Description	Range	Default
	For this mode to support, the user requires to configure VLAN Pool details available under **Configure > Network > VLAN pool**. During the association phase, AP obtains pool, and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4 address from the VLAN selected by the Enterprise Wi-Fi AP device.		
Max Clients	This specifies the maximum number of wireless stations that can be associated with a WLAN profile. This varies based on the Enterprise Wi-Fi AP device model number. Refer to Table 24 for more details.	1-512 (Refer Table 24)	256
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: • **Disable** This option when selected disables the client isolation feature. i.e. any wireless station can communicate to other wireless stations. • **Local** This options when selected enable the client isolation feature. This option prevents wireless station communications connected to the same AP. • **Network Wide** This options when selected enable the client isolation feature. It prevents wireless stations communications connected to different AP deployed in the same L2 network. **Note**: • Network-wide mode is not supported when Redundancy Gateway protocol is used on deployment. • In the Redundancy Gateway case, Network-wide static can be used to provide a list of Gateway MAC addresses. • **Network Wide Static**		

Parameters	Description	Range	Default
	This option when configured enables client isolation feature across the 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 are selected, the user has the provision to add the whitelist MAC addresses to allow the communication. A maximum of 64 MAC addresses can be added.		
cnMaestro Managed Roaming	Provision to enable centralized management of roaming for wireless clients through cnMaestro.	-	-
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 applies to all wireless clients connected to the SSID. When a wireless station connects, a session timer is triggered. Once session time expires, the wireless station must undergo either re-authentication or re-association based on the state of the wireless station. By default, it is enabled. **Note** • Following priority takes precedence for the session timeout: a. Configured from the RADIUS server b. Configured from the AP	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 send a de-authentication to that wireless station. By default, it is enabled. **Note** • Following priority takes precedence for the inactivity timeout: a. Configured from the RADIUS server b. Configured from the AP	60-28800	1800

Figure 16: *Basic parameter*



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 (2.4 GHz, 5 GHz) 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 **cnMaestro Managed Roaming** checkbox.
11. Enable **Hide SSID** checkbox.
12. Enter the session timeout value in the **Session Timeout** textbox.
13. Enter the inactivity timeout value in the **Inactivity timeout** textbox.
14. Click **Save**.

Table 24: WLAN (Max clients) parameters

Number of clients	2.4 GHz	5 GHz	6 GHz	Concurrent
XV3-8	512	1024*	NA	1536
XE5-8	512	1024*	1024**	2560
XV2-2	512	512	NA	1024
XV2-2T0	512	512	NA	1024
XV2-2T1	512	512	NA	1024
XE3-4	512	512	512	1536
XE3-4TN	512	512	512	1536
XV2-21X	128	128	NA	256
XV2-23T	128	128	NA	256
XV2-22H	128	128	NA	256

* Two 5 GHz radios are available in Single Band Simultaneous (SBS) mode.

** Two 6 GHz radios are available in XE5-8 platform.

Maximum wireless client

At present, the WLAN profile provides an option to configure the maximum wireless clients association limit. This configuration limits the maximum number of clients per SSID per Radio. For example, if a user configures the maximum wireless client as 10, on a device capable of 2.4 GHz and 5 GHz radios, the total number of clients that can be associated is 10 across each Radio. This has been enhanced in Release 6.5 to set the maximum clients limit per SSID irrespective of the number of Radios to which SSID has been mapped.

Maximum clients per device

Most customers commonly use more than a single SSID. They prefer to set the maximum number of wireless clients connection per device, i.e. irrespective of the number of WLAN profiles and the number of radios, the maximum number of clients that can be associated is equivalent to the value configured for the parameter max-clients. This is a global configuration.

CLI configuration:

```
XV3-8-EC7708(config)# max-clients
0|<1-1536> '0' disables max client per device
```

Maximum clients per SSID

This option helps to limit the number of wireless clients connected to a WLAN profile (SSID) irrespective of the number of Radios. This configuration is supported at the WLAN level. This can be enabled as follows:

CLI configuration:

```
XV3-8-EC7708(config)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# enforce-max-clients-per-ssid
```

Maximum clients per SSID per Radio

This is the default configuration of the device. This configuration limits the maximum number of clients per SSID per radio. For example, if a user configures the maximum wireless client as 20, on a device capable of 2.4 GHz and 5 GHz Radios, the total number of clients that can be associated is 20 across each Radio. This configuration is supported at the WLAN level.

CLI configuration:

```
XV3-8-EC7708(config)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# max-associated-clients
<1-1536>
```

The default priority order can be:

1. Per device (Global limit)
2. Per SSID and (enforce at SSID level)
3. Per SSID Per Radio basis (present default option)

To keep backward compatibility with the existing deployments, the default option can be Per SSID Per Radio basis.

Opportunistic Wireless Encryption (OWE)

OWE is a Wi-Fi standard, which ensures that the communication between each pair of endpoints is protected from other endpoints. The OWE transition mode allows OWE-capable STAs to access the network in OWE authentication mode. The OWE transition mode is implemented as follows:

You need to create two WLANs on an AP.

For example,

1. WLAN-1:

   open authentication

   owe-transition-ssid: Provides WLAN-2 owe security SSID

2. WLAN-2:

   owe authentication

   owe-transition-ssid: Provides WLAN-1 open security SSID

CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# owe-transition-ssid
owe-transition-ssid : Configure the matching open/owe transition ssid
```

Note

The OWE transition mode SSIDs does not apply to a 6 GHz radio.

Table 25: Advanced parameters

<table>
<tr><th>Parameters</th><th>Description</th><th>Range</th><th>Default</th></tr>
<tr><td colspan="4">WLAN > Advanced</td></tr>
<tr><td>UAPSD</td><td>When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming are in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by the 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. This IE provides information on channel usage by AP, so that smart wireless stations can decide better AP for connectivity. Station count, Channel utilization, and Available admission capacity are the information available in this IE.</td><td>–</td><td>Disabled</td></tr>
<tr><td>DTIM interval</td><td>This parameter plays a key role when power save supported mobile stations are part of the infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.</td><td>1-255</td><td>1</td></tr>
<tr><td colspan="4">Monitored Host</td></tr>
<tr><td>Host</td><td>This feature is required where there is an interrupted backbone network. Enterprise Wi-Fi AP device monitors the reachability of hostname/IP configured in this parameter and modifies the state of WLAN.</td><td>-</td><td>Disabled</td></tr>
<tr><td>Interval</td><td>The frequency of monitoring the network health based on the status of the keep-alive mechanism w.r.t configured monitored host.</td><td>60-3600 sec</td><td>300</td></tr>
<tr><td>Attempts</td><td>The number of packets in the keep-alive mechanism to determine the status.</td><td>1-20</td><td>1</td></tr>
<tr><td>DNS Logging Host</td><td>By enabling this feature, the Administrator can monitor the websites accessed by wireless stations connected to WLAN profile.</td><td>–</td><td>Disabled</td></tr>
</table>

Parameters	Description	Range	Default
Connection Logging Host	When enabled provides information of all IP connections accessed by a wireless station that is associated with WLAN and logs the connection data seamlessly onto an external syslog server.	–	Disabled
Band Steering	This feature when enabled steers wireless stations to connect to 5GHz. There are three modes supported by Enterprise Wi-Fi devices. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces the wireless station to connect to the 5 GHz band. • Low • Normal • Aggressive	–	Disabled
Proxy ARP	Provision to avoid ARP flood in a wireless network. When enabled, AP responds to ARP requests for the wireless stations connected to that AP. This is for IPv4 infrastructure.	–	Enabled
Insert DHCP Option 82	When enabled, DHCP packets generated from wireless stations that are associated with APs are appended with Option 82 parameters. Option 82 provides a provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID: • Hostname • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom • All  **Note** In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered: 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration	–	Disabled

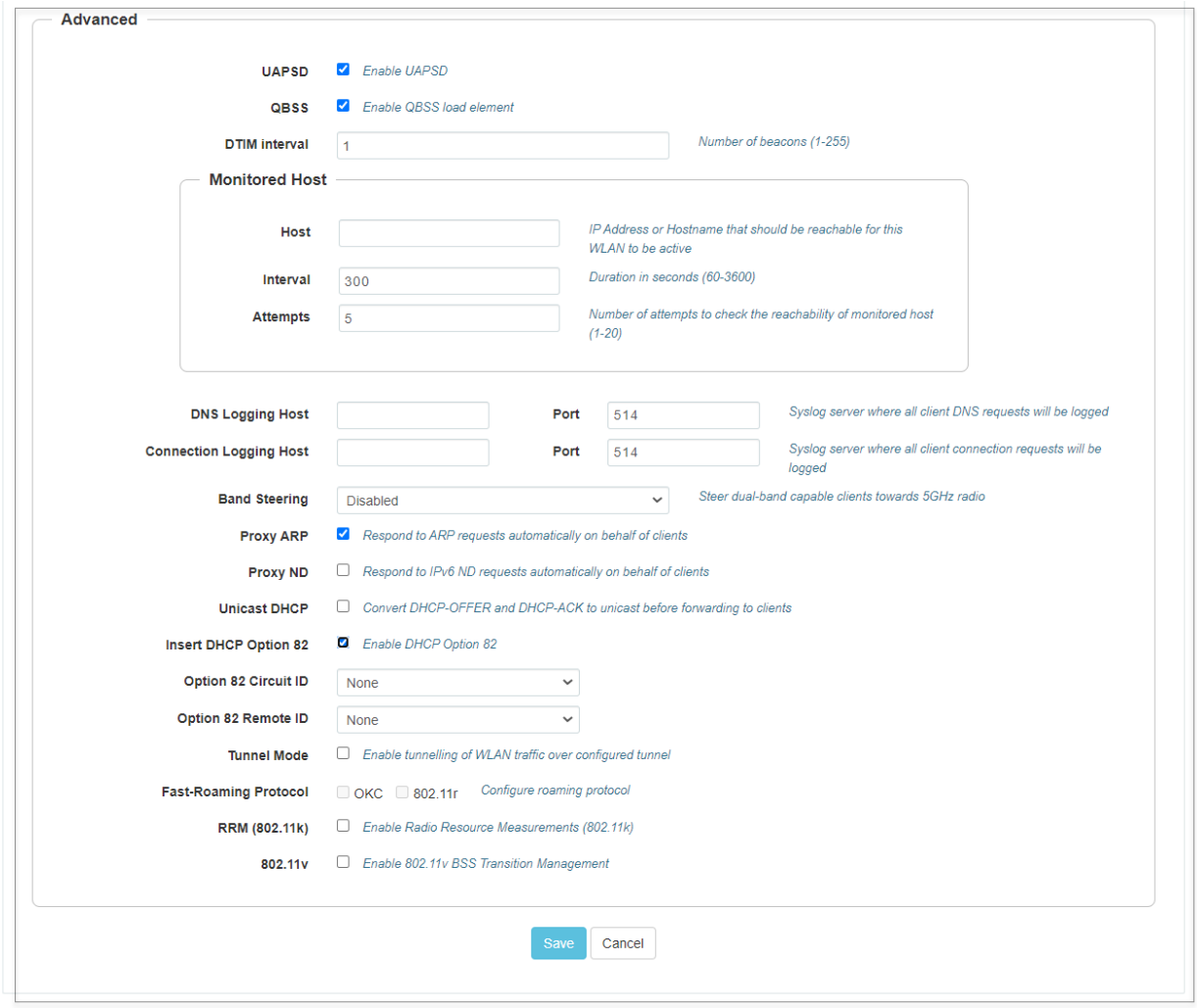
Parameters	Description	Range	Default
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	One of the important aspects to support voice applications on a Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 ms to avoid any call drop. This is easily achievable when the 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 the AAA server, and hence depending on the location of the AAA server the roaming time will be above 700 ms. Select any one of the following: • **OKC** This roaming method is a Cambium Networks proprietary solution to share the client authentication information with other Cambium Networks APs on the same network by sending encrypted information on wire on SSID VLAN. This information sharing does not require cnMaestro so even in cases where AP is not connected to cloud, the roaming will be seamless. • **802.11r** Fast transition (FT) is an IEEE standard to permit continuous connectivity aboard wireless devices in motion, with fast and secure client transitions from one Basic Service Set (abbreviated BSS, and also known as a base station or more colloquially, an access point) to another, performed in a nearly seamless manner. The terms handoff and roaming are often used, although 802.11 transition is not a true handoff/roaming process in the cellular sense, where the process is coordinated by the base station and is generally uninterrupted.	–	Disabled
RRM (802.11k)	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 802.11k clients. The following parameter must be enabled: • **Enable RRM**	–	Disabled
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF (802.11w)	802.11w also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames make wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	–	Optional

Parameters	Description	Range	Default
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 the 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 the 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 a customized port number in the textbox. If the port number is not entered, AP will take the 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 a customized port number in the textbox. If the port number is not entered, AP will take the default value as 514.
9. Select **Band Steering** parameter for 5GHz band from the drop-down list.
10. Enable **Proxy ARP** checkbox to avoid ARP flood in a wireless network.
11. Enable **Insert DHCP Option 82** checkbox.
12. Select **Option 82 Circuit ID** to enable DHCP Option-82 from the drop-down list.
13. Select **Option 82 Remote ID** to choose the MAC address of the AP from the drop-down list.
14. Select **Tunnel Mode** checkbox to enable tunneling of WLAN traffic over the configured tunnel.
15. Enable the required OKC or 802.11r configure roaming protocol in the **Fast-Roaming Protocol** checkbox.
16. Enable **RRM (802.11k)** checkbox.
17. Enable **802.11v** checkbox.
18. 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.
19. Click **Save**.

Figure 17: *Advanced parameter*



Band steering also supports client load balancing based on the below CLI configuration:

```
XV3-8-EC7708(config)# wireless wlan 1

XV3-8-EC7708(config-wlan-1)# band-steer-load-balancing

client-counts : client counts for band steer to consider clients load balancing

client-percentage : Client percentage for band steer to consider clients load
balancing
```

WLAN VLAN allowed list

This is an optional CLI to configure the allowed VLAN list upfront. It is needed in multiple VLAN scenarios such as Dynamic VLAN, ePSK-based VLAN, and RADIUS VLAN.

CLI configuration:

```
XV3-8-EC7708(config)# wireless wlan 1

XV3-8-EC7708(config-wlan-1)# vlans-allowed

{vlan_list} <e.g 1-10,15,100>
```

```
XV3-8-EC7708(config-wlan-1)# vlans-allowed 1-10
```

ICMPv6 Router advertisement (RA) unicast conversion

Convert ICMPv6 RA Multicast packets to Unicast for all stations. ICMPv6 RA unicast conversion is needed in multiple VLAN scenarios such as Dynamic VLAN, ePSK-based VLAN, and RADIUS-based VLANs.

This CLI configuration allows to configure the VLANs where ICMPv6 RA unicast conversion is needed.

CLI configuration:

```
XV3-8-EC7708(config)# wireless wlan 1

XV3-8-EC7708(config-wlan-1)# ipv6-router-advertisement-unicast

vlans : Configure vlans where IPV6 Router Advertisement unicast conversion needed

XV3-8-EC7708(config-wlan-1)# ipv6-router-advertisement-unicast vlans

{vlan_list} <e.g 1-10,15,100>

XV3-8-EC7708(config-wlan-1)# ipv6-router-advertisement-unicast vlans 1-10
```

802.11k/v

802.11k

Radio Resource Measurement (RRM) defines and exposes radio and network information to facilitate the management and maintenance of a wireless network. 802.11k is intended to improve the way traffic is distributed within the network.

The client can request a neighbor report from the AP using the neighbor_report_req management message. The client may request neighbors with **matching** SSID or request for all neighbors in the vicinity. The AP collects the neighbor information using proprietary methods and provides the list of neighbors to the client in the neighbor_report_rsp message.

802.11v

802.11v is deployed on the APs to govern the wireless networking transmission methods. It allows clients and APs to exchange information regarding the network topology, and RF environment. This facilitates the wireless devices to be RF-aware for participating in network-assisted power savings and network-assisted roaming methods.

The client may send solicited BSS Transition Management messages to AP before making roaming decisions. The idea is to identify the best APs to roam. The AP, after receiving the message from a client is expected to respond with the best APs in the vicinity to assist the client in roaming. The neighbor information is collected using proprietary methods.

RADIUS server

Table 4 lists configurable fields that are displayed in the **Configuration > WLAN > AAA Servers** page:

Table 26: Radius Server parameters

Parameters	Description	Range	Default
Authentication Server	Provision to configure RADIUS Authentication server details such as Hostname/IPv4, Shared Secret, Port Number and Realm. A maximum of three RADIUS servers can be configured.	-	Disabled
Accounting Server	Provision to configure Accounting server details such as Hostname/IPv4, Shared Secret, Port Number. A maximum of three RADIUS servers can be configured.	-	Disabled
Timeout	This field indicates wait time period for a response from the AAA server.	1-30	3
Attempts	Parameter to configure many attempts that a device should send AAA request to server if no response is received within the configured timeout period.	1-3	1
Accounting Mode	This field is enabled based on customer requirements. The accounting packet is transmitted based on the mode selected. • **Start-Stop** Accounting packets are transmitted by AP to the AAA server when a wireless station is connected and then disconnects. • **Start-Interim-Stop** Accounting packets are transmitted by AP to the AAA server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects. • **None** The accounting mode will be disabled.	-	Disabled
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Sync Accounting Records	Provision to configure accounting records to be synced across neighboring APs.	-	-
Server Pool Mode	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode. • **Load Balance**—AP communicates with multiple servers and ensures that authorization and accounting are equally shared across configured servers.	-	Failover

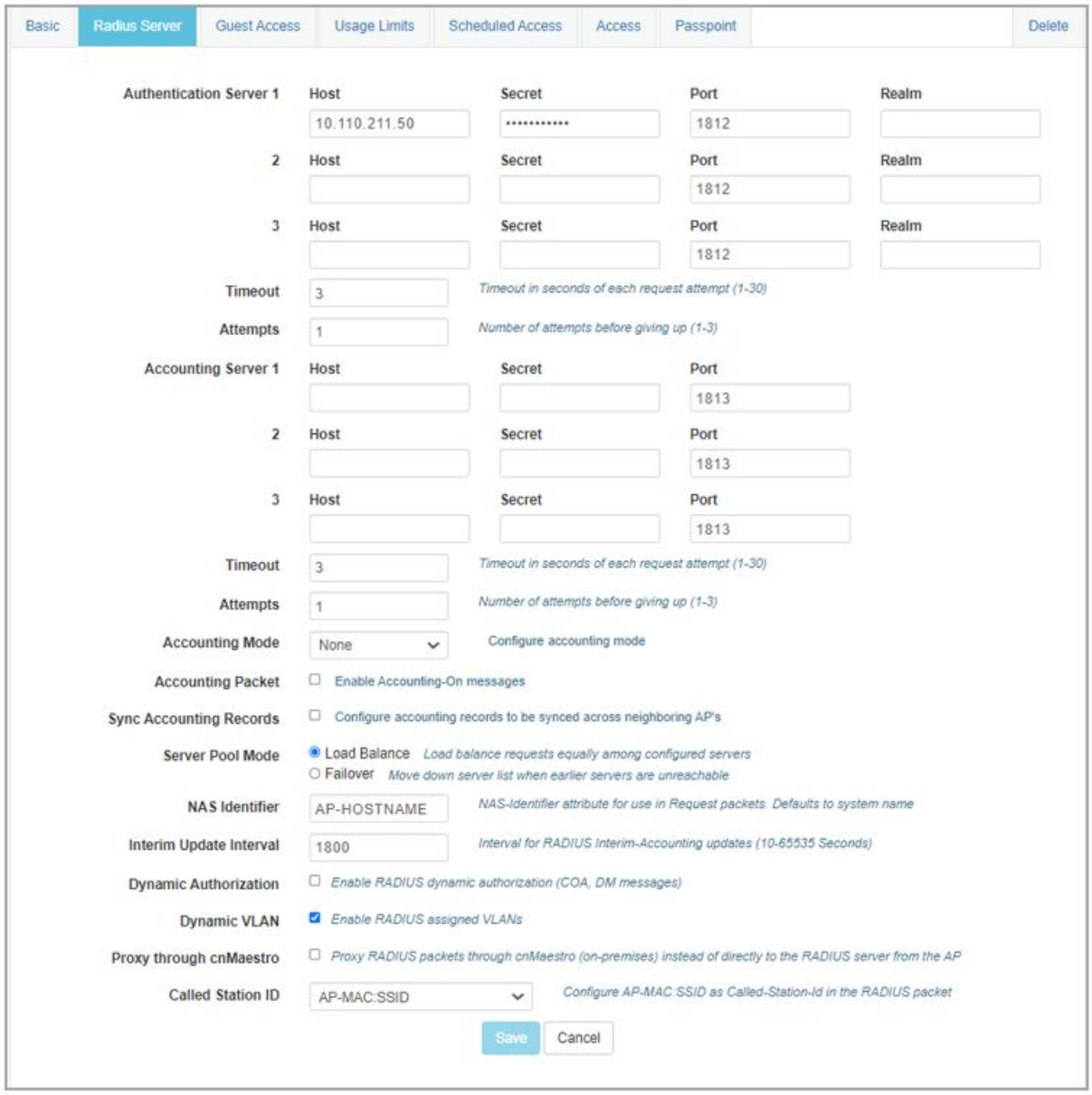
Parameters	Description	Range	Default
	• **Failover**—AP selects the RADIUS server which is up and running based on the order of configuration.		
NAS-Identifier	This is a configurable parameter and is appended in the RADIUS request packet.	-	Hostname/ System Name
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled
Dynamic VLAN	When enabled, AP honors the VLAN information provided in the RADIUS transaction. Wireless station requests IP address from the same VLAN learned through RADIUS.	-	Enabled
Called Station ID	The following information can be communicated to the RADIUS server: • AP-MAC • AP-MAC: SITE-NAME • AP-MAC: SSID • AP-MAC: SSID-SITE-NAME • AP-NAME • AP-NAME: SITE-NAME • AP-NAME: SSID • SITE-NAME • SSID • CUSTOM	-	AP-MAC: SSID

To configure the above parameters, navigate to the **Configure > WLAN** tab, 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 or Realm in the **Authentication Server 1** textbox.
2. Enter the time in seconds of each request attempt in the **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. Enter the **Interim Update Interval** parameter value in the textbox.
9. Enable **Dynamic Authorization** checkbox to configure dynamic authorization for wireless clients.
10. Enable **Dynamic VLAN** checkbox.
11. Enable **Proxy through cnMaestro** checkbox.

12. Select **Called Station ID** from the drop-down list.
13. Click **Save**.

Figure 18: *The Radius Server parameter page*



Proxy Through Controller

cnMaestro On-Premises can act as a proxy server for a AAA request coming from Enterprise Wi-Fi 6 Access Points. In this scenario, cnMaestro acts as Network Access Server (NAS) for the AAA server.

The AP sends AAA packets to cnMaestro On-Premises, and cnMaestro forwards them to the AAA server. When the Proxy Through Controller feature is enabled, CoA is supported other than AAA requests.

CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# radius-server through-controller
```

Note: Applicable only with on-premises controller

For activating Proxy Through Controller feature in cnMaestro On-Premises:

1. Go to **Administration > Settings**.
2. Enable **RADIUS Proxy** checkbox as shown in below figure.

Figure 19: *RADIUS proxy*

EAP-FAST support

EAP-FAST authentication occurs in two phases. In the first phase, EAP-FAST employs the TLS handshake to provide an authenticated key exchange and to establish a protected tunnel. Once the tunnel is established the second phase begins with the peer and server engaging in further conversations to establish the required authentication and authorization policies.

Guest Access

Internal Access Point

Below table lists configurable fields that are displayed in the **Configuration > WLAN > Guest Access > Internal Access Point** page:

Table 27: Internal Access Point parameters

Parameters	Description	Range	Default
WLAN > Guest Access > Internal Access Point			
Enable	Enables the Guest Access feature.	-	Disabled
Access Policy	There are four types of access types provided for the user: 1. Clickthrough This mode allows the users to get access data without any authentication mechanism. User can access the internet as soon as he is connected and accepts Terms and Conditions 2. RADIUS	-	Clickthrough

Parameters	Description	Range	Default
	This mode when selected, the user has to provide a username and password, which is then redirected to the RADIUS server for authentication. If successful, the user is provided with data access. 3. Local Guest Account Users must configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.		
Redirect Mode	This option helps the user to configure the HTTP or HTTPS mode of redirection URL. 1. HTTP AP sends an HTTP POSTURL to the associated client, which will be http://<Pre-defined-URL>. 2. HTTPS AP sends HTTPS POSTURL to the success associated client, which will be https://<Pre-defined-URL>.	-	HTTP
Redirect Hostname	Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.	-	-
Title	Users can configure a Title to the splash page. Configured text in this parameter will be displayed on the redirection page. This text is usually Bold.	Up to 255 characters	Welcome To Cambium Powered Hotspot
Contents	Users can configure the contents of the Splash page using this field. Displays the text configured under the Title section of the redirection page.	Up to 255 characters	Enter username and password to get Web Access
Terms	Splash page displays the text configured when the user accepts the 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 the logo is supported.	-	-

Parameters	Description	Range	Default
Background Image	Displays the background image updated in URL http (s)://<ipaddress>/backgroundimage.png. Either PNG or JPEG format of the logo is supported.	-	-
Success Action	Provision to configure redirection URL after successful login to captive portal services. Users can configure three modes of redirection URL: 1. Internal Logout Page After successful login, the wireless client is redirected to the logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to the URL which is configured on the device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to the URL that is accessed by the user before successful captive portal authentication.	-	Internal Logout page
Redirect user to External URL	Provision to configure re-direction URL after successful login and 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. The following information is appended in the redirection URL: ◦ SSID ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC ◦ Redirection URL ◦ Users can provide either HTTP or HTTPS URL	-	-
Redirection user to Original URL	Users will be redirected to the URL that is accessed by the user before successful captive portal authentication. There are 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. The following information is appended in the redirection URL: ◦ SSID ◦ AP MAC ◦ NAS ID		
Success message	Provision to configure the 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 the Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to the Guest Access login page.	-	Enabled
Redirect User Page	IPv4 address configured in this field is used as logout URL for Guest Access sessions.	-	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	-
Session Timeout	This is the duration of time, the client will be allowed to access the internet if quota persists, after which AP sends de-authentication. The wireless station has to undergo Guest Access authentication after session timeout. **Note** • Following priority takes precedence for the session timeout: a. Configured from the RADIUS server b. Configured from the AP	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.	60 - 2592000	1800

Parameters	Description	Range	Default
	Note • Following priority takes precedence for the inactivity timeout: a. Configured from the RADIUS server b. Configured from the AP		
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to the Guest Access login page after any supported type of MAC address authentication fails.	-	Disabled
Whitelist	Provision to configure either IPv4 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 **Redirect Hostname** in the textbox.
6. Enter the title to appear on the splash page in the **Title** textbox.
7. Enter the content to appear on the splash page in the **Contents** textbox.
8. Enter the terms and conditions to appear in the splash page in the **Terms** textbox.
9. Enter the logo to be displayed in the **Logo** textbox.
10. Select the **Background Image** to be displayed on the splash page in the textbox.
11. Enable configured modes of redirection URL in **Success Action** checkbox.
12. Enter **Success message** to appear in the textbox.
13. Enable **Redirect** checkbox for HTTP packets.
14. Enter configuring IP address in the **Redirect User Page** textbox.
15. Enter Port number in **the Proxy Redirection Port** textbox.
16. Enter the session timeout in seconds in the **Session Timeout** textbox.
17. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.

18. Enable **MAC Authentication Fallback** checkbox if guest-access is used only as a fallback for clients failing MAC-authentication.

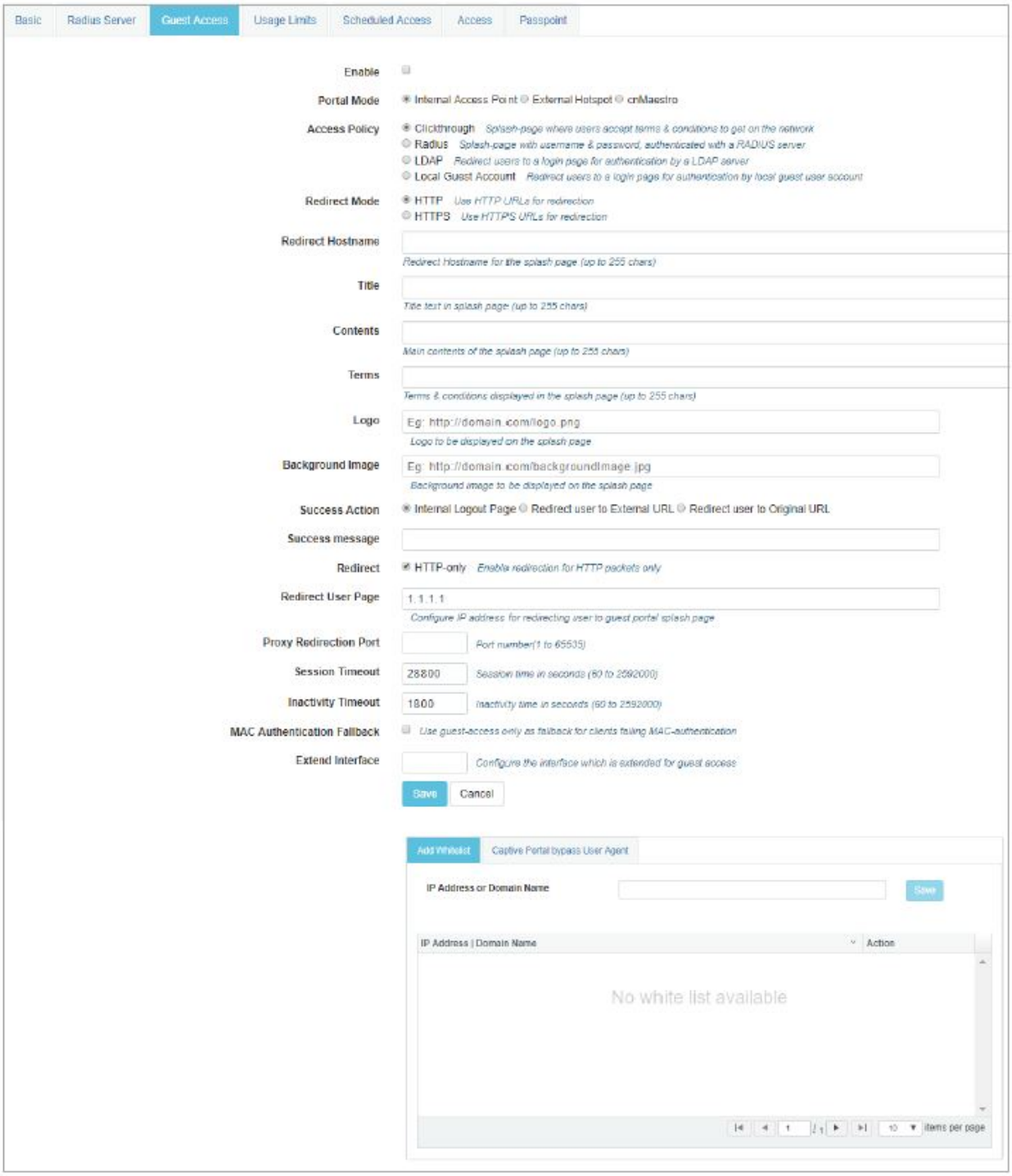
19. Click **Save**.

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 20: *The Internal Access Point parameter*



External Hotspot

Below table lists the configurable fields that are displayed in the **Configuration > WLAN > Guest Access > External Hotspot** tab:

Table 28: 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. The user can access the internet as soon as he is connected and accepts the Terms and Conditions. 2. **RADIUS** The user has to provide a username and password, which is then redirected to a RADIUS server for authentication. If successful, the user is provided with data access. 3. **Local Guest Account** The user has to configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.	–	Clickthrough
Redirect Mode	Provision to configure the HTTP or HTTPS mode of redirection URL. 1. **HTTP** AP sends an HTTP POSTURL to the associated client, which will be http://<Pre-defined-URL>. 2. **HTTPS** AP sends an HTTPS POSTURL to the associated client, which will be https://<Pre-defined-URL>.	–	HTTP

Parameters	Description	Range	Default
Redirect Hostname	Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.	-	-
External Page URL	Users can configure a landing/login page that 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 an external guest access portal. This option when enabled minimizes certification. The certificate is required to install only in cnMaestro On-Premises.	–	Disabled
External Portal Type	Enterprise Wi-Fi AP products are supported by standard mode configuration. • **Standard** This mode is selected, for all third-party vendors whose Guest Access services are 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, the wireless client is redirected to the logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to the URL which is configured on a device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to a URL that is accessed by the user before successful captive portal authentication.	–	Internal Logout Page
Redirect user to External URL	Provision to configure re-direction URL after successful login and 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. The following information is appended in the redirection URL:	–	–

Parameters	Description	Range	Default
	◦ SSID ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC • Redirection URL Users can provide either HTTP or HTTPS URLs.		
Redirection user to Original URL	Users will be redirected to the URL that is accessed by the user before successful captive portal authentication. There are 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. The following information is appended in the redirection URL: ◦ SSID ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC	–	–
Success message	Provision to configure the text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	–	–
Redirection URL Query String	The following information is appended in the redirection URL, if **Prefix Query Strings in Redirect URL** is enabled. • Client IP • RSSI • AP Location	-	Disabled
Redirect	• If enabled, only HTTP URLs will be redirected to the Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to the Guest Access login page.	–	Enabled

Parameters	Description	Range	Default
Redirect User Page	The IP address configured in this field is used as logout/disconnect/redirect to captive portal URL for Guest Access sessions. The IP address configured should not be reachable to the internet.	–	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	–
Session Timeout	This is the duration of time, the client will be allowed to access the internet if quota persists, after which AP sends de-authentication. The wireless station has to undergo Guest Access authentication after session timeout.  **Note** • Following priority takes precedence for the session timeout: a. Configured from the RADIUS server b. Configured from the AP	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.  **Note** • Following priority takes precedence for the inactivity timeout: a. Configured from the RADIUS server b. Configured from the AP	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to the Guest Access login page after any supported type of MAC address authentication failures.	–	Disabled

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. Enter **External Page URL** in the textbox.
5. Enable **External Portal Post Through cnMaestro** checkbox.
6. Select External Portal Type from the drop-down list.
7. Enable configured modes of redirection URL in **Success Action** checkbox.
8. Enter **Success message** to appear in the textbox.
9. Enable the required **Redirection URL Query String** checkbox.
10. Enable **Redirect** checkbox for HTTP packets.
11. Enter configuring IP address in the **Redirect User Page** textbox.
12. Enter Port number in the **Proxy Redirection Port** textbox.
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. Select the **MAC Authentication Fallback** checkbox if guest-access is used only as a fallback for clients failing MAC authentication.
16. Click **Save**.

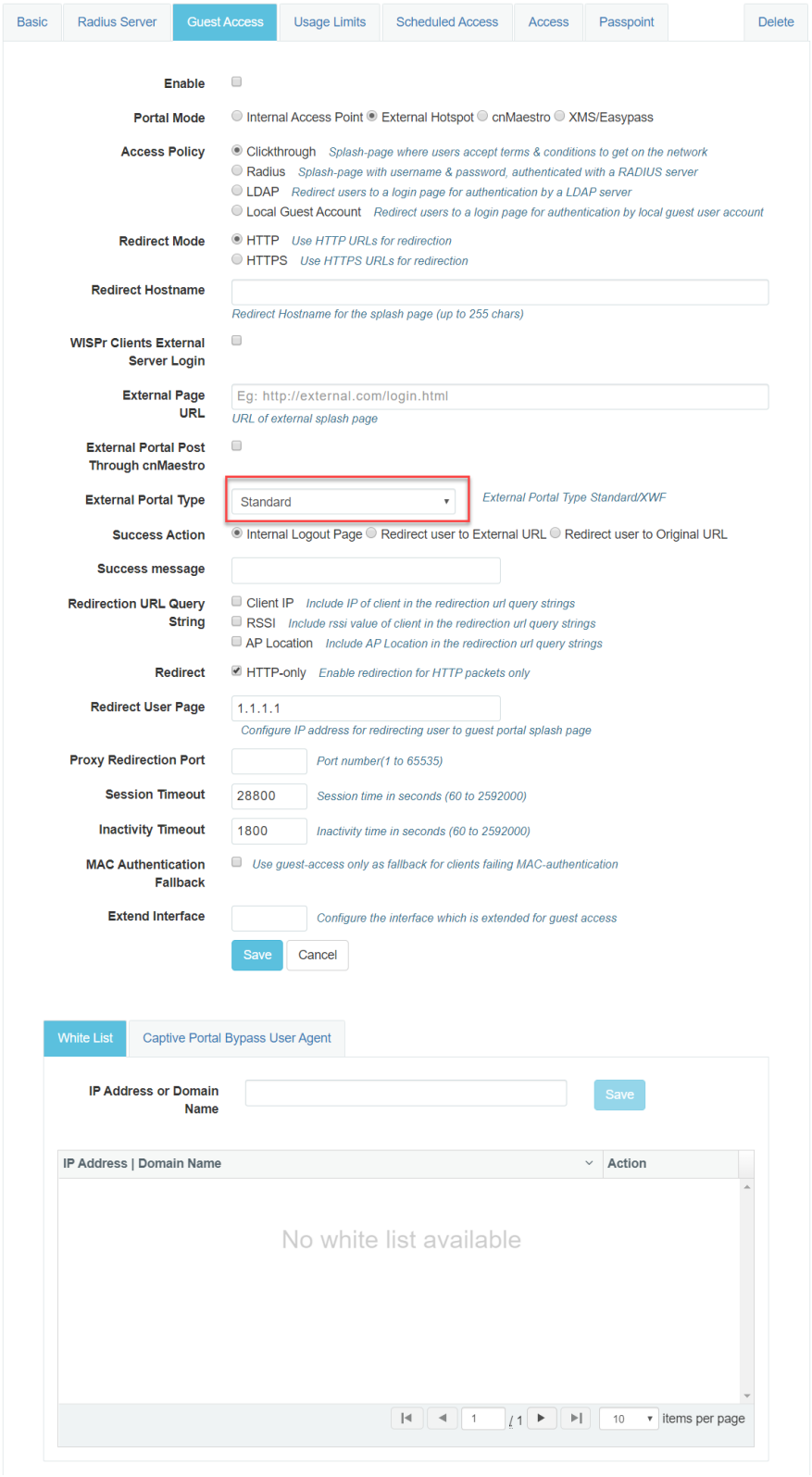
To configure **Whitelist**:

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

To configure **Captive Portal bypass User Agent**:

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

Figure 21: *The External Hotspot (Standard) parameter*



cnMaestro

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

Table 29: The 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 the Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	–	Enabled
Redirect User Page	The IP address configured in this field is used as a logout URL for Guest Access sessions. The IP address configured should be not reachable to the internet.	–	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	–
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero. **Note** • Following priority takes precedence for the inactivity timeout: a. Configured from the RADIUS server b. Configured from the AP	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:

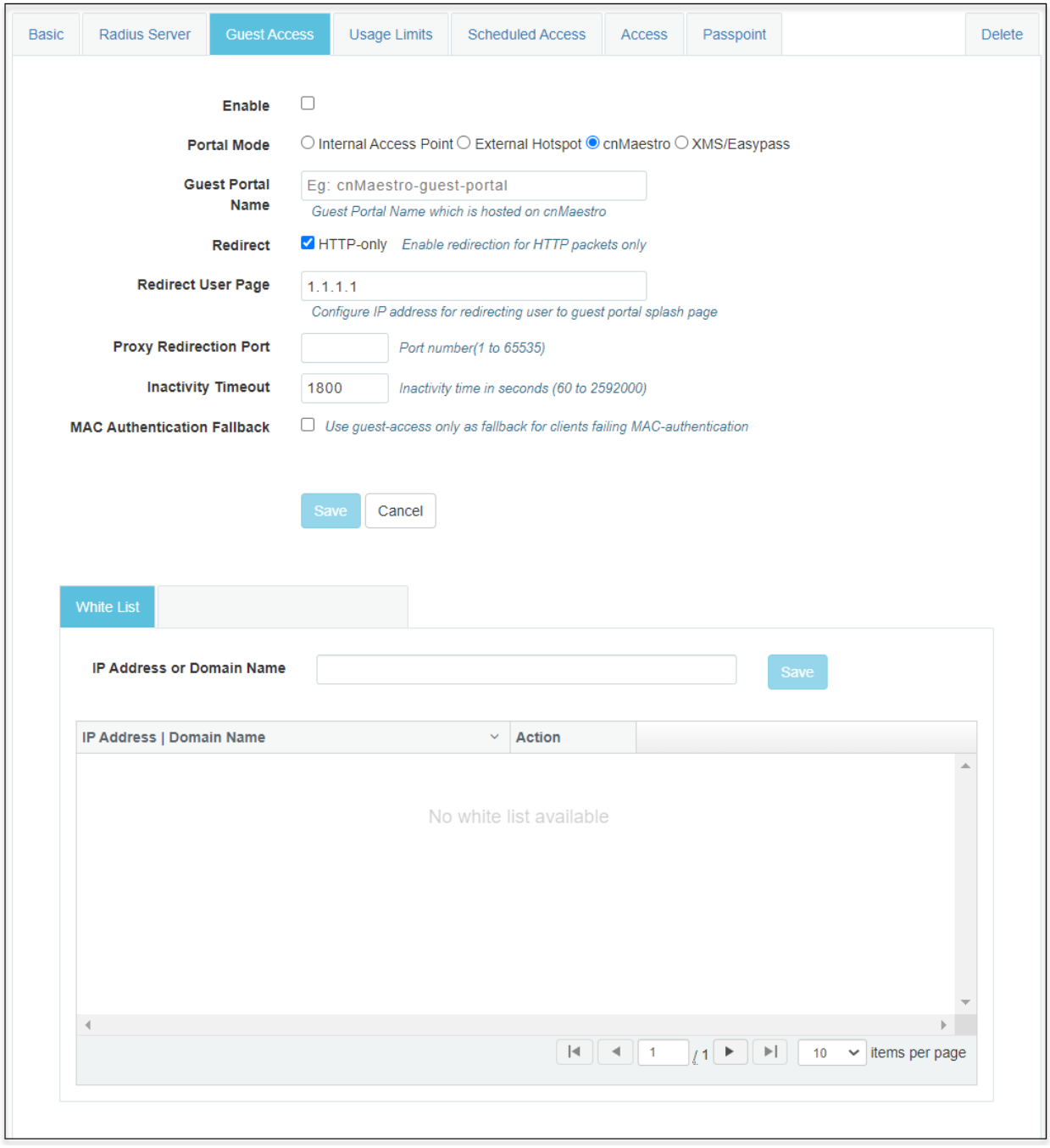
1. Enter **Guest Portal Name** which is hosted on cnMaestro in the textbox.
2. Enable **Redirect** checkbox for HTTP packets.
3. Enter configuring IP address in the **Redirect User Page** textbox.
4. Enter Port number in the **Proxy Redirection Port** textbox.

5. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.
6. 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 22: *The cnMaestro parameter*



XMS/EasyPass

Below table lists configurable fields that are displayed in the **Configuration > WLAN > Guest Access > XMS/EasyPass** tab:

Table 30: XMS/EasyPass parameters

Parameters	Description	Range	Default
External Page URL	Users can configure a login page that is posted to wireless stations that are not Guest Access authenticated.	–	–
Secret	Provision to configure the secret to be used during redirection.	–	–
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	–	–

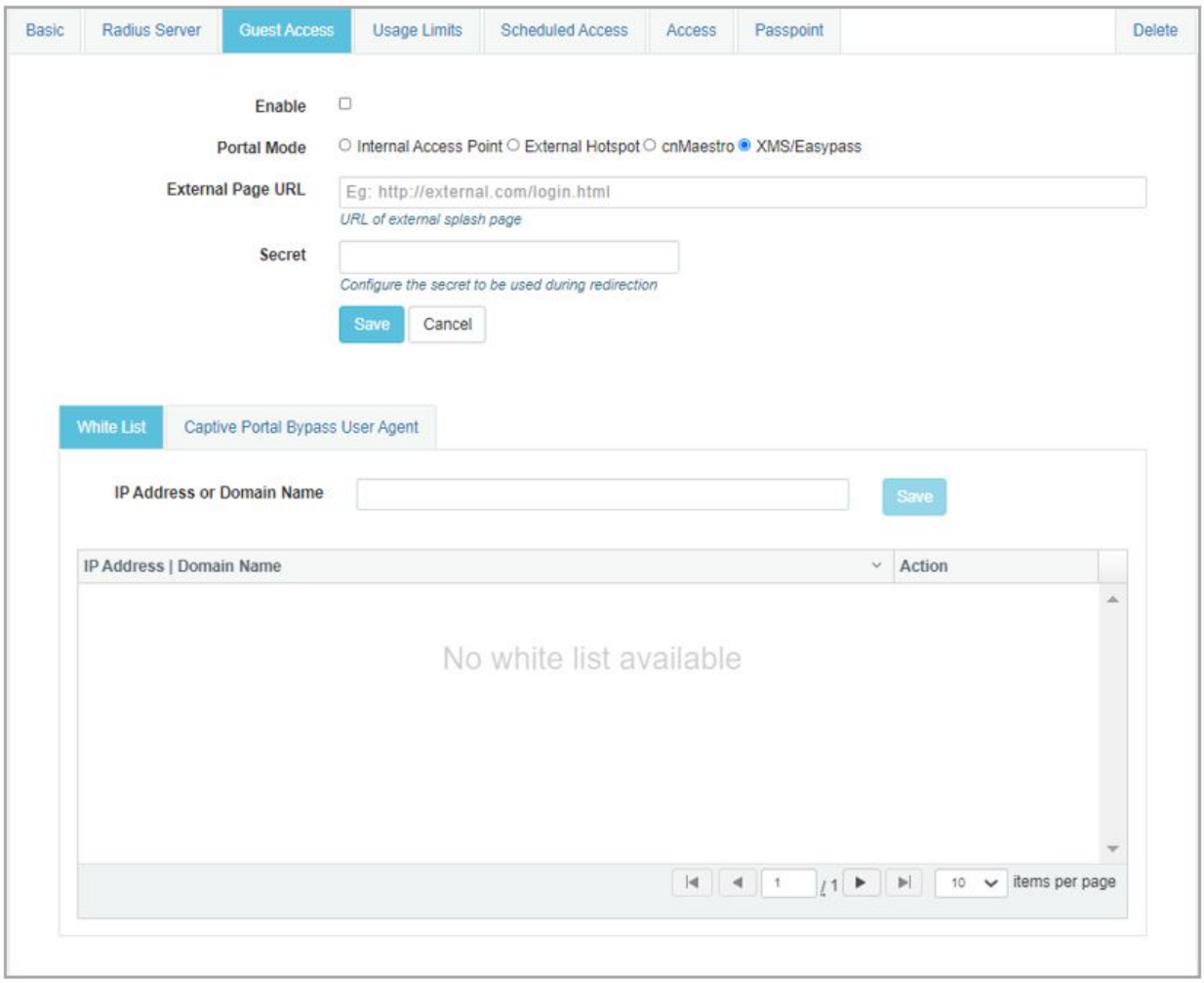
To configure the above parameters, navigate to the **Configure > WLAN > XMS/EasyPass** tab and provide the details as given below:

1. Enter **External Page** URL in the textbox.
2. Enter **Secre**t to be used during redirection in the textbox.
3. 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 23: *XMS/EasyPass*



Note

- For more information about XMS-Cloud EasyPass settings and onboarding, refer to the latest *XMS-Cloud Help* document.
- For more information about cnMaestro Guest Access Portal and onboarding, refer to the *cnMaestro User Guide*.

Usage Limits

Below table lists configurable fields that are displayed in the **Configuration > WLAN > Usage Limits** tab:

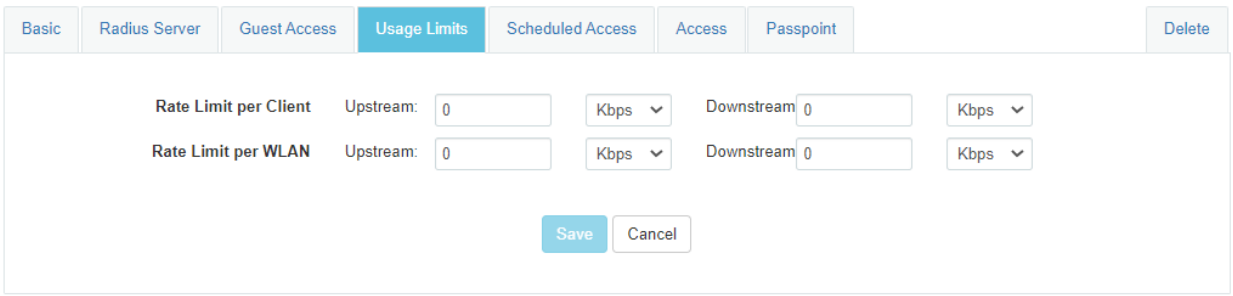
Table 31: Usage Limits parameters

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 an SSID can be rate-limited in either direction by configuring the 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 a 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** text box.
2. Enter Upstream and Downstream parameters in the **Rate Limit per WLAN** text box.
3. Click **Save**.

Figure 24: *The Usage Limits parameters*



Scheduled Access

Below table lists configurable fields that are displayed in the **Configuration > WLAN >Scheduled Access** page:

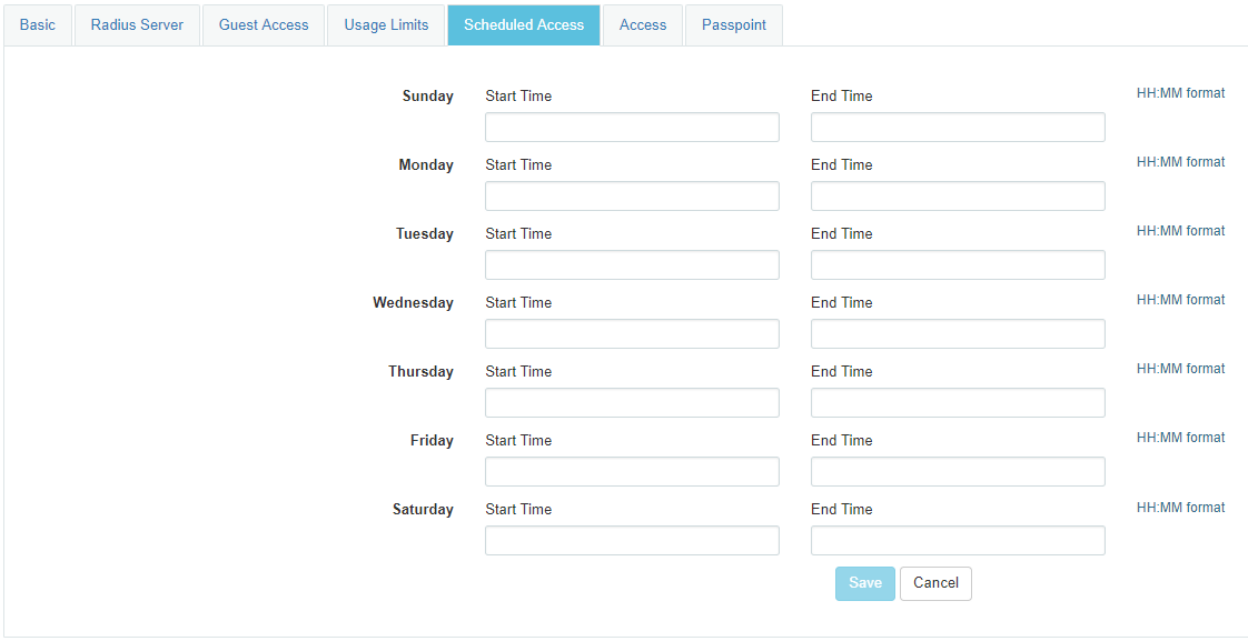
Table 32: The Scheduled Access parameters

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 the capability of configuring the availability of Wi-Fi services on all days or a specific day (s) of a week. The time format is in Hours. **Note** From Release 6.3 onwards, the user can configure up to a maximum of twelve schedule access rules per day on a particular WLAN instead of 1 rule per day.	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 Wi-Fi access in the respective text boxes.
2. Click **Save**.

Figure 25: *The Scheduled Access parameters*



CLI Configuration:

```
XV3-8-EC7708(config)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# scheduled-access
all : all
friday : friday
monday : monday
saturday : saturday
sunday : sunday
thursday : thursday
tuesday : tuesday
wednesday : wednesday
weekday : weekday
weekend : weekend
XV3-8-EC7708(config-wlan-1)# scheduled-access all
Time period in HH:MM-HH:MM,HH:MM-HH:MM format
```

Access

Below table lists configurable fields that are displayed in the **Configuration > WLAN > Access** tab:

Table 33: The Access parameters

Parameters	Description	Range	Default
DNS-ACL			
Precedence	Provision to configure index of ACL rule. Packets are validated and processed based on the Precedence value configured.	-	1
Action	Provision to configure whether to allow or deny traffic.	-	Deny
Domain	Provision to configure domain names and rules are applied based on Action configured.	-	-
MAC Authentication			
MAC Authentication Policy	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 the user configures a MAC address, those wireless stations shall be denied to associate and the non-listed MAC address will be allowed.	-	Deny

Parameters	Description	Range	Default
	3. Radius For every wireless authentication, AP sends a RADIUS request and if RADIUS acceptance is received, then the wireless station is allowed to associate. 4. cnMaestro This option is preferable when the administrator prefers a centralized MAC authentication policy. For every wireless authentication, AP a sends query to cnMaestro if it is allowed or disallowed to connect. Based on the configuration, wireless stations are either allowed or denied.		

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

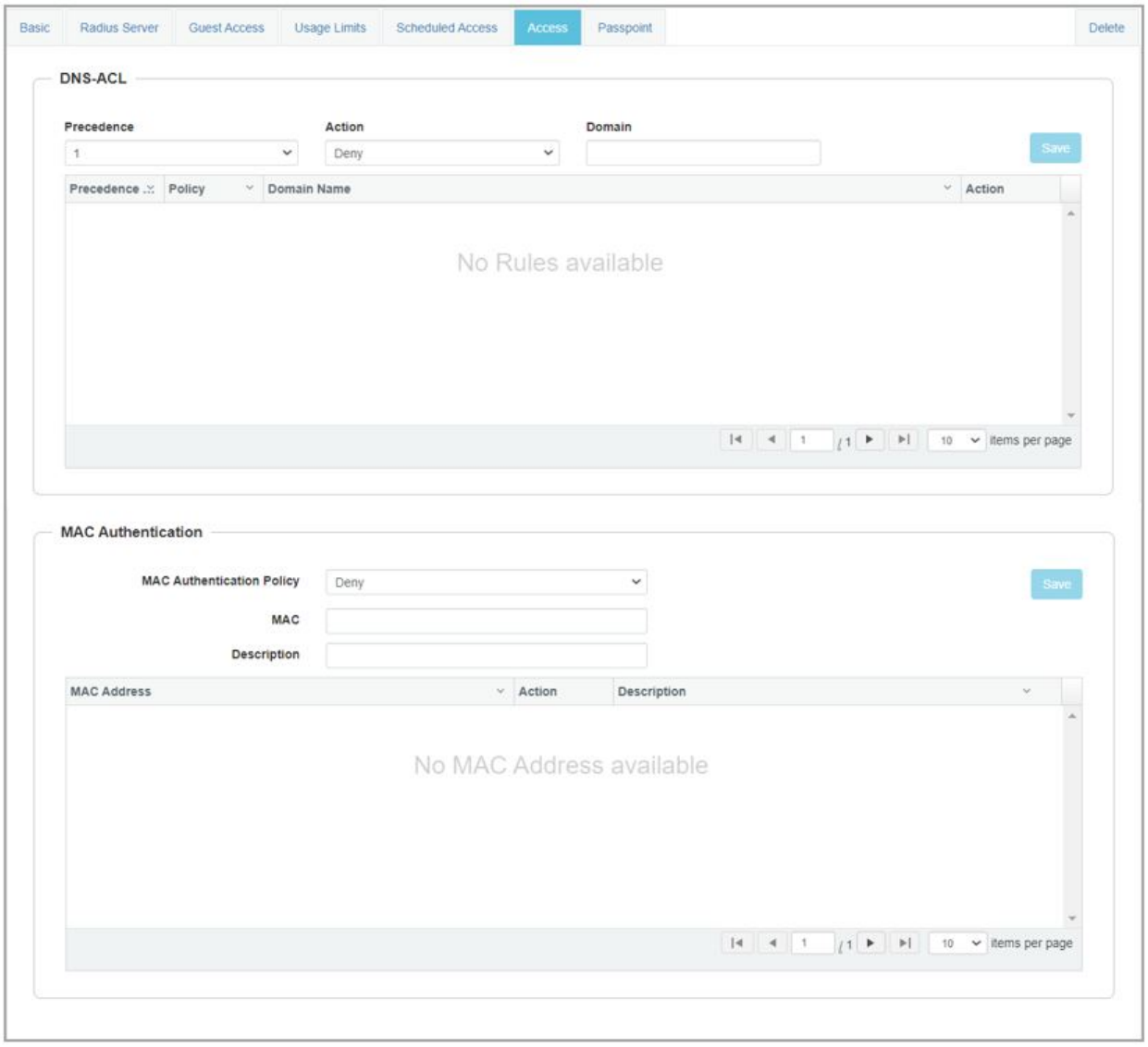
To configure **DNS ACL**:

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

To configure **MAC Authentication**:

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

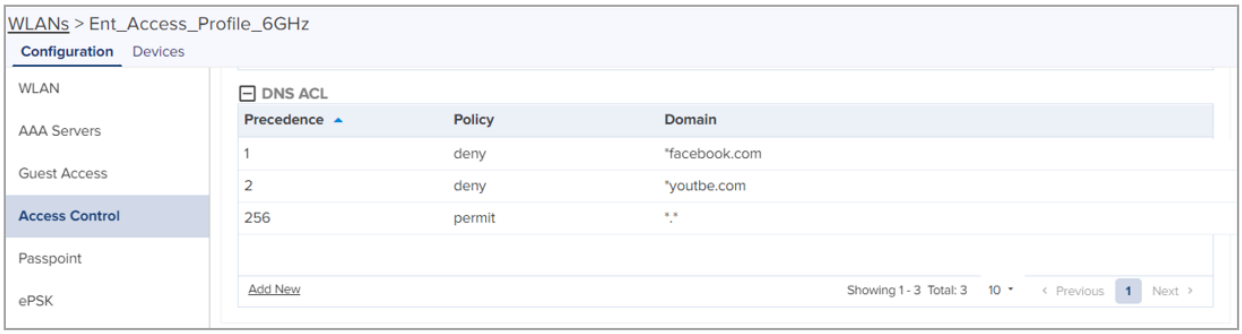
Figure 26: *The Access parameters*



Sample DNS-ACL configuration

If any user wants to block Facebook or Youtube traffic and allow the rest of the traffic, the configuration is shown in below figure:

Figure 27: *Sample DNS-ACL configuration*



Passpoint

Below table lists configurable fields that are displayed in the **Configuration > WLAN > Passpoint** tab:

Table 34: Passpoint parameters

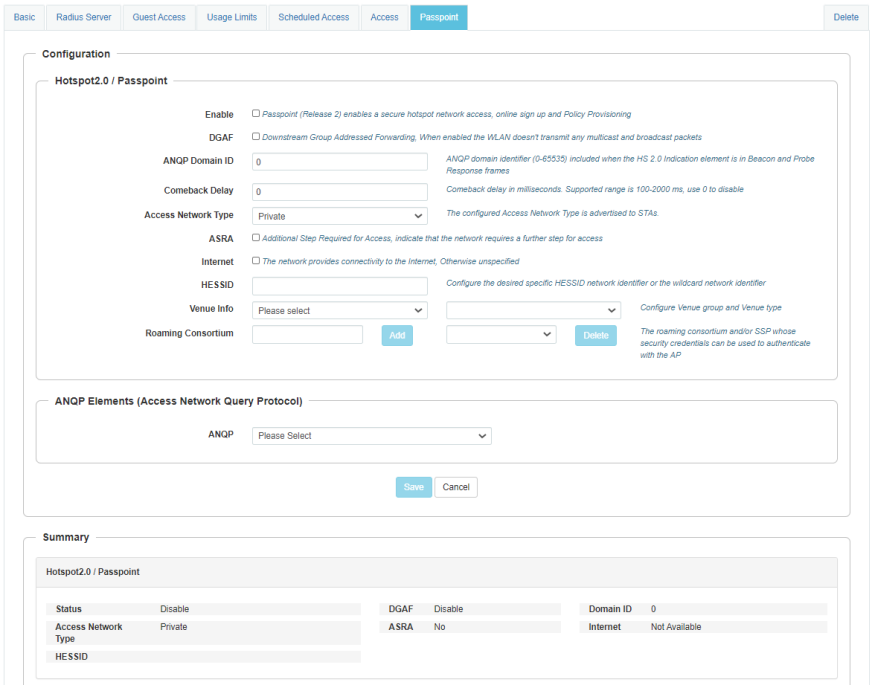
Parameters	Description	Range	Default
Configuration > Hotspot2.0 / Passpoint			
Enable	Passpoint (Release 2) enables secure hotspot network access, online sign-up, and policy provisioning.	–	Disabled
DGAF	Downstream Group Addressed Forwarding when enabled the WLAN does not transmit any multicast and broadcast packets.	–	Disabled
ANQP Domain ID	ANQP domain identifier is included when the HS 2.0 indication element is in Beacon and Probe Response frames.	0-65535	0
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with Guest • Test • Wildcard	–	Private
ASRA	This 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.	–	–

Parameters	Description	Range	Default
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 the **DGAF** checkbox to enable Downstream Group Addressed Forwarding functionality.
3. Enter the domain identifier value in the **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 the **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 28: *The Passpoint parameters*



Radius attributes

The table below shows the attributes processed by the CaOS and describes their interpretation.

Table 35: Radius attributes parameters

Type	Attribute Name	Attribute Number	Purpose
Standard	Acct-Interim-Interval	85	Specifies the interval between accounting interim updates
Standard	Acct-Session-Id	44	Session identification (RFC 5176)
Standard	Calling-Station-Id	31	Session identification (RFC 5176)
Standard	Class	25	Accounting classification
Standard	Event-Timestamp	55	Replay protection (RFC 5176)
Standard	Filter-ID	11	• Assign station to a user group • Re-assign station to a different user group (RFC 5176)
Standard	Framed-IP-Address	8	Session identification (RFC 5176)
Standard	Idle-Timeout	28	Specifies the amount of time a station may remain idle

Type	Attribute Name	Attribute Number	Purpose
			before its session is terminated
Standard	NAS-IP-Address	4	NAS identification (RFC 5176)
Standard	NAS-Identifier	32	NAS identification (RFC 5176)
Standard	Session-Timeout	27	Specifies the interval at which session is terminated
Standard	Termination-Action	29	Specifies the action to take when the session is terminated
Standard	Tunnel-Type	64	Dynamic VLAN assignment (1 of 3 required), should be set to VLAN (Integer = 13)
Standard	Tunnel-Medium-Type	65	Dynamic VLAN assignment (2 of 3 required), should be set to 802 (Integer = 6)
Standard	Tunnel-Private-Group-ID	81	Dynamic VLAN assignment (3 of 3 required), should be set to the VLAN ID or name
Standard	User-Name	1	• Station username update • Session identification (RFC 5176)
Microsoft Vendor-Specific	MS-MPPE-Send-Key	16	Session key distribution
Microsoft Vendor-Specific	MS-MPPE-Recv-Key	17	Session key distribution
Cambium Vendor-Specific	Cambium-Vlan-Pool-Id	157	Radius based VLAN pool
Nas Port ID	NAS-Port-Id	87	NAS identification (RFC 5176)

Enterprise PSK (ePSK)

By using the ePSK feature, users can configure and support individual PSKs for different clients. This feature can be configured under a given WLAN configuration in cnMaestro UI. For on devices, only CLI support is available.

This feature also supports individual VLAN assignments for a given key which helps to put client traffic on different VLANs for limiting broadcast traffic.

Note:

- Maximum key limit for cnMaestro Essentials: 300 per account
- Maximum key limit for cnMaestro X: 2000 per WLAN and 50000 per account

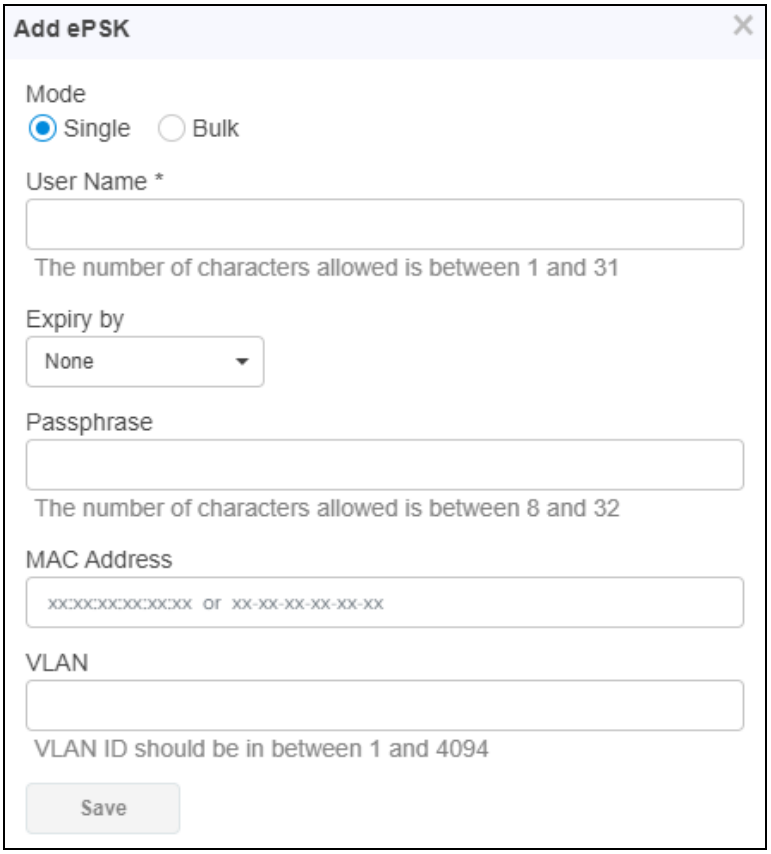
Configuring ePSKs

To create an ePSK, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles**.
2. Select **WLAN** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and enter details in the **Basic Information** section.
4. In the **Basic Settings** section, ensure the **WPA2 Pre-Shared Keys** option is selected in the **Security** drop-down list.
5. Click **Save**.
6. Click the **ePSK** tab and select the **Local** option in the **Mode** field.
7. Select the type of **Passphrase Strength** as one of the following options:
    - **Easy**—Supports a maximum of eight alphanumeric characters
    - **Strong**—Supports a maximum of 16 alphanumeric and special characters
    - **Number**—Supports a maximum of eight integers
8. Click **Add New**.

    The **Add ePSK** window is displayed.
9. Select **Mode** type as one of the following options and configure the corresponding parameters:

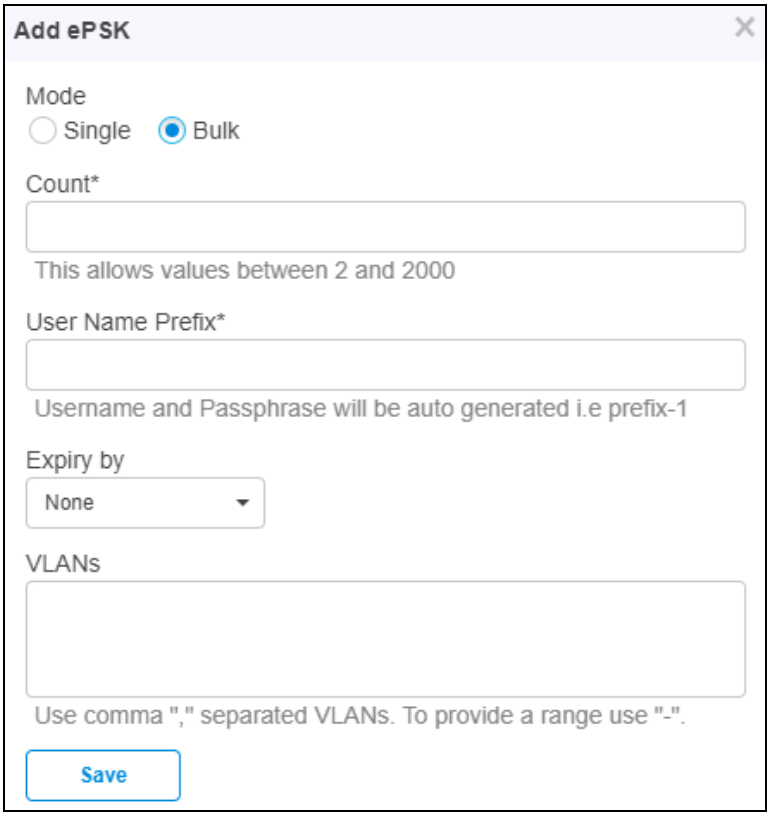
- **Single** mode—Only one entry is created in this mode

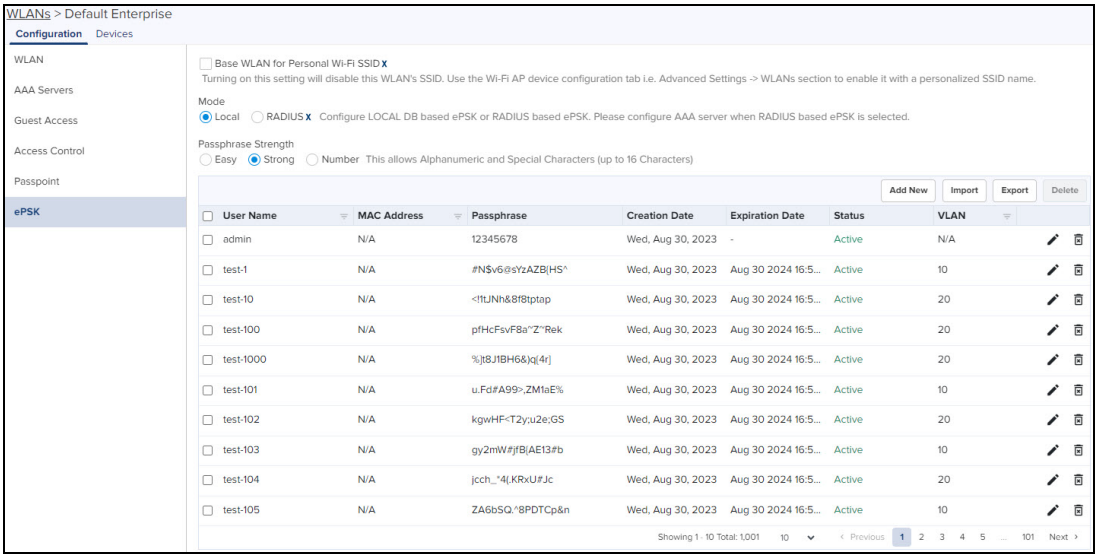


Note:

The **Passphrase** field is optional and is automatically generated based on the selected **Passphrase Strength**.

- **Bulk** mode—Multiple entries are created in this mode depending on the count configured





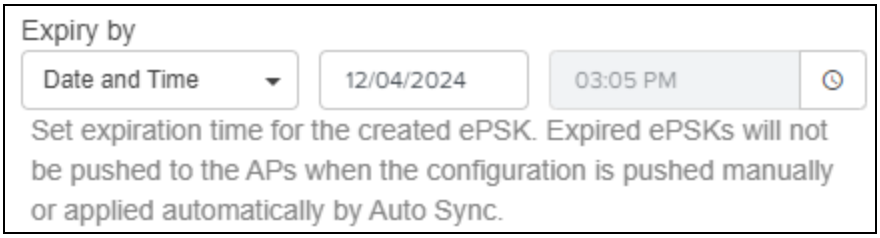
10. To automatically expire ePSK details after a specific duration. The following options are available:

Note:

This feature is available from cnMaestro 4.1.0 and later versions only.

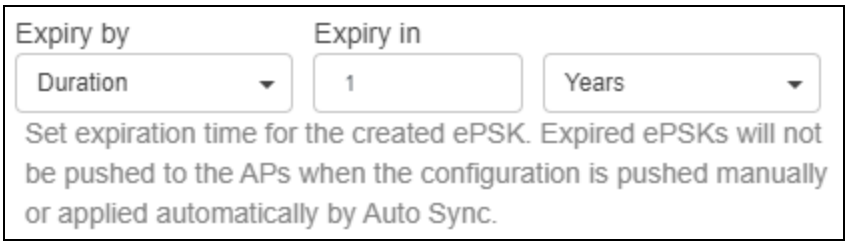
- **None**—ePSK details never expire. Select **None** to never expire the ePSK credentials.
- **Date and Time**— ePSK expires after the specified date and time (in dd/mm/yyyy hh:mm AM/PM format)

  Supported minimum time is 12 A.M. on the next day and the maximum is five years.



- **Duration**— ePSK expires after the specified (in hours, days, months, or years) in the **Expiry by** drop-down.

  Supported minimum duration is one hour and the maximum is five years. No decimal values are supported, for example, 1.5 hours.



- The configured expiry time appears in the **Expiration Date** column on the **WLANs** > <*WLAN name*> page.
- The **Status** column on the **WLANs** > <*WLAN name*> page displays the status of the ePSK details—**Active**, **Expired**, or **None**. **None** is displayed only when older ePSK keys are imported to cnMaestro.
- Expired ePSK details are deleted from the AP only when the next configuration sync functionality is initiated or when there is a configuration change in the AP.

Creating a Personal Wi-Fi ePSK

Note:

This feature is available from cnMaestro 4.1.0 and later versions only.

In Multiple Dwelling Units (MDU), personal Wi-Fi allows a user to connect all the personal devices to a unique SSID associated with a VLAN.

To configure personal W-Fi on the AP, complete the following steps in the cnMaestro UI:

1. Add and enable the SSID details (to be used as personal Wi-Fi) in the **WLANs** tab, under **Manage and Operation** > **Networks** > *<network name>* > **Configuration** > **Device Configuration** > **Advanced**

Settings section.

a. Select the **Enable SSID** checkbox.

b. In the **Passphrase** field, configure the passphrase.

c. Configure the VLAN with which the SSID must be associated.

2. Enable personal Wi-Fi on the ePSK page for the WLAN profile by selecting the **Base Personal SSID** checkbox.

   By default, this feature is disabled. Once enabled, the **Enable** checkbox (under **WLANs** > **WLAN** > **Basic Settings** > **SSID**) is cleared. Also, the local and RADIUS ePSKs are disabled.

For more information on configuring personal Wi-Fi, refer to the *cnMaestro User Guide*.

RADIUS-based ePSK Premium feature

Cambium Networks ePSK feature is an extension of WPA2 PSK where multiple passphrases can be assigned to a single SSID. The Wi-Fi clients can have unique passphrases that can be used by each client using this feature. The same feature has been now extended to RADIUS.

The RADIUS server can provide the matching PMK for a given client, and corresponding standard RADIUS attributes can be enforced for a client session. This requires custom development on the RADIUS server.

Note:

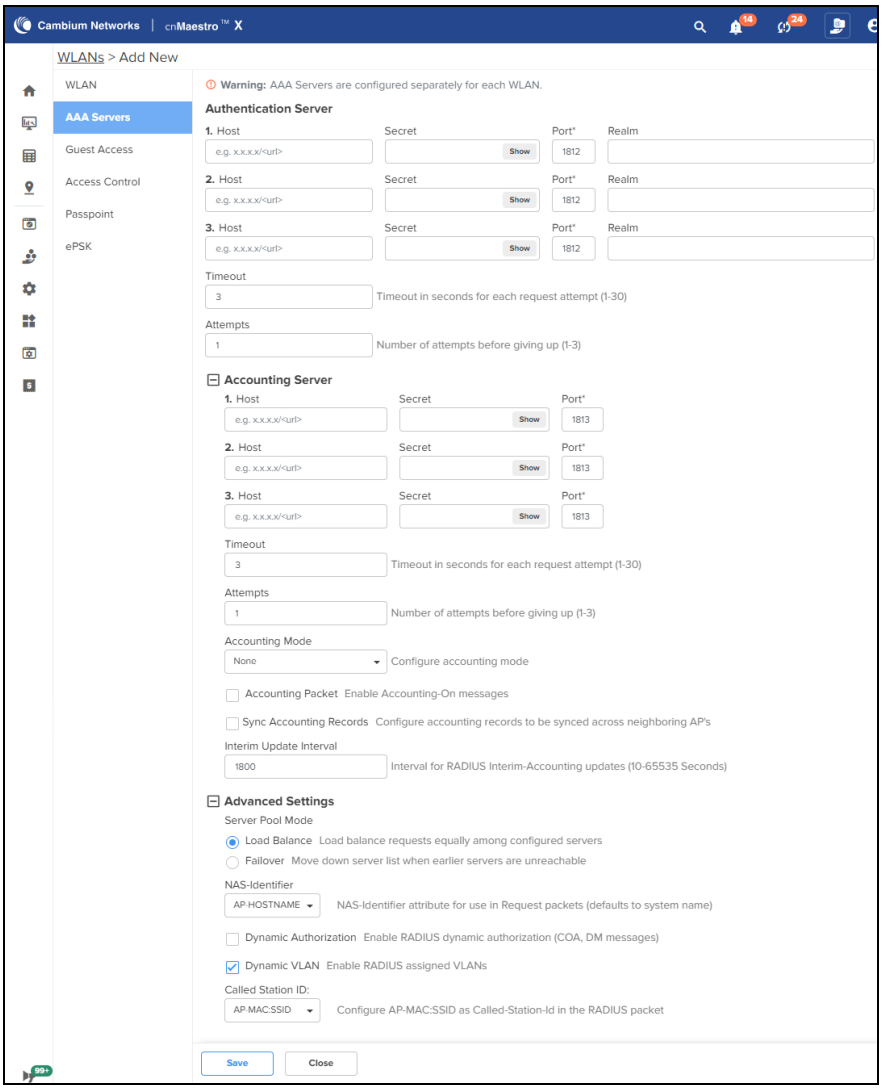
ePSK feature is not supported with WPA3.

Configuring RADIUS-based ePSK

To configure RADIUS-based ePSK, complete the following steps:

1. Navigate to **Configuration** > **Wi-Fi Profiles**.
2. Select **WLAN** tab and click **Add**.
3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and enter details in the **Basic Information** section.
4. In the **Basic Settings** section, ensure the **WPA2 Pre-Shared Keys** option is selected in the **Security** drop-down list.
5. Click **Save**.
6. Click the **ePSK** tab and select the **RADIUS**^{X} option in the **Mode** field.

You must configure AAA servers when configuring RADIUS-based ePSK. See *cnMaestro User Guide* for information on configuring AAA servers.

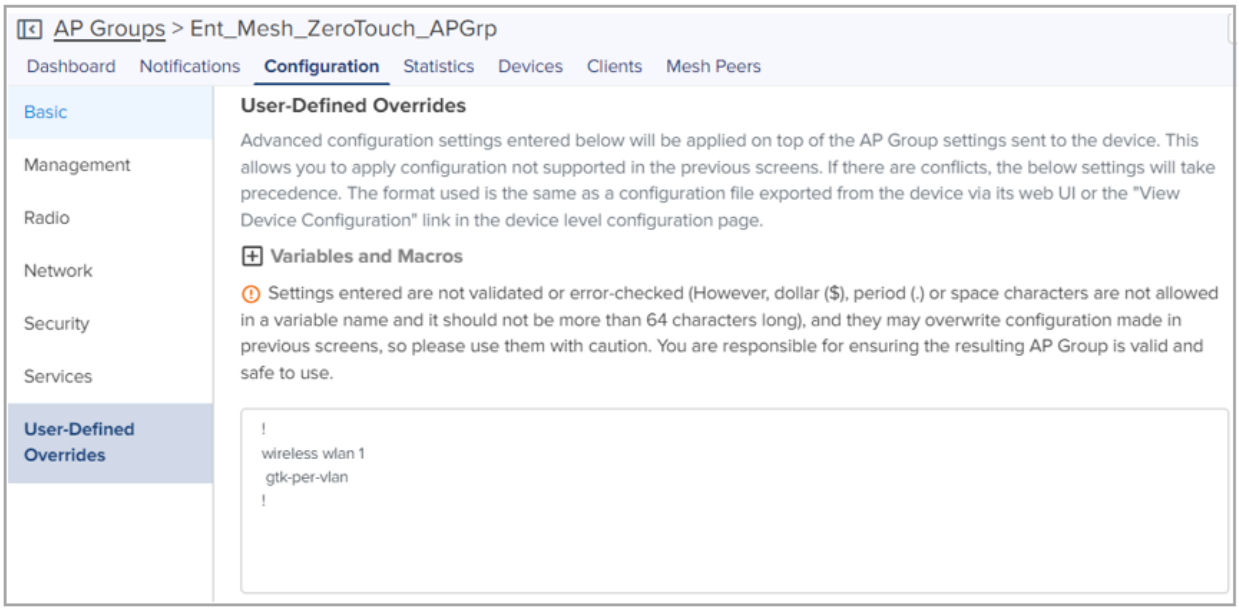

Cambium Networks | cnMaestro™ X
WLANs > Add New
WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK
Warning: AAA Servers are configured separately for each WLAN.
Authentication Server
1. Host
Secret
Port*
Realm
e.g. x.x.x.x/<url>
Show
1812
2. Host
3. Host
Timeout
3
Timeout in seconds for each request attempt (1-30)
Attempts
1
Number of attempts before giving up (1-3)
Accounting Server
1813
Interim Update Interval
1800
Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)
Advanced Settings
Server Pool Mode
Load Balance Load balance requests equally among configured servers
Failover Move down server list when earlier servers are unreachable
NAS-Identifier
AP-HOSTNAME
NAS-Identifier attribute for use in Request packets (defaults to system name)
Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)
Dynamic VLAN Enable RADIUS assigned VLANs
Called Station ID:
AP-MAC:SSID
Configure AP-MAC:SSID as Called-Station-Id in the RADIUS packet
Save
Close

Groupwise Transient Key (GTK) per VLAN

The APs support dynamic VLAN via ePSK/RADIUS based/VLAN-pool feature on a given WLAN profile. The client traffic is tagged as per the VLAN assigned dynamically. The unicast traffic works fine as each client generates a unique PTK. However, the AP provides common GTK for all the clients associated with the WLAN profile irrespective of the VLAN that belongs to. This causes all clients irrespective of the VLAN assigned can receive broadcast/multicast data traffic of other VLAN traffic.

The solution is to generate the GTK per VLAN and forward it to clients as part of the WPA2 handshake. So that the broadcast/multicast data traffic is encrypted using GTK based on the VLAN tag of the packet. The maximum number of GTKs supported is 127 per radio. By default it is disabled.

cnMaestro configuration:



Configuration CLI:

```
XV3-8-EC7708(config)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# gtk-per-vlan
```

Chapter 7: Configuring the Network

This chapter describes the following topics

Overview

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

Configuring Network parameters

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

- VLAN
- Routes
- Ethernet Ports
  - Port Control—802.1X Authentication
- Security
- DHCP
- Tunnel
- PPPoE
- VLAN Pool

IPv4 network parameters

VLAN

Below table lists the fields that are displayed in **Configure > Network > VLAN** tab:

Table 36: VLAN (IPv4) parameters

Parameters	Description	Range	Default
VLAN > IPv4			
Edit	Provision to select the VLAN interface that the user is intended to view/update the configuration.	–	VLAN 1
Address	Provision to configure the mode of IPv4 address configuration for an interface selected. Two modes are supported: • **DHCP**—This is the default mode in which the Enterprise Wi-Fi AP device tries to obtain an IPv4 address from the DHCP server. • **Static IP**—Users must explicitly configure the IPv4 address and Netmask for a VLAN selected.	–	DHCP

Parameters	Description	Range	Default
NAT	This option enables wireless traffic gets NAT'ed with APs respective uplink interface IP. This option is recommended when DHCP pools are configured in AP.	–	Disabled
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only in the 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 the DHCP IP. Enabling this appends Option 82 in the DHCP packets. Following information is allowed to configure: • **DHCP Option 82 Circuit ID** Configurable parameters under this option are as follows: ◦ Hostname ◦ APMAC ◦ BSSID ◦ SSID ◦ Custom • **DHCP Option 82 Remote ID** Configurable parameters under this option are as follows: ◦ Hostname ◦ APMAC ◦ BSSID ◦ SSID ◦ Custom **Note** In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered: 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration	–	Disabled
Request Option All	This configuration decides the interface on which Enterprise Wi-Fi AP will learn the following: • IPv4 default gateway	–	Enabled on VLAN1

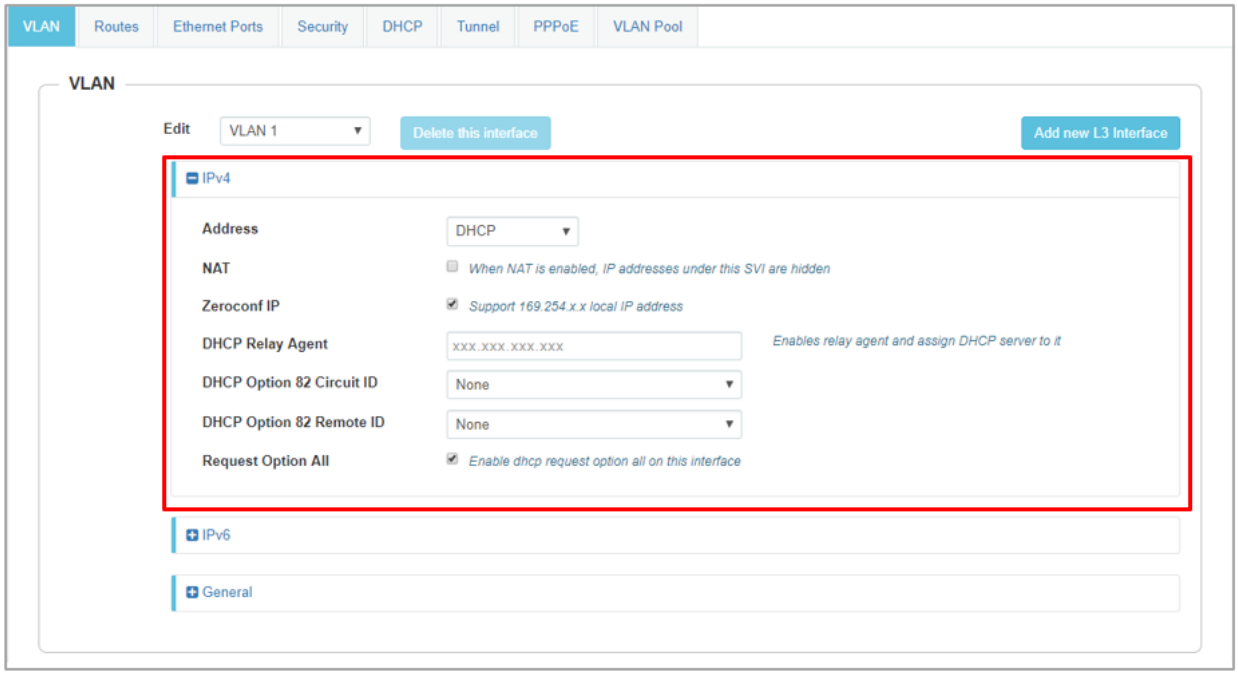
Parameters	Description	Range	Default
	• DHCP client options like Option 43 and Option 15 (Controller discovery like controller host name / IPv4 address) • DNS Servers • Domain Name		

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

To configure VLAN IPv4:

1. Select **Edit** check box to enable VLAN1 functionality.
2. Enable **DHCP** or **Static IP** mode of IPv4 address configuration from the **Address** check box.
3. Enable **NAT** check box.
4. Enable **Zeroconf IP** check box.
5. Enter **DHCP Relay Agent** parameter in the text box.
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** check box.
9. Click **Save**.

Figure 29: *Network (IPv4) parameters*



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. The below table lists the different DHCP options.

Table 37: 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 the state of "Request Option All", the device chooses a subnet mask from the 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 the state of "Request Option All", the device chooses a route learned from the respective VLAN interface. The 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 the state of "Request Option All", the device chooses a subnet mask from the respective VLAN interface. the top two DNS servers are honored by Enterprise Wi-Fi AP devices.	`show ip name-server`
Option 15	This option specifies the domain name that the 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 Configuring the Network.	`show ip dhcp-client info`
Option 28	This option specifies the broadcast address that the client should use.	A broadcast address learned 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 the cnMaestro IP address from the DHCP server while a 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 the DHCP server.	`show ip dhcp-client info`

Options	Description	Usage	Reference CLI
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`

DHCP Option 43—Zero-touch onboarding

This option is used to help the AP in obtaining cnMaestro/XMS IP address from the DHCP server while a DHCP request to get an IP address is sent to the DHCP server.

With Release 6.4, this option is used to learn HTTPS Proxy server address from the DHCP server as well.

DHCP Option 43 format

From Release 6.4 onwards, a new way of Option 43 format is supported. If HTTP proxy needs to be configured then the following format should be used:

The cnMaestro/XMS URL and HTTPS proxy URL can be packed into Option 43 payload in a key-value pair separated by ',' like <key=value,key=value>. Key and its value are separated by '=' character.

For example, 0=CMBM;1=cloud.cambiumnetworks.com;2=http://user:userpass@IP/URL:port, where identifiers are listed below:

- 0 is for header CMBM - **Mandatory**
- 1 is for the server's URL
- 2 is for HTTP proxy URL

Note

If only cnMaestro/XMS URL configuration is needed then Option 43 payload can contain only that too without key-value format as described above.

Routing and DNS

Table 38: Configure: Network > VLAN > Routing & DNS > IPv4 parameters

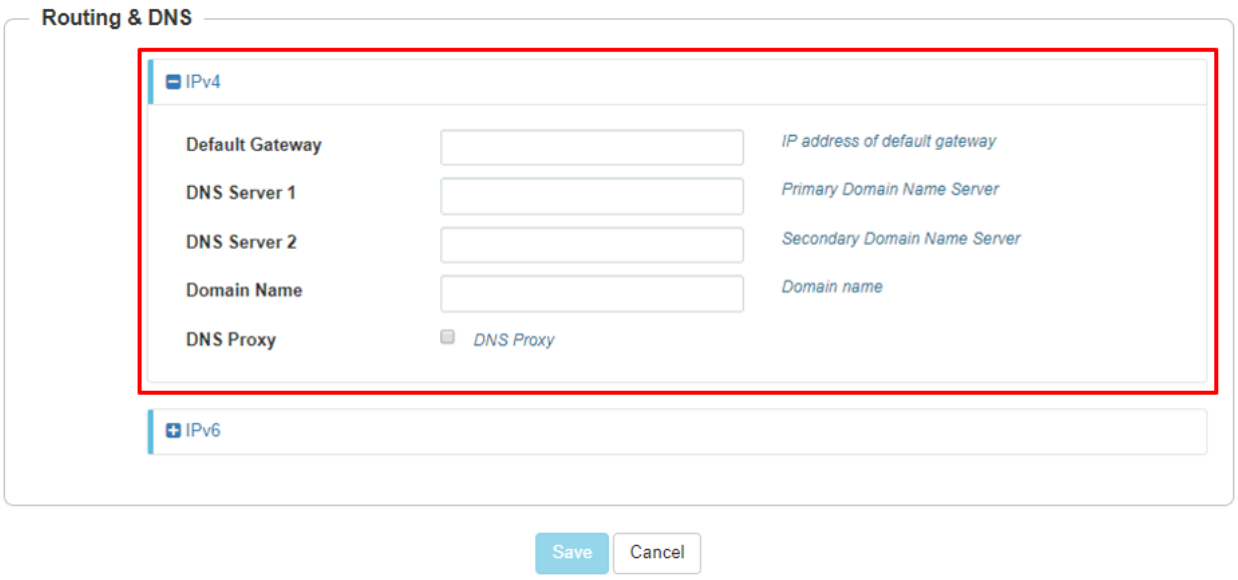
Parameters	Description	Range	Default
Default Gateway	Provision to configure the default gateway. If this is provided, Enterprise Wi-Fi AP device installs this gateway as this is the highest priority.	–	–
DNS Server	Provision to configure Static DNS server on Enterprise Wi-Fi AP device. A maximum of two DNS servers can be configured.	–	–

Parameters	Description	Range	Default
Domain Name	Provision to configure Domain Name. If this is provided, Enterprise Wi-Fi AP device installs this Domain Name as this is the 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 text box.
2. Enter **Domain** Name in the text box.
3. Enter primary domain server name in the **DNS Server 1** text box.
4. Enter secondary domain server name in the **DNS Server 2** text box.
5. Enable **DNS Proxy** check box.
6. Click **Save.**

Figure 30: *Routing & DNS (IPv4) parameters*



Routes

Below table lists the fields that are displayed in **Configure > Network > Routes** tab:

Table 39: 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 learned from multiple ways. Default order is Static and DHCP.	–	Static
Add Multiple Route Entries	The 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. Users can access the services hosted on wireless stations using this feature. Following configurable parameters are required to gain access to 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** check box.
2. Click **Save**.

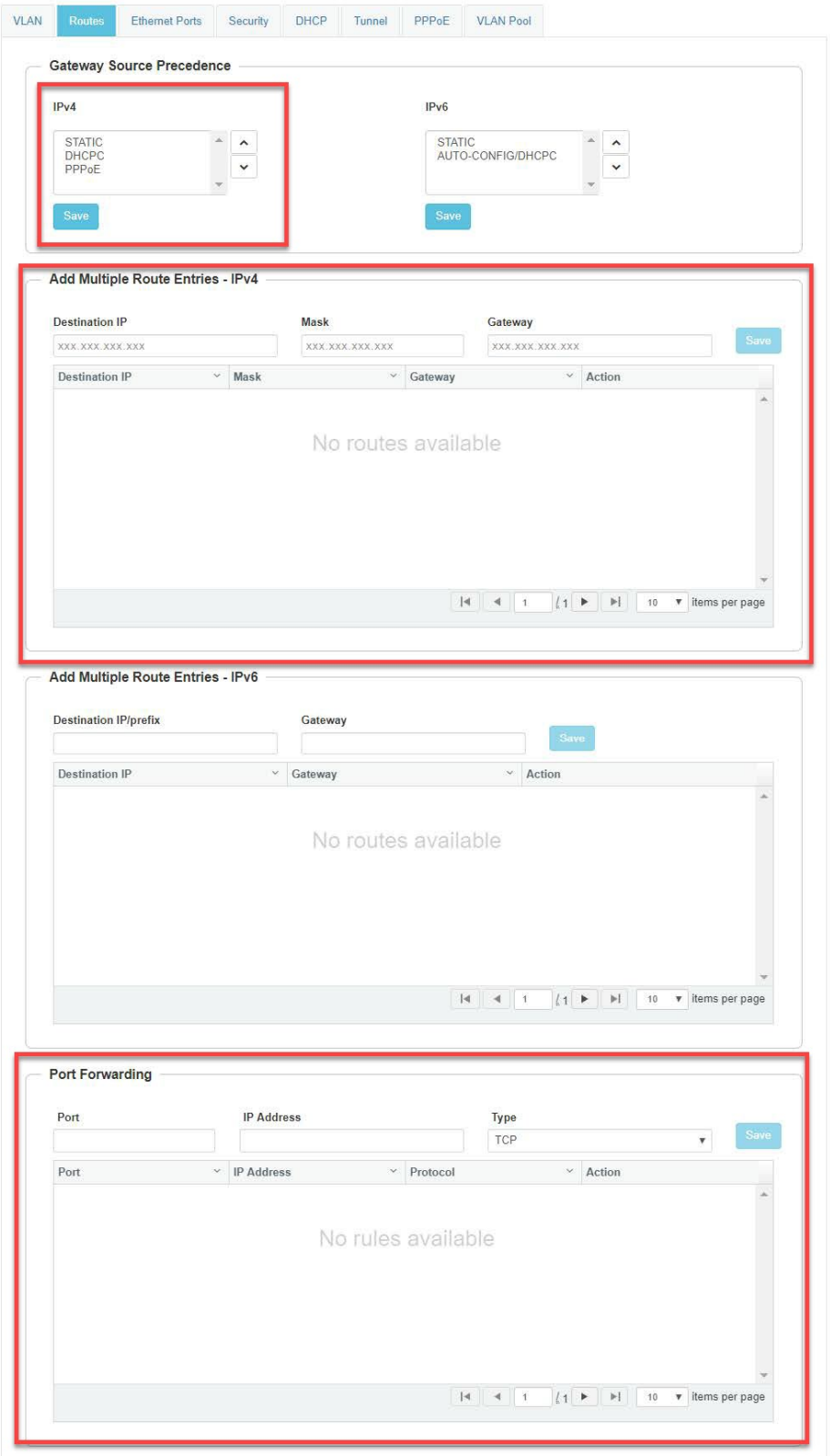
To configure Add Multiple Route Entries:

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

To configure Port Forwarding:

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

Figure 31: *Routes (IPv4) parameters*



IPv6 network parameters

VLAN

Table 40: VLAN (IPv6) parameters

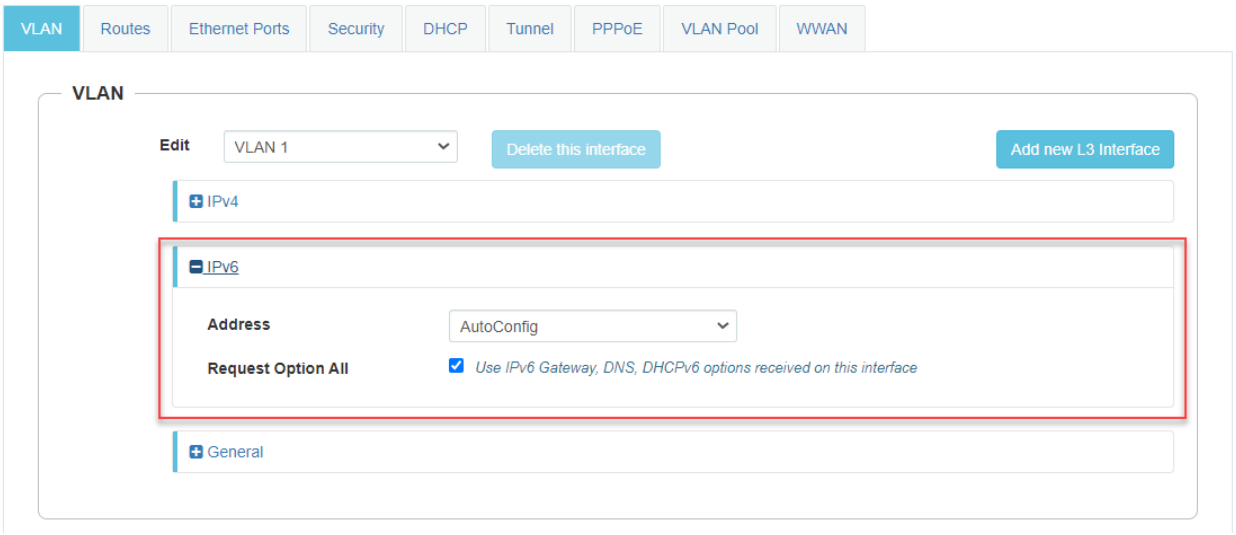
Parameters	Description	Range	Default
Address	Provision to configure the mode of IPv6 address configuration for an interface selected. Five modes are supported: • Disabled • AutoConfig • Static • Stateless DHCPv6 • Stateful DHCpv6	–	AutoConfig
Request Option All	This configuration decides the interface on which AP will learn the following: • IPv6 default gateway • DHCP client options like Option 52 and Option 24 (Controller discovery like controller hostname / IPv6 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 IPv6**:

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

Figure 32: *VLAN (IPv6) parameters*



Routing & DNS

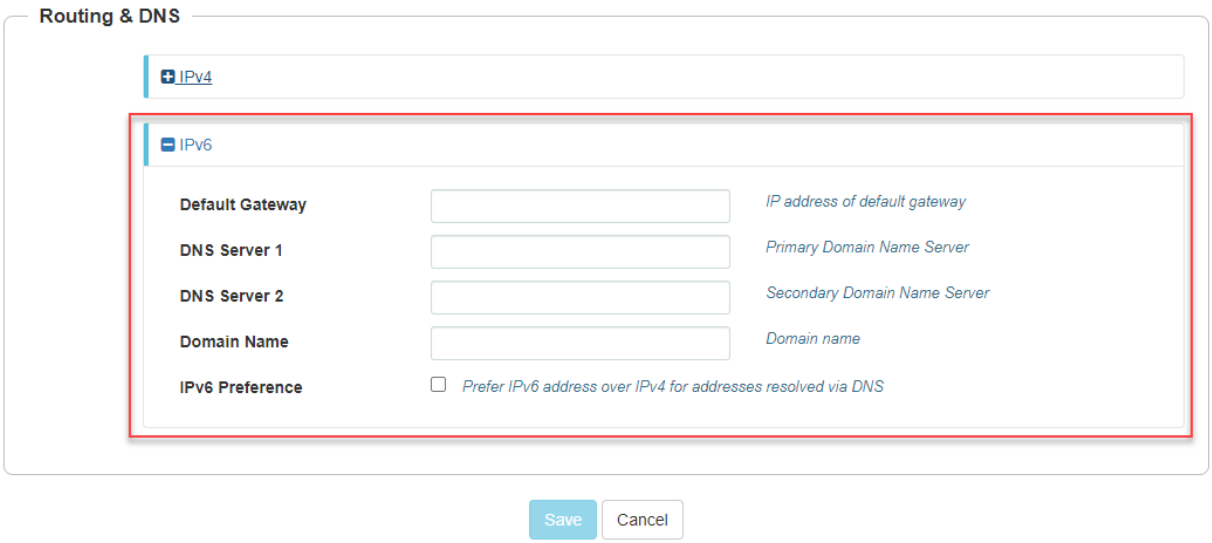
Table 41: Routing & DNS (IPv6) parameters

Parameters	Description	Range	Default
Default Gateway	Provision to configure the 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. A 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 the highest priority.	–	–
IPv6 Preference	When enabled, IPv6 is preferred over IPv4 based on DNS response.	–	Disabled

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

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

Figure 33: *Routing & DNS (Pv6) parameters*



Routes

Table 42: Routes (IPv6) parameters

Parameters	Description	Range	Default
Gateway Source Precedence	Provision to prioritize default gateway and DNS servers when Enterprise Wi-Fi AP device has learned from multiple ways. Default order is Static and AUTO-CONFIG/DHCPC.	–	Static
Add Multiple Route Entries	The user has provision to configure static Routes. Parameters that are required to configure static Routes are as follows: • Destination IP/prefix • Gateway	–	–

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

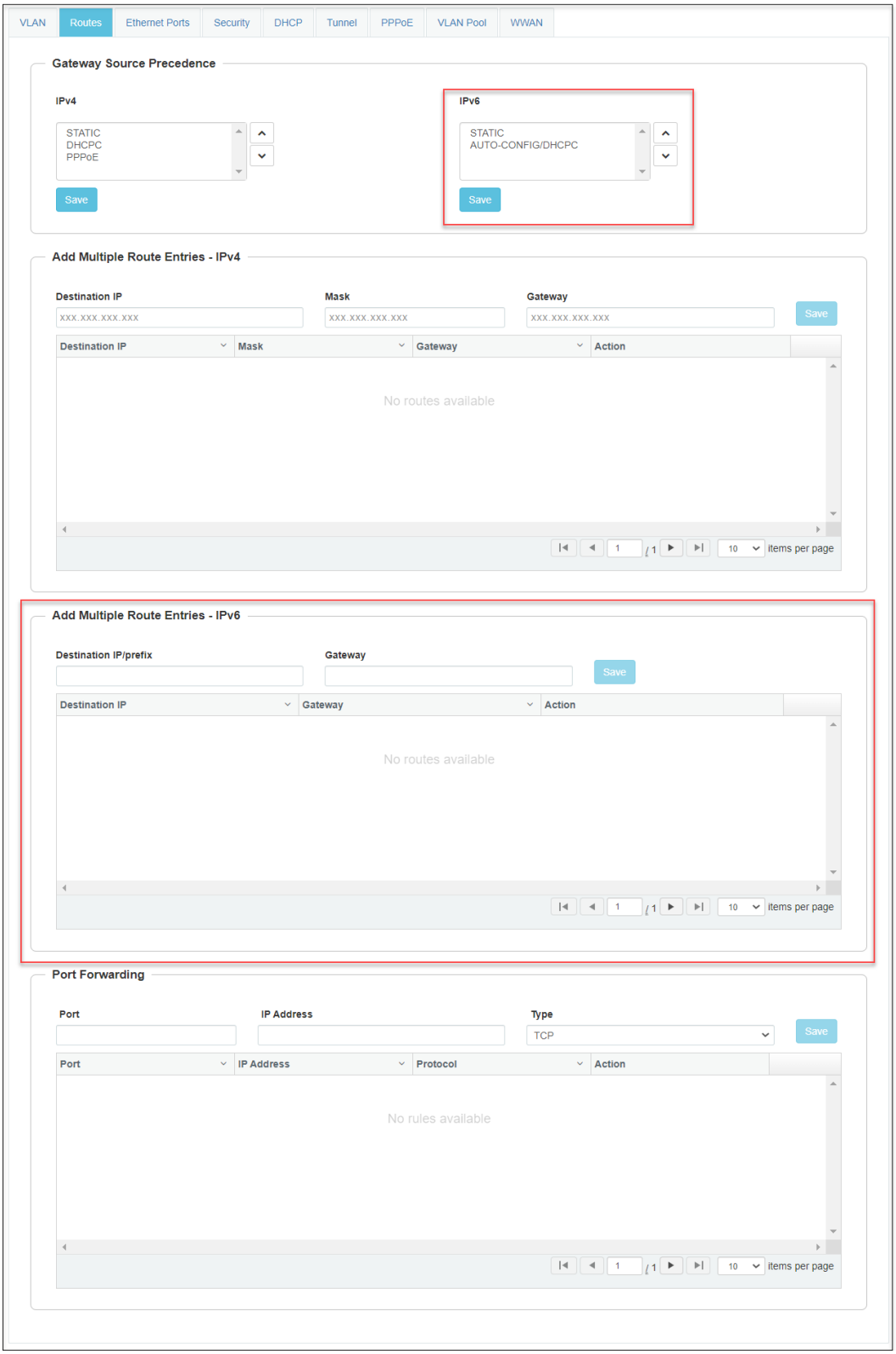
To configure **Gateway Source Precedence**:

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

To configure **Add Multiple Route Entries**:

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

Figure 34: *Routes (IPv6) parameters*



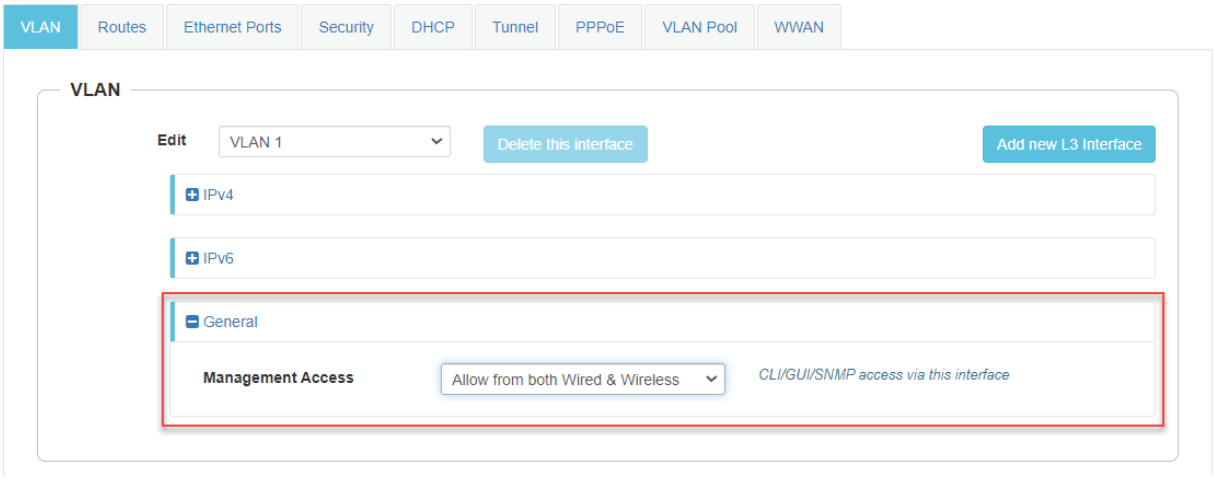
General network parameters

Table 43: VLAN (General) parameters

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

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

Figure 35: *VLAN (General) parameters*



Ethernet Ports

Below table lists the fields that are displayed in **Configure > Network > Ethernet Ports** tab.

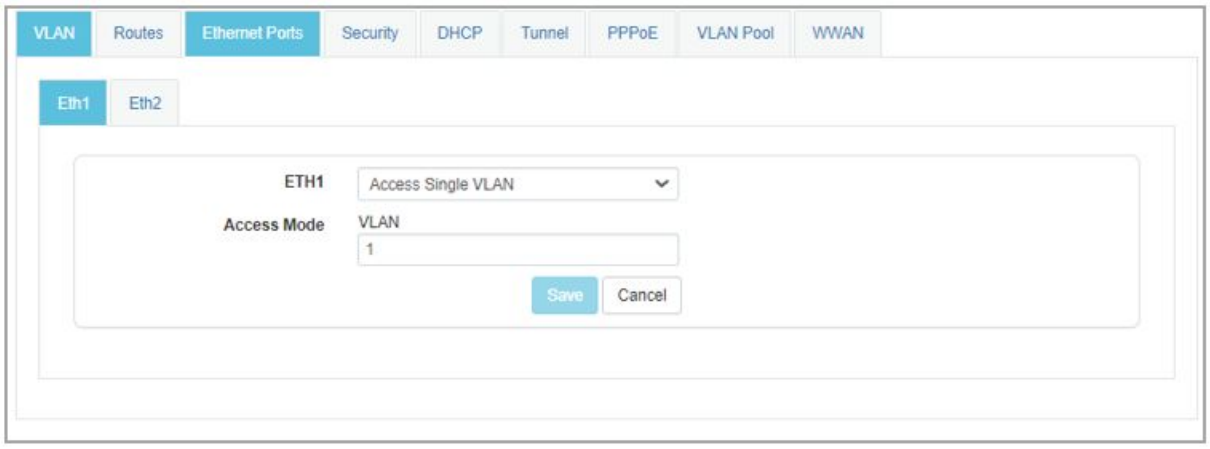
Table 44: Ethernet Ports parameters

Parameters	Description	Range	Default
Ethernet	Enterprise Wi-Fi AP devices Ethernet port is provisioned to operate in the following modes: • **Access Single VLAN**—Single VLAN traffic is allowed in this mode. • **Trunk Multiple VLANs**—Multiple VLANs are supported in this mode.	–	Access Single VLAN

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 text box.
3. Click **Save**.

Figure 36: *Ethernet Ports parameters*



Port Control—802.1X Authentication

802.1X authentication on Ethernet ports enhance the network security of the AP. The AP supports 802.1X port-based authentication in the single-host authentication mode. In this mode, only one client is allowed to access the network after successful 802.1X port-based authentication. After successful authentication, the port VLAN is assigned based on RADIUS assigned VLAN.

Note

- 802.1X port-based authentication does not support CoA messages.

802.1X port-based authentication requires a RADIUS AAA server for authentication and accounting.

The following table lists the parameters for configuring the RADIUS AAA server on Ethernet ports available on the **Configuration > Network > Ethernet Ports > RADIUS Server** page:

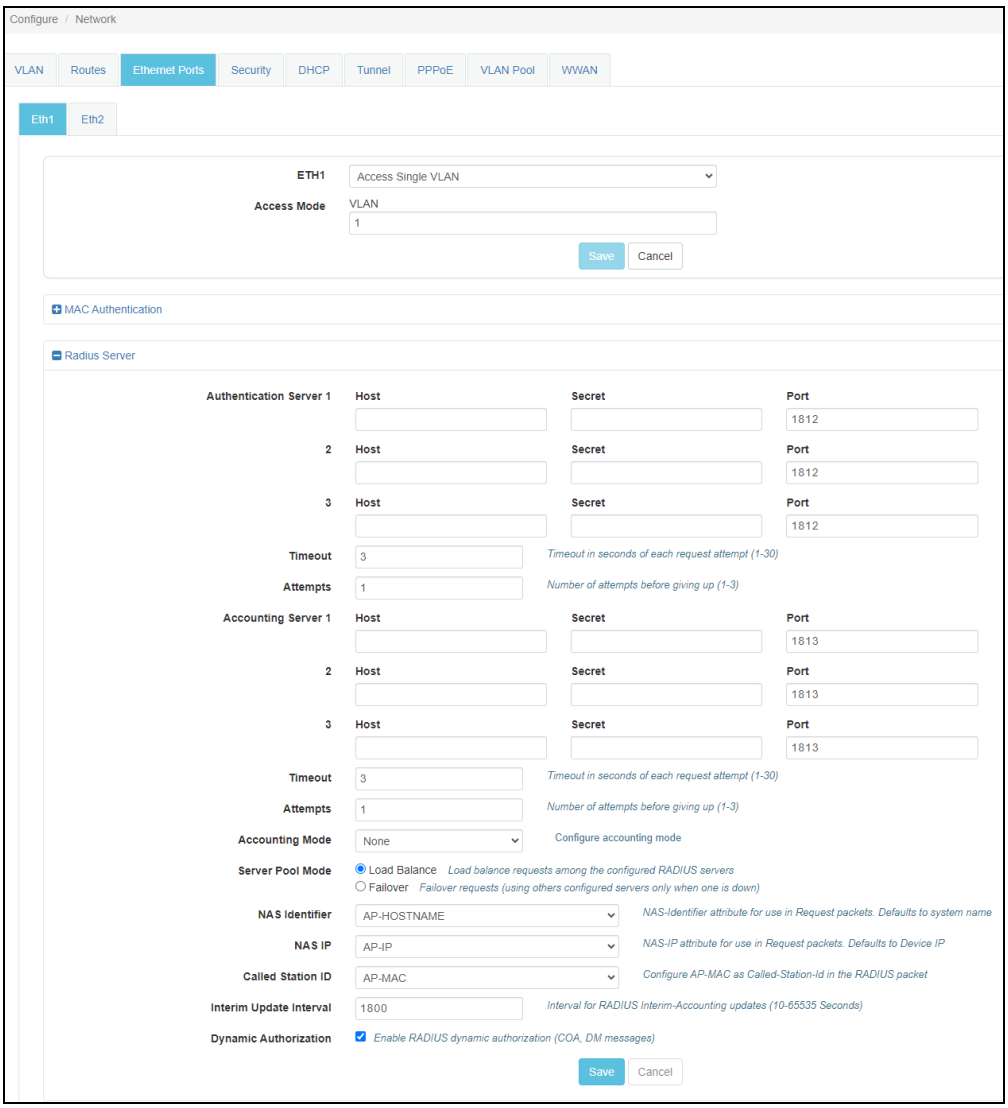
Table 45: RADIUS Server parameters

Parameters	Description	Range	Default
Authentication Server	Specifies the authentication server details, such as: • **Host**—IPv4 or IPv6 address or hostname of the server • **Secret**—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • **Port**—Port number of the authentication server. Default—`1812`	-	Disabled

Parameters	Description	Range	Default
	A maximum of three RADIUS authentication servers can be configured.		
Accounting Server	Specifies the accounting server details, such as: • **Host**—IPv4 or IPv6 address or hostname of the server • **Secret**—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • **Port**—Port number of the accounting server. Default—`1813` A maximum of three RADIUS accounting servers can be configured.	-	Disabled
Timeout	Time (in seconds) to wait for a response from the RADIUS server.	`1-30`	`3`
Attempts	Number of retry attempts for contacting the RADIUS server.	`1-3`	`1`
Accounting Mode	Specifies the accounting mode to be used. The following modes are supported: • **Start-Stop**—Accounting packets are transmitted by APs to the AAA server when a wireless client is connected and when the client disconnects. • **Start-Interim-Stop**—Accounting packets are transmitted by APs to the AAA server when a wireless client connects, then at regular intervals (configured in the **Interim Update Interval** field) and also when the client disconnects. • **None**—Disables the accounting mode. This is the default mode.	-	**None** (Disabled)
Accounting Packet	Specifies whether the AP must send the Accounting-On message to every client when connected. Select the check box to enable.	-	Disabled
Server Pool Mode	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode. • **Load Balance**—AP equally distributes the requests between the configured RADIUS servers, • **Failover**—AP selects the RADIUS server that is functional based on the order of configuration.	-	Failover

Parameters	Description	Range	Default
NAS Identifier	This is a configurable parameter and is appended in the RADIUS request packet.	-	AP hostname (System Name)
NAS IP	NAS IP address to be included in the outgoing RADIUS request packets.	-	AP-IP (Device IP)
Interim update interval	Time (in seconds) to wait for sending RADIUS interim accounting update packets. **Note**: This interval is applicable only when you select the **Start-Interim-Stop** option in the **Accounting Mode** parameter.	10–65535	1800
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled
Called Station ID	The following information can be communicated to the RADIUS server: • AP-MAC • AP-MAC: SITE-NAME • AP-NAME • AP-NAME: SITE-NAME • SITE-NAME • CUSTOM	-	AP-MAC

Figure 37: *RADIUS Server parameters*



General network parameters

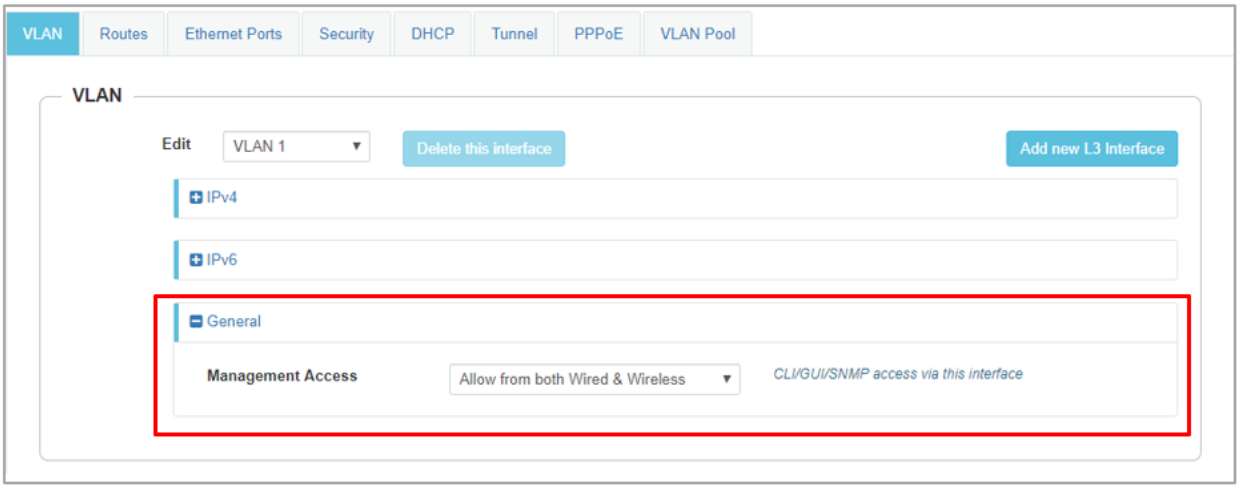
Below table lists the fields that are displayed in **Configure > Network > VLAN > General parameters** tab:

Table 46: The General parameters

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

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

Figure 38: *The General parameters*



Security

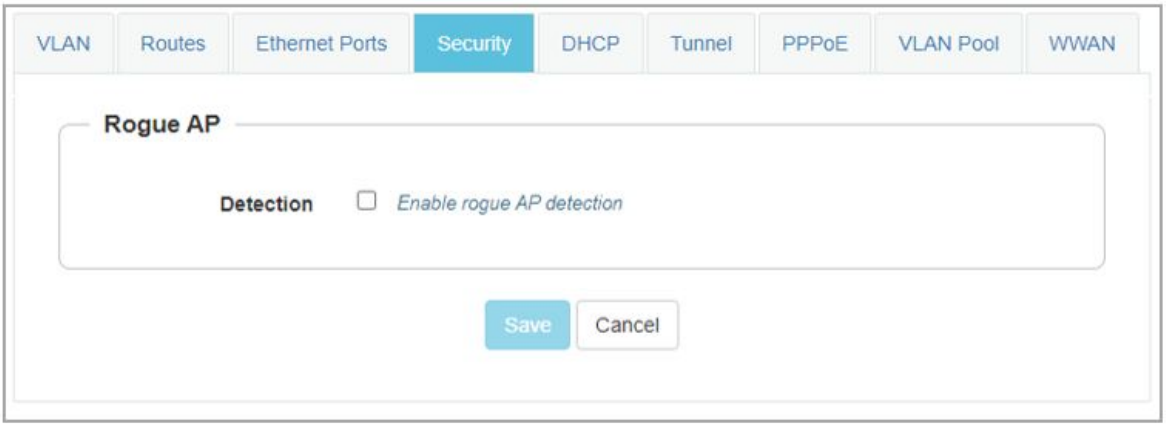
The below table lists the fields that are displayed in the **Configuration > Network > Security** tab.

Table 47: Security parameters

Parameters	Description	Range	Default
Rogue AP			
Detection	Enterprise Wi-Fi devices in association with cnMaestro have the capability of detecting Rogue APs. On enabling this all neighbor information is shared to cnMaestro and reports Rogue APs in the networks.	–	Disabled

To configure the above parameter, navigate to the **Configuration > Network > Security** tab. Select **Detection** check box to enable this functionality.

Figure 39: *Security parameters*



DHCP

Below table lists the fields that are displayed in the **Configuration > Network > DHCP** tab.

Table 48: 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	Users 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 the drop-down box.	–	–
Domain Name	Provision to configure the domain name for a DHCP pool selected from the drop-down box.	–	–
DNS Address	Provision to configure DNS server for a DHCP pool selected from the drop-down box.	–	–
Network	Provision to configure Network ID for a DHCP pool selected from the drop-down box.	–	–
Lease	Provision to configure lease for a DHCP pool selected from the drop-down box.	–	–
Add Bind List			
	For every DHCP pool configured, the user can bind MAC and IP from the address pool defined, so that the wireless station gets the same IP address every time they connect. Following parameters are required to bind IP address: • MAC Address • IP Address	–	–

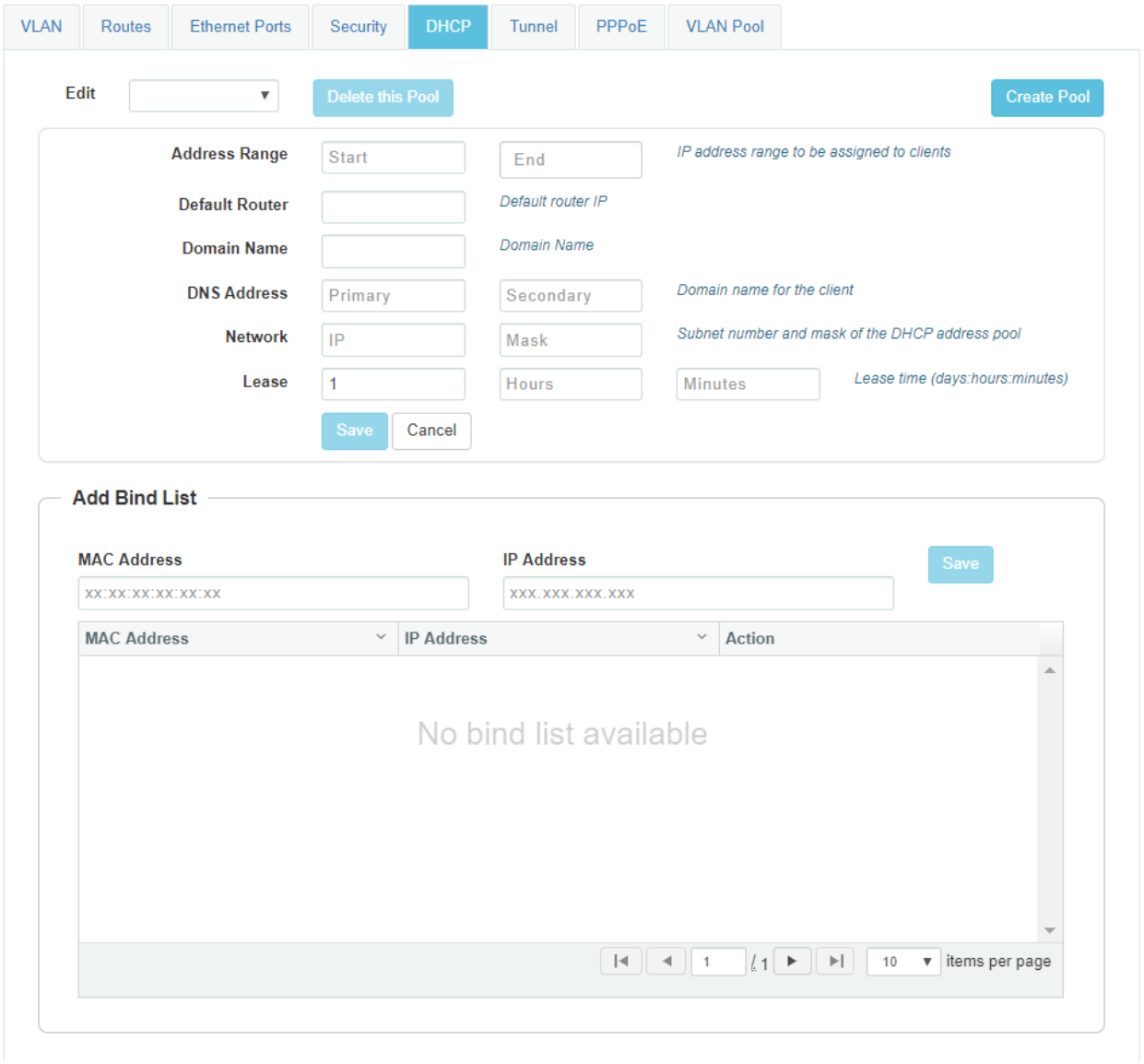
To configure the above parameter, navigate to the **Configure > Network > DHCP** tab and provide the details as given below:

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

To configure **Add Bind List,** follow the below steps:

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

Figure 40: *DHCP parameters*



Tunnel

The following table lists the fields that are displayed in **Configure > Network > Tunnel** tab.

Table 49: The Tunnel parameters

Parameters	Description	Range	Default
Tunnel Encapsulation	Provision to enable tunnel type. Following tunnel types are supported by Enterprise Wi-Fi AP devices: • L2TP • L2GRE • OFF	–	OFF
L2TP			
Remote Host	Configure L2TP end point. IPv4 address or Primary hostname of the endpoint is supported.	–	–
Authentication Info	Provision to configure credentials required for L2TP authentication.	–	–
Auth Type	Provision to select the PPP authentication method. Following are the options available: • DEFAULT • CHAP • MS-CHAP • MS-CHAPv2 • PAP	–	DEFAULT
Secondary Remote Host	Configure secondary L2TP end point.IPv4 address or Secondary hostname of an endpoint is supported.	–	–
Secondary Authentication Info	Provision to configure credentials required for secondary L2TP authentication.	–	–
Secondary Auth Type	Provision to select the secondary PPP authentication method. Following are the options available: • DEFAULT • CHAP • MS-CHAP • MS-CHAPv2 • PAP	–	DEFAULT
TCP MSS	Provision to configure TCP Maximum Segment Size.	422- 1410	1400

Parameters	Description	Range	Default
PMTU Discovery	Provision to enable to discover PMTU in network.	–	Enabled
Disconnect Wireless Clients	Provision to disconnect Wireless Client when the state of L2TP tunnel is down.	–	Enabled
L2GRE-1 You can configure a maximum of two L2GRE tunnels. Configure L2GRE-1 tunnel by configuring the below parameters in the **Configure > Network > Tunnel** tab. However, configuring L2GRE-2 tunnel is allowed only using the device CLI. The following parameters for L2GRE-1 are also applicable for L2GRE-2.			
Primary Remote Host	Configure L2GRE endpoint. IPv4 address or Primary hostname of an endpoint is supported.	–	–
Secondary Remote Host	Configure L2GRE endpoint. IPv4 address or Secondary hostname of an endpoint is supported. The tunnel operates in failover mode. After determining the peer is down (no Rx packet received from PEER), AP sends periodic ICMP packet to verify the reachability to the peer before failing over to secondary peer. So ensure ICMP reachability to the tunnel PEER.	–	–
DSCP	Users can configure priority of GRE packets.	–	0
TCP MSS	Provision to configure TCP MSS value.	472-1460	1402
PMTU Discovery	Provision to enable to discover PMTU in a network.	–	–
MTU	Maximum Transmission Unit.	850-1460	1460
GRE in UDP	GRE protocol is designed to establish a tunnel between any third-party vendor which complies with RFC 8086.	–	Disabled
Disconnect Wireless Clients	Provision to disconnect Wireless Client when a state of L2TP tunnel is down.	–	Enabled
Tunnel Reachability	The periodic interval for verifying the RX packet from GRE peer.	30-240	240
Tunnel Retry Attempts	Number of retries before failover to secondary peer.	2-10	5
IPv6 Tunnel	Enables tunnel resolution to send packets through the IPv6 network.	-	Disabled

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

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

To configure **L2TP**:

2. Enter IP address or domain name in the **Remote Host** text box.
3. Enter credentials required for L2TP authentication in the **Authentication Info** text box.

4. Select authentication type from the **Auth Type** drop-down list.
5. Enter IP address or domain name in the **Secondary Remote Host** text box.
6. Enter credentials required for secondary L2TP authentication in the **Secondary Authentication Info** text box.
7. Select authentication type from the **Secondary Auth Type** drop-down list.
8. Enter TCP Maximum Segment Size in the **TCP MSS** text box.
9. Enable **PMTU Discovery** check box.
10. Enable **Disconnect Wireless Clients** check box.
11. Click **Save**.

To configure **L2GRE-1**:

12. Enter the IP address or domain name in the **Primary Remote Host**/**Secondary Remote Hos**t text box.
13. Enter **DSCP** in the text box.
14. Enter TCP Maximum Segment Size in the **TCP MSS** text box.
15. Enable **PMTU Discovery** check box.
16. Enter Maximum Transmission Unit in the **MTU** text box.
17. Enable GRE in UDP in the **GRE** check box.
18. Enable **Disconnect Wireless Clients** check box.
19. Enter periodic interval value in **Tunnel Reachability** text box.
20. Enter a number of retries in **Tunnel Retry Attempts** text box.
21. Click **Save**.

Configuring **L2GRE-2** tunnel is allowed only using the device CLI. The values of the above parameters are shared across both L2GRE-1 and L2GRE-2 tunnels, except the following:

- Primary Remote Host
- Secondary Remote Host
- IPv6 Tunnel

  IPv6 tunnel is configurable only in the device CLI using the `ipv6-tunnel` command.

  Execute the `ipv6-tunnel` command in the `config-l2gre-<1/2>` context, as shown in the figure:

  Figure 41: *ipv6-tunnel command*

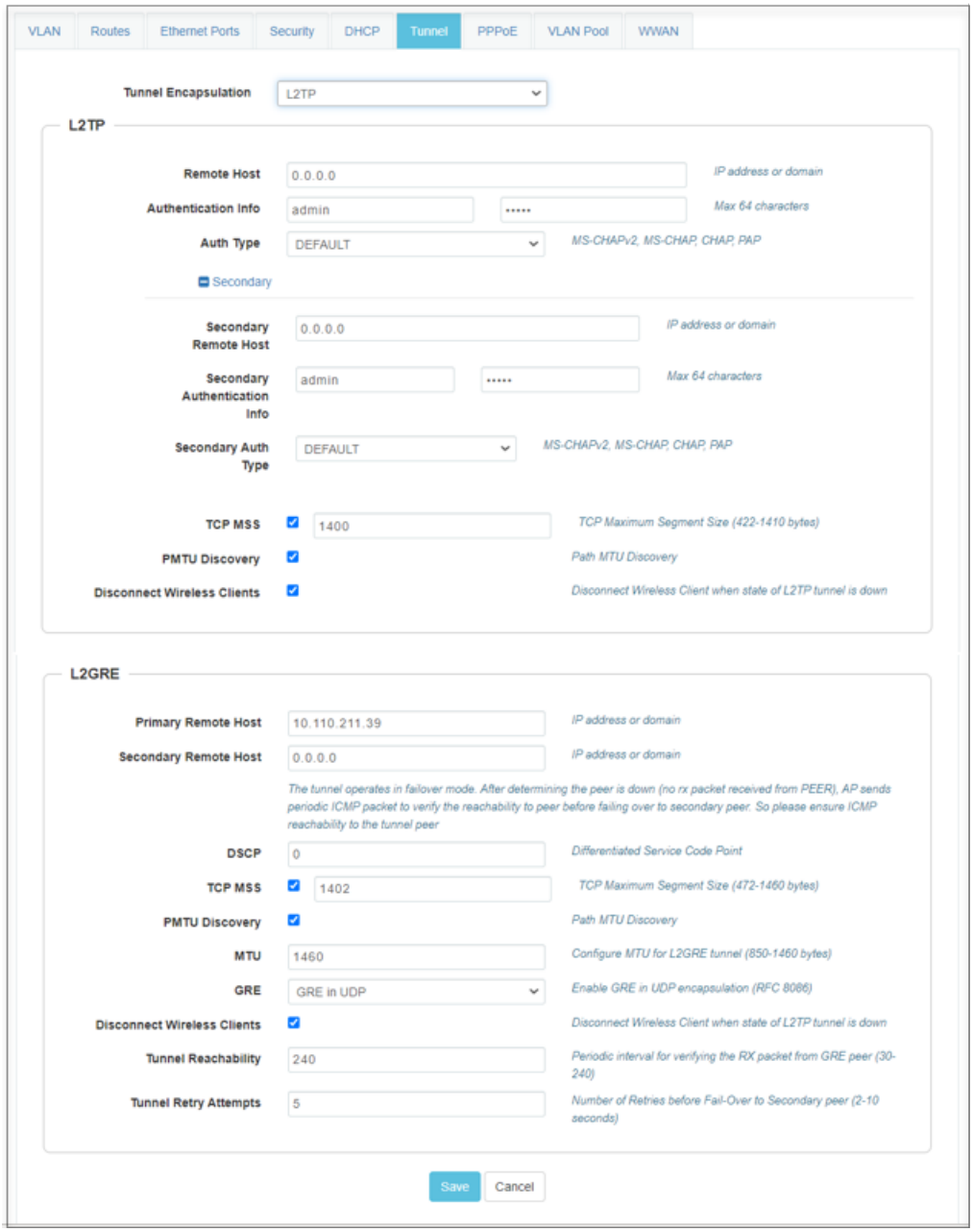
```
XV2-22H-E53E28(config)# tunnel l2gre 1
XV2-22H-E53E28(config-l2gre-1)# ipv6-tunnel
XV2-22H-E53E28(config-l2gre-1)#
```

Figure 42 displays the parameter differences between L2GRE-1 and L2GRE-2 tunnels.

Figure 42: *L2GRE-1 and L2GRE-2 parameters differences*

```
XV2-22H-E53E28(config)# tunnel l2gre 1
XV2-22H-E53E28(config-l2gre-1)# remote-host 10.10.10.1
XV2-22H-E53E28(config-l2gre-1)# exit
XV2-22H-E53E28(config)# tunnel l2gre 2
XV2-22H-E53E28(config-l2gre-2)# remote-host 2001:db7::d43:2ee2:26c4:6465
XV2-22H-E53E28(config-l2gre-2)# exit
XV2-22H-E53E28(config)# save
[Config Save OK]
XV2-22H-E53E28(config)#
```

Figure 43: *Tunnel parameters*



Point-to-Point Protocol over Ethernet (PPPoE)

PPPoE provides the ability to establish a connection to ISP with user authentication. Below table lists the fields that are displayed in **Configuration > Network > PPPoE** tab.

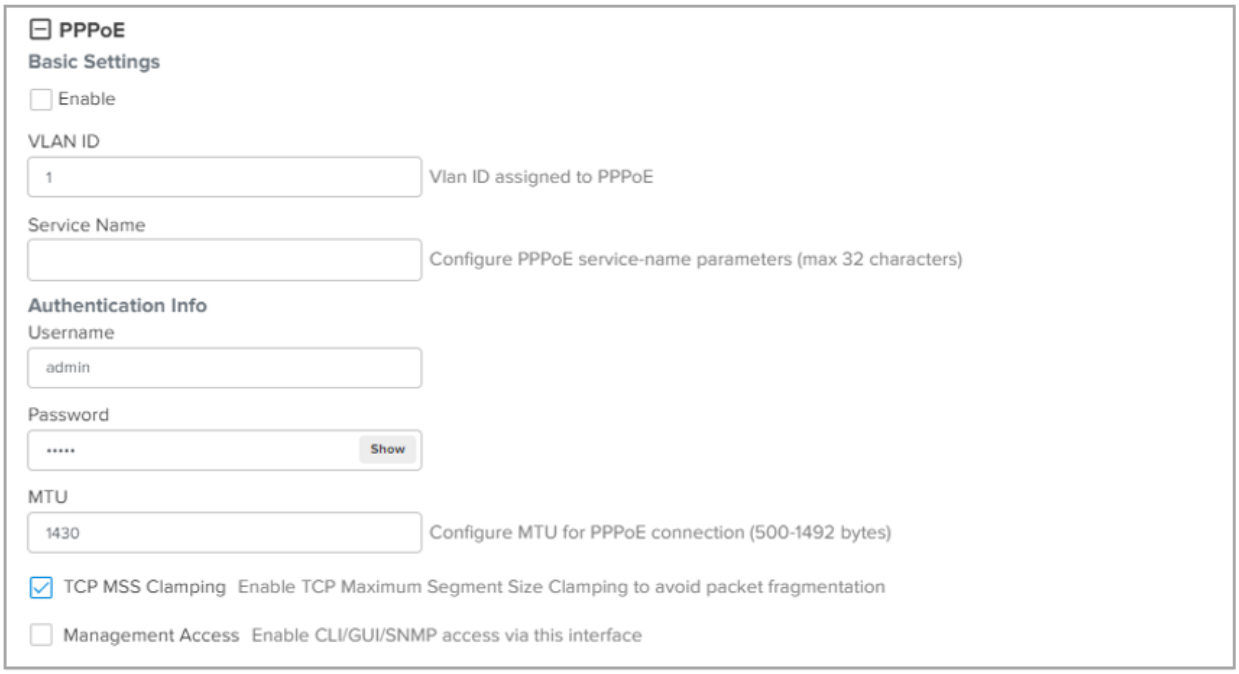
Table 50: PPPoE parameters

Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disabled
VLAN	Users can configure VLAN ID where PPPoE clients should obtain an IP address.	–	–
Service Name	Configure PPPoE service name	–	–
Authentication Info	Provision to configure credentials required for PPPoE authentication.	–	–
MTU	Maximum Transmission Unit.	500-1492	1430
TCP-MSS Clamping	Configure PPPoE endpoint. Either IP or hostname of an endpoint is supported.	–	Enabled
Management Access	If enabled, the user can access the device either using UI or SSH with PPPoE IP.	–	Disabled

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

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

Figure 44: *PPPoE parameters*



VLAN Pool

The following table lists the fields that are displayed in **Configure > Network > VLAN Pool** tab.

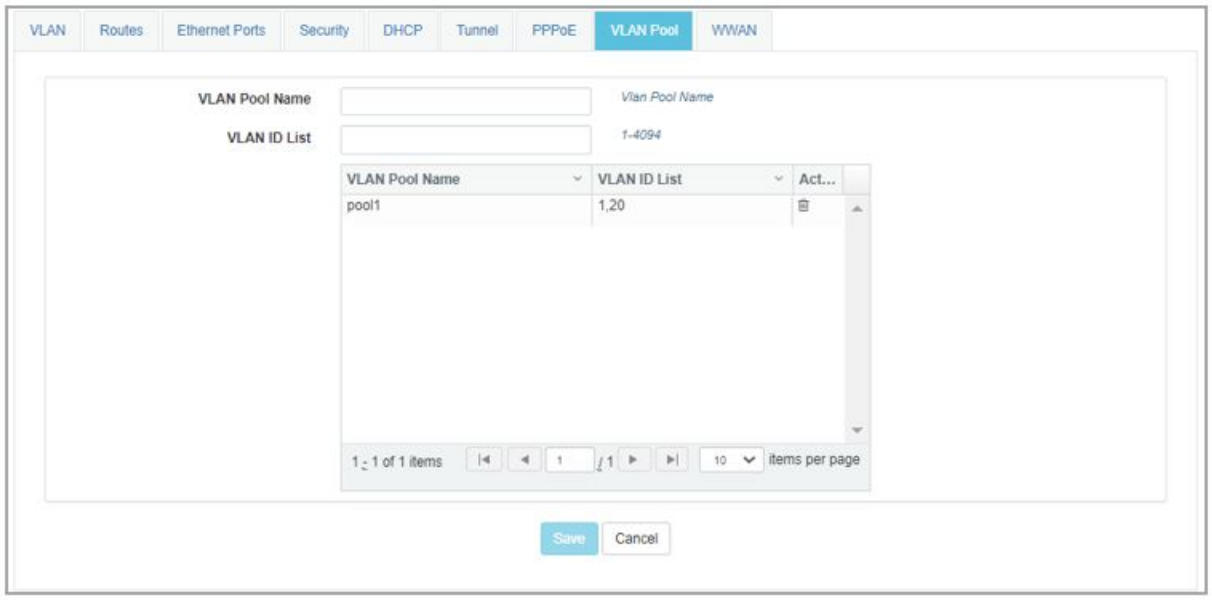
Table 51: The VLAN Pool parameters

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

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

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

Figure 45: *The VLAN Pool parameters*



Wireless Wide Area Network (WWAN)

The following table lists the fields that are displayed in **Configure > Network > WWAN** tab.

Note

This feature is supported in XV2-2, XV3-8, XE3-4, and XE5-8 platforms only.

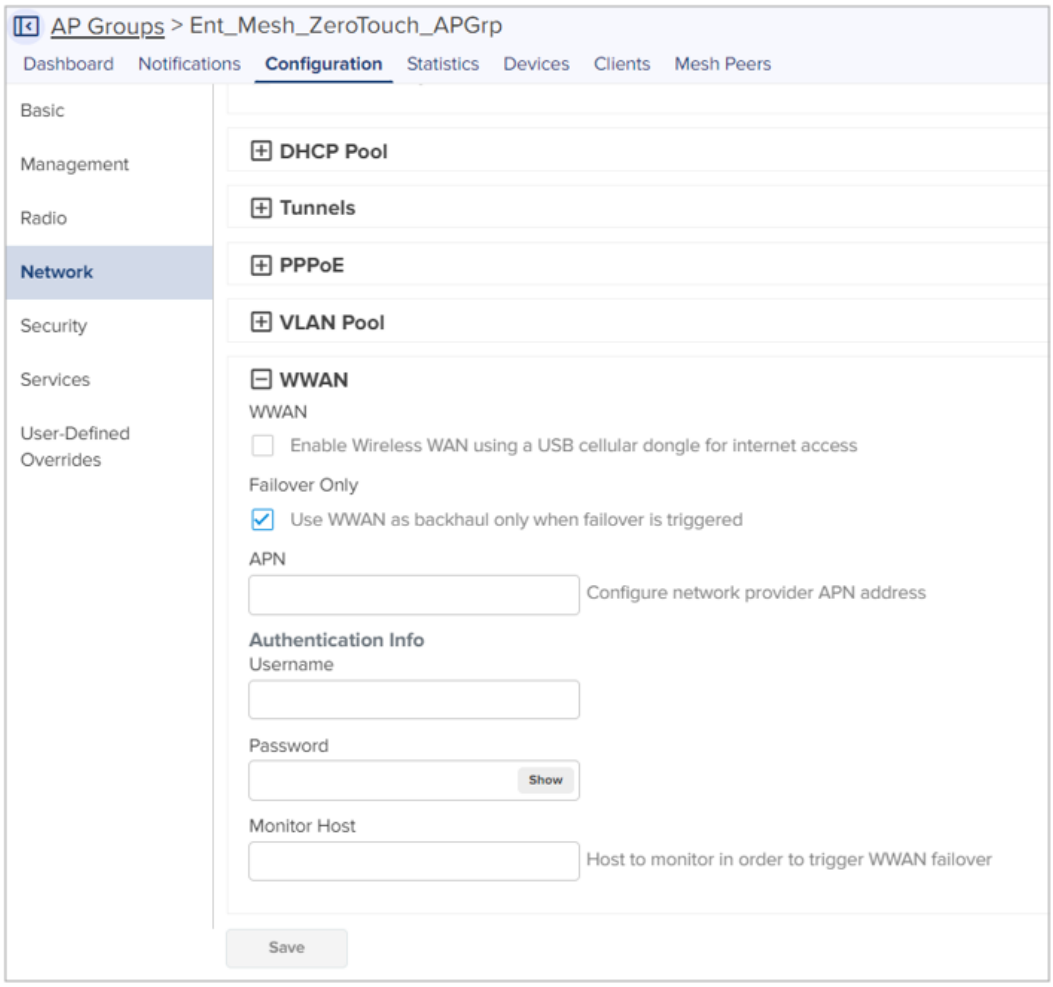
Table 52: WWAN parameters

Parameters	Description	Range	Default
WWAN	Provision to enable wireless WAN using a USB cellular dongle for internet access.	–	–
Failover Only	Failover only can be configured in two modes: • Enabled: Ethernet will be the primary connection and WWAN will be backup. • Disabled: 3G/4G (WWAN) will be the only working connection. **Note**: Cellular link can be configured as backup only to Ethernet connection.	–	Enabled
APN	Provision to configure network provider APN address.	–	–
Authentication	Provision to configure credentials required for WWAN authentication.	–	–
Monitor Host	Running a check in the background that constantly monitors a user configured IP address (example: 8.8.8.8) for reachability through ping.	–	–

To configure the above parameter, login to cnMaestro **AP Group > Network > WWAN** tab and provide the details as given below:

1. Enable **WWAN** check box to enable this functionality.
2. Check/Uncheck **Failover Only** to enable/disable.
3. Enter the **APN** address in the text box.
4. Enter the **Authentication** credentials.
5. Enter any IPv4 address to **Monitor Hoist** text box.
6. Click **Save**.

Figure 46: *WWAN parameters*



Supported hardware

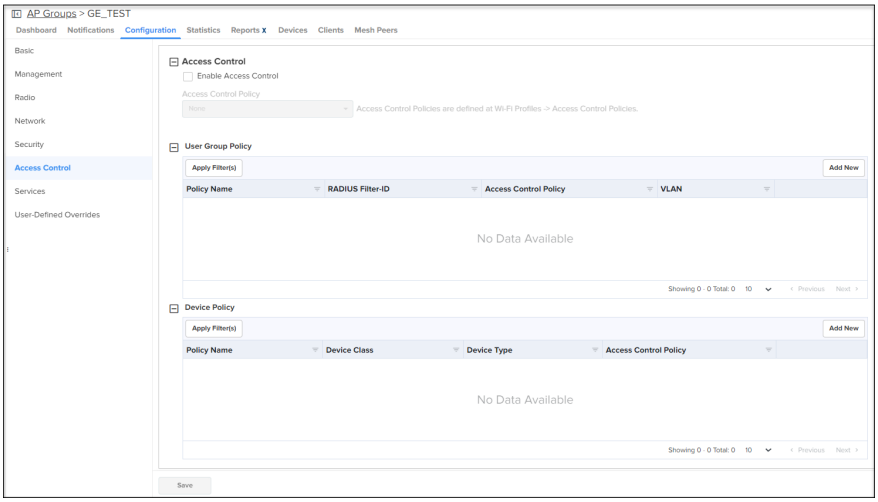
Cambium Networks currently support following models:

- Huawei
    - E8372
    - E3372
- Alcatel
    - Link Key 4G IK40V
- ZTE
    - MF833V

Chapter 8: Configuring Access Control

The Access Control page allows the users to enable or assign access control policies and configure user group policies and device policies. It offers visibility into the configured rules, ensuring efficient and secure network management.

Figure 47: *Access Control page*



Note

If an Access Control Policy is assigned at the AP group level, it does not appear under User Group or Device Group policies.

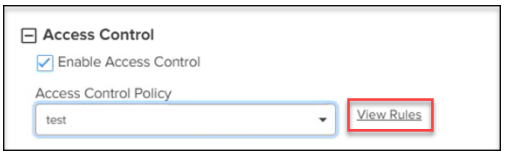
This chapter describes the following topics

- Enabling Access Control Policy
- User Group Policy
- Device Policy

Enabling Access Control Policy

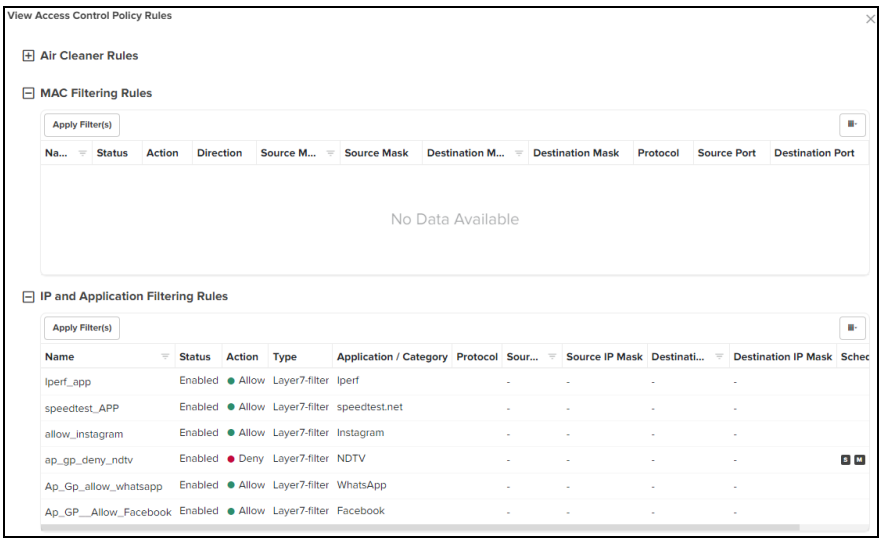
Users have the provision to enable or disable access control policies under **Access Control** tab.

Figure 48: *Enabling Access Control Policy*



Users can select the available access control policies listed in the Wi-Fi profiles in the **Access Control Policy** drop-down list. They can also view the configured rules associated with these policies by clicking **View Rules**. This provides a comprehensive view of the policies and rules within the network.

Figure 49: *Access Control Policy Rules*



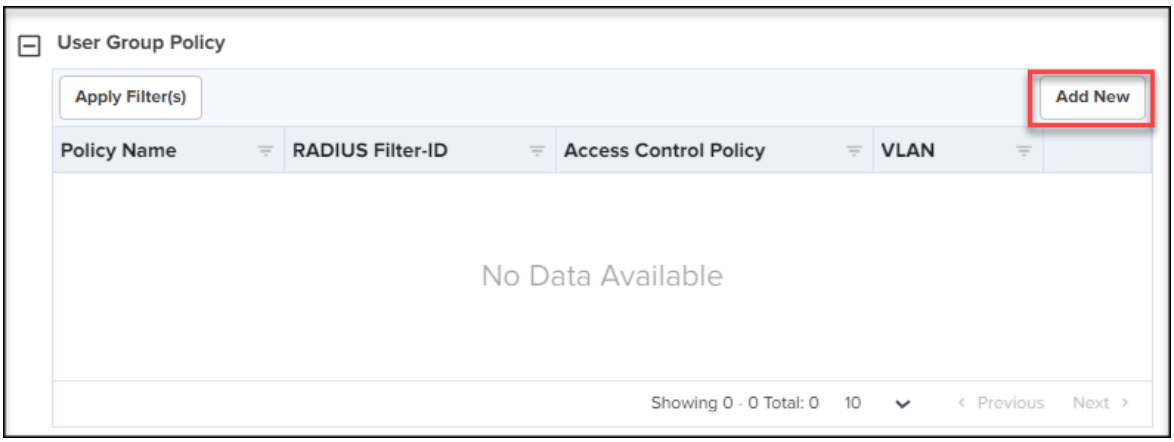
User Group Policy

User group policies allow you to categorize users into specific roles with customized access permissions and restrictions, facilitating a fine-tuned control over network access.

To add a new to User Group Policy, perform the following steps:

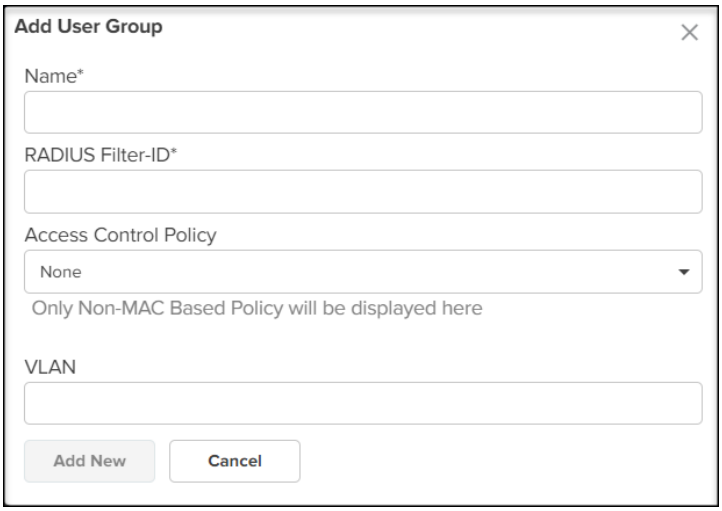
1. Navigate to **Configuration** > Wi-Fi Profiles > AP Groups > **Access Control** page.
2. Click **Add** to create a new AP group.
3. Click the **Access Control** tab in the **Add New** page.
4. Click **Add New** in the **User Group Policy** section.

   Figure 50: *User Group Policy*



5. Complete the details in the **Add User Group** window.

Figure 51: *Add User Group*



Note

- The user must assign an Access Control Policy or VLAN to create a User Group Policy.
- A maximum of 64 User Group Policies are supported.
- Users can select Access Control Policies with non-MAC filters only from the **Access Control Policy** drop-down list.
- Mapping an Access Control Policy to a User Group Policy enables its use for the AP group, and vice versa. However, the same Access Control Policy cannot be shared between the User Group Policy and the AP group. You can apply it either to the User Group Policy or to the AP group only.

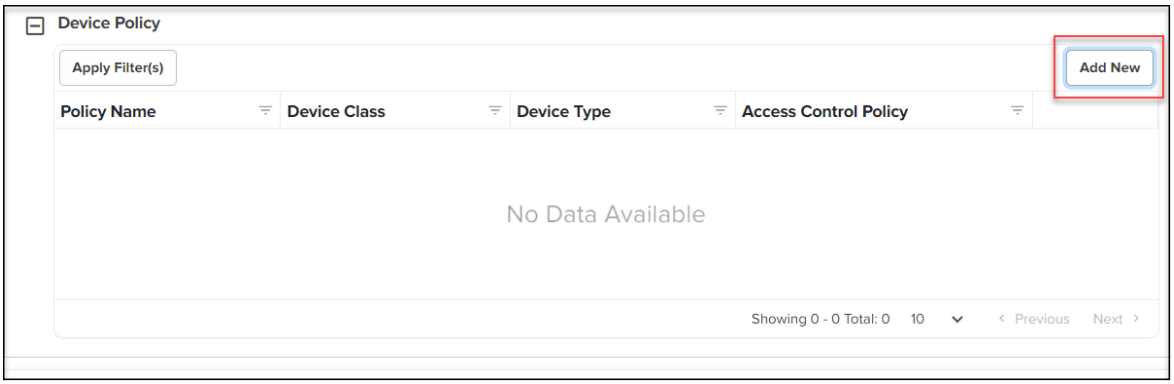
Device Policy

Device Policy allows users to apply specific rules and access control policies based on the type and characteristics of devices, offering customized control over device behavior within the network.

To add a new Device Policy, perform the following steps:

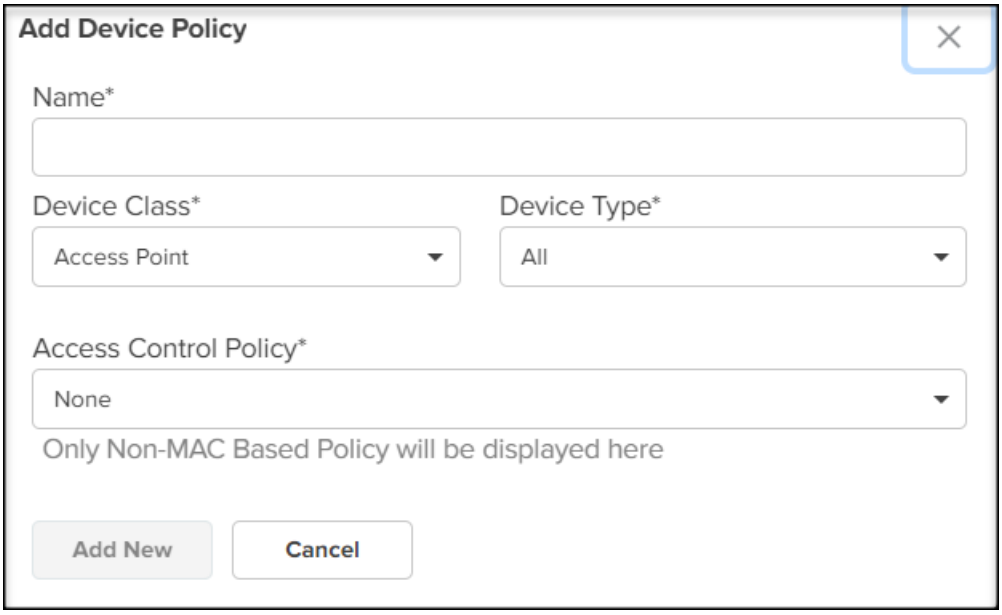
1. Navigate to **Configuration** > **Wi-Fi Profiles** > **AP Groups** tab.
2. Click **Add** to create a new AP group.
3. Click the **Access Control** tab in the **Add New** page.
4. Click **Add New** in the **Device Policy** section.

Figure 52: *Device Policy*



5. Complete the details in the **Add Device Policy** window.

Figure 53: *Add Device Policy*



Note

- A maximum of 64 Device Policies are supported.
- Users can select Access Control Policies with non-MAC filters only from the **Access Control Policy** drop-down list.

Chapter 9: Managing Filters

This chapter describes the following topics:

Overview

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 the 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 users to apply a uniform set of filters to SSIDs. AP supports 16 filter lists 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 Layer 2 and Layer 3 or application/category control (Layer 7). Layer 2 rule takes high precedence over Layer 3 application control and Layer 2 supports 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.

Configuring filter CLI

By configuring the filter CLI, the user can define ACL rules for blocking or passing traffic, DSCP/QoS rules for modifying packets, and rate-limiting for selected traffic.

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

   ```
   XV3-8-EC7708(config)# filter
   ```

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

2. Global-filter is for global rules in AP. Global-filter includes the below options:

```
XV3-8-EC7708(config-global-filter)#
air-cleaner : Configure Preset air cleaner filters
application-control : Enable application control
clear : Clear command
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
show : Show command
```

   - **Stateful filtering** : Stateful operation of the integrated firewall can be Enabled or Disabled. By default, it is enabled.
   - **Application Control** Premium feature: Operation of the Application Control feature may be Enabled or Disabled.
   - **Disable**: Disable or enable filter list.

3. Each filter list includes below options:

```
clear                : Clear command
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
show                 : Show command
```

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-EC7708(config-list-1-filter-precedence-1)# exit
XV3-8-EC7708(config-filter-list-1)# filter precedence 1
XV3-8-EC7708(config-list-1-filter-precedence-1)#

  application-control  : Configure application control filters
  category-control     : Configure application category control filters
  clear                : Clear command
  disable              : Disable filter
  layer2-filter        : Configure Layer2 filter
  layer3-filter        : Configure Layer3 filter
  logging              : Enable filter logging
  rate-limit           : Set traffic limit for this filter
  schedule             : Schedule Layer3 rules
  wlan-to-wlan         : Restrict 'in' direction rule's egress direction as wlan


  apply                : Apply configuration that has just been set
  exit                 : Exit from custom filter configuration
  no                   : Disable the filter options
  save                 : Save configuration to Flash so it persists across reboots
  show                 : Show command
```

Note

The filter type is either Layer 2 or Layer 3 or application control can be added in one precedence level.

5. Layer 3 filter has the below provisions.

```
XV3-8-EC7708(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
```

- **QoS** Premium feature**:** Set packets QoS level (0 to 3). Level 0 has the lowest priority; level 3 has the highest priority
- **DSCP** Premium feature: 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.
- **Rate limit** Premium feature: Filters support rate limiting per station or all stations and support Kbps/Mbps/pps.
- **Schedule** Premium feature: Filter support scheduling the activation of the layer3 /application control rules based on the day and local time selected.
- **Disable**: Each filter and filter list can be turned on/off.

Note:

Application Control, QoS, DSCP, Schedule and **Rate limit** are Premium features.

6. Each layer 3 rule category has below types

```
XV3-8-EC7708(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.

```
XV3-8-EC7708(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{/{ma
sk|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 the direction of the rule. if it is 'in', the rule is applicable for traffic from the wireless side. If it is 'out', the rule is applies for traffic to wireless.

8. For non-proto or port number-based rules, select IP.

```
XV3-8-EC7708(config-list-1-filter-precedence-1)# layer3-filter set-dscp ip

  layer3-filter set-dscp ip (SOURCE-IP{/{mask|prefix-length}}|any) (DESTINATION-IP{/{ma
sk|/prefix-length}}|any) (in|out|any) (DSCP{0-63})   <(optional)//Filter_name>
```

9. Layer 2 filter has below options:

```
XV3-8-EC7708(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-EC7708(config-list-1-filter-precedence-11)# layer2-filter permit

  mac                   : Mac or IP based Rule with out Protocol
  proto                 : Mac or IP based rule with Protocol
```

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

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

```
XV3-8-EC7708(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)  <(option
al)//Filter_name>
```

Example:

```
 e.g. 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

```
XV3-8-EC7708(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-leng
th}}|any) (DESTINATION-PORT|any) (in|out|any)  <(optional)//Filter_name>
```

Example:

```
 e.g 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  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. To attach the filter list into the 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:

```
XV3-8-441BCC(config)# show filter-statistics

  Filter ID | global
```

Device class filter

This feature applies wireless policies to the client-based device class (notebook, phone, tablet, and laptop) and its type (Windows, Mac, and Android).

CLI configuration:

```
XV3-8-EC7708(config)# device-class-filter 1
```

```
XV3-8-EC7708(config-device-class-filter-1)# class
ap : Configure filter rules for the AP device class
appliance : Configure filter rules for the appliance device class
desktop : Configure filter rules for the desktop device class
game : Configure filter rules for the game device class
notebook : Configure filter rules for the notebook device class
phone : Configure filter rules for the phone device class
player : Configure filter rules for the player device class
tablet : Configure filter rules for the tablet device class
XV3-8-EC7708(config-device-class-filter-1)# class notebook
all : Configure filter rules for all notebook device classes
chrome : Configure filter rules for the Chrome-OS device type
linux : Configure filter rules for the Linux device type
mac : Configure filter rules for the Mac device type
windows : Configure filter rules for the Windows device type
XV3-8-EC7708(config-device-class-filter-1)# class notebook linux
XV3-8-EC7708(config-device-class-filter-1)# filter-list
Filter list ID <1-16> or Name
```

Wi-Fi Calling support

Cambium Networks Access Point has the inbuilt application visibility engine, which can detect Wi-Fi calling and provide better call quality by reducing the latency, jitter, and roaming delays for voice calls over Wi-Fi.

When the Access Point detects the Wi-Fi calling traffic, it classifies and puts the traffic in the voice priority queue for achieving better call quality.

CLI configuration:

```
filter precedence 5
   application-control wificall set-qos 3
```

Note

Filter precedence can be from 1 to 50.

Air cleaner

The Air Cleaner feature offers several predetermined filter rules that eliminate a great deal of unnecessary wireless traffic.

Configuration CLI:

```
XV3-8-EC7708(config)# filter global-filter
XV3-8-EC7708(config-global-filter)# air-cleaner
all : All air cleaner filters
```

```
arp : Eliminate station to station ARPs over the air
broadcast : Eliminate broadcast traffic from the air
dhcp : Eliminate stations serving DHCP addresses from the air
multicast : Eliminate chatty multicast traffic from the air
```

When we configure the Air Cleaner rule, pre-defined filter rules will get populated automatically as shown below:

```
XV3-8-EC7708(config-global-filter)# air-cleaner all
XV3-8-EC7708(config-global-filter)# show config filter
!
!
filter global-filter
stateful
application-control
air-cleaner all
filter precedence 1
layer2-filter deny proto arp any any in //Air-cleaner-Arp.1
wlan-to-wlan
exit
filter precedence 2
layer2-filter deny proto udp any any FF:FF:FF:FF:FF:FF 67 out //Air-cleaner-Dhcp.1
exit
filter precedence 3
layer2-filter deny proto udp any any FF:FF:FF:FF:FF:FF 68 in //Air-cleaner-Dhcp.2
exit
filter precedence 4
layer2-filter permit proto arp any FF:FF:FF:FF:FF:FF any //Air-cleaner-Bcast.1
exit
filter precedence 5
layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 67 any //Air-cleaner-Bcast.2
exit
filter precedence 6
layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 68 any //Air-cleaner-Bcast.3
exit
filter precedence 7
layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 22610 any //Air-cleaner-
Bcast.4
exit
filter precedence 8
```

```
layer2-filter deny mac any FF:FF:FF:FF:FF:FF any //Air-cleaner-Bcast.5
exit
filter precedence 9
layer2-filter permit mac any 01:00:5E:00:00:FB any //Air-cleaner-mDNS.1
exit
filter precedence 10
layer2-filter deny mac any multicast any //Air-cleaner-Mcast.1
exit
```

Note

In Mesh link configuration, the Air Cleaner rules need customization like disabling Precedence 2 and Precedence 3 (DHCP rules).

Application control Premium feature

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 to 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. (for example, 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 riskier 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 the AP CLI, the below options are available to view the Application Statistics:

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

```
XV3-8-441BCC(config)# show application-statistics by-application
Applications Count = 24
Application Statistics for All Applications
```

Protocol or Application	Productivity Index	& Risk	TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4	1	4	220	3	231
Amazon	2	1	75	31437	69	8337
Bonjour	4	1	15	1737	14	1664
Doubleclick	1	1	84	30190	65	12228
Google Ads	3	1	103	47136	78	12223
Google Analytics	4	1	13	3750	15	1711
Google APIs	3	1	4713	6288091	892	153251
Google	3	1	2544	3248915	568	48664
Google Play	3	1	350	396456	181	15261
Mozilla	3	1	54	44708	48	5854
NetBIOS NS	1	3	0	0	12	936
NTP	1	3	2	152	2	152
OCSP	3	1	63	6404	71	5247
OpenX	1	1	32	8374	27	3507
Quantcast	1	1	14	4733	17	2341
Rapleaf	3	1	19	6745	19	2288
Reddit	3	1	1227	1477596	752	74695
Scorecard Research	1	1	26	5876	27	2748
SSDP	4	1	329	146086	20	4000
SSL	3	3	226	136435	176	22509
TCP	3	1	2376	1617471	1665	330377
Twitter	3	4	79	53301	68	7532
Wikipedia	3	3	19	3126	28	3873
YouTube	1	4	95	26393	99	12233

```
XV3-8-EC7708(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

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

File-Transfer 1 1 81 17881 0 0

Mail 3 1 1351 1057897 1318 155897

Messaging 2 2 633 245164 558 68508

Network-Monitoring 3 4 43 2580 1 60

Networking 3 1 51911 4422799 2524 1488418

Proxy 2 2 8637 7892737 6454 1008520

Social-Networking 2 3 52038 68131289 19772 2285979

Streaming-Media 2 3 15030 18700791 9156 1366044

Web-Services 2 2 38872 26757562 32219 7094216
```

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

```
XV3-8-EC7708(config)# show application-statistics by-application ssid 1

Applications Count = 79
```

```
Application Statistics for wlan index 1
================================================================================
Protocol or Productivity TX TX RX RX
Application Index & Risk Packets Bytes Packets Bytes
--------------------------------------------------------------------------------
-
Ad Analytics 4 1 221 113639 204 27874
Admeta 4 1 20 8577 17 3470
Aggregate Knowledge 4 1 72 25718 67 11423
Amazon 2 1 1245 773227 1307 413188
Amazon Web Services 1 2 2102 2543236 1522 111343
Amp 4 1 163 144673 157 16258
AOL Ads 3 1 21 11459 24 3769
Appier 4 1 39 13552 26 5046
AppNexus 1 1 172 72763 167 62363
Bing 3 1 17 8140 12 1175
Bluekai 1 1 35 13127 23 2856
Bonjour 4 1 0 0 1067 332560
Casale 3 1 97 36559 85 12244
CloudFlare 3 2 31 12537 20 2286
Captive Network Ass 2 1 18 1194 10 918
Connexity 3 1 22 13348 27 3954
Contextweb 4 1 81 41240 100 20963
Criteo 4 1 376 171618 396 60013
Crashlytics 1 1 74 29571 82 10660
Doubleclick 1 1 3549 2691946 2587 759544
DHCP 4 1 52 17212 0 0
Dotomi 4 1 59 21308 64 8324
Drawbridge 4 1 28 6164 23 4780
Facebook 2 1 6053 5188935 4732 1217723
Facebook Messages 2 2 202 71996 150 18393
Facebook Video 2 3 44585 61497202 14049 941942
Flurry 3 1 17 5694 27 15624
Font Awesome 4 1 94 98415 88 5341
gmail 3 1 1351 1057897 1318 155897
Google Ads 3 1 1356 903620 1066 123597
Google Analytics 4 1 475 165753 407 91298
Google APIs 3 1 5437 2829186 4775 1605169
```

```
GoogleDuo 4 1 84 22238 82 23226
Google 3 1 5381 3955811 4385 799374
Google Play 3 1 980 242763 880 254459
Google Video 2 2 0 0 20 23771
hotstar 1 4 100 64443 82 21328
HTTP 3 1 1184 371037 1100 173347
HTTP 2.0 3 1 1410 360603 1271 232993
HTTP VIDEO 3 2 3801 5360601 1841 105901
HWCDN 3 1 213 259756 200 12745
ICICI Bank 2 2 29 33613 21 2025
ICMP 3 4 5 300 1 60
Instagram 1 1 322 330979 242 33346
Krux 1 1 71 31719 53 6993
Lotame 1 1 109 63865 84 10168
MDNS 3 1 0 0 86 21324
Media Innovation Gr 3 1 45 14819 40 5662
Media Math 1 1 25 5413 8 1034
Mixpanel 3 1 451 139375 496 275463
NrData 4 1 371 56753 341 108525
NTP 1 3 1 76 1 76
OpenX 1 1 113 20680 86 12298
Outbrain 3 1 34 16363 46 6344
OwnerIQ 3 1 38 8977 29 5783
Paytm 2 3 2015 2201287 1177 146483
Psiphon 2 2 8562 7869967 6392 983509
PubMatic 3 1 331 103338 262 57072
Quantcast 1 1 47 23413 47 9495
Quic 3 1 0 0 817 1052805
Rapleaf 3 1 66 28602 65 8000
Rubicon Project 1 1 17 9524 24 7846
Scorecard Research 1 1 96 35762 90 12758
Smart AdServer 3 2 35 13345 45 6116
SpotXchange 3 2 59 14418 49 14522
SSDP 4 1 0 0 287 43911
SSL 3 3 6029 4347809 5173 1029629
Taboola 3 2 2177 2715316 1082 123164
TCP 3 1 169 37436 194 26160
```

```
The Trade Desk 3 1 101 67145 67 13168

Turn 1 1 71 31424 81 9438

Twitter 3 4 867 1040706 593 73816

UDP 3 1 0 0 62 10664

Ultrasurf 2 2 31 10286 19 1848

WhatsApp Media Mess 2 2 145 167080 135 10680

WhatsApp 2 2 404 55846 341 34602

Xiaomi 3 1 1244 718018 1376 285219

Yahoo 3 3 204 77608 251 48694

YouTube 1 4 11031 13254451 7129 1156065
```

- **Display for Station**: This gives detailed information about a particular station. Provide the station MAC address the user wants to check for statistics.
  - Tx means downlink traffic concerning AP and Rx mean uplink traffic with respect to AP.

```
XV3-8-441BCC(config)# show application-statistics by-application station  D4-6A-6A-E7-D0-15
Applications Count = 24
Application Statistics for station D4-6A-6A-E7-D0-15
================================================================================
Protocol or              Productivity     TX            TX          RX            RX
Application              Index & Risk   Packets        Bytes      Packets        Bytes
-------------------------------------------------------------------------------------
 Ad Analytics               4    1       4            220          3             231
 Amazon                     2    1       75           31437        69            8337
 Bonjour                    4    1       0            0            15            1810
 Doubleclick                1    1       84           30190        65            12228
 Google Ads                 3    1       103          47136        78            12223
 Google Analytics           4    1       13           3750         15            1711
 Google APIs                3    1       4713         6288091      892           153251
 Google                     3    1       2544         3248915      568           48664
 Google Play                3    1       387          404916       215           20326
 Mozilla                    3    1       117          67446        104           12051
 NetBIOS NS                 1    3       0            0            12            936
 NTP                        1    3       2            152          2             152
 OCSP                       3    1       63           6404         71            5247
 OpenX                      1    1       32           8374         27            3507
 Quantcast                  1    1       14           4733         17            2341
 Rapleaf                    3    1       19           6745         19            2288
 Reddit                     3    1       1235         1478487      761           77186
 Scorecard Research         1    1       26           5876         27            2748
 SSDP                       4    1       0            0            28            5600
 SSL                        3    3       226          136435       176           22509
 TCP                        3    1       2770         1675214      2075          424531
 Twitter                    3    4       79           53301        68            7532
 Wikipedia                  3    3       19           3126         28            3873
 YouTube                    1    4       113          32330        116           15918
```

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

```
XV3-8-441BCC(config)# show application-statistics debug

============Station Count 1========================================

     MAC                      IP                    VLAN      SSID
 D4-6A-6A-E7-D0-15        10.10.0.113                1     TIGER_XV3_8_OPEN_SSID

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

VLAN          STA_COUNT
 1               1
```

```
XV3-8-EC7708(config)# show application-statistics debug

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

MAC IP VLAN SSID

9A-FD-AA-B4-9C-8E 0.0.0.0 0

FC-D9-08-A4-D4-55 0.0.0.0 0

52-78-93-70-38-35 0.0.0.0 0

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

VLAN STA_COUNT

1 3
```

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

```
XV3-8-441BCC(config)# show application-statistics by-application vlan 1
Applications Count = 24
Application Statistics for VLAN 1
=================================================================================
Protocol or             Productivity     TX            TX         RX          RX
Application             Index & Risk    Packets       Bytes      Packets     Bytes
-------------------------------------------------------------------------------------
 Ad Analytics              4    1       4           220          3            231
 Amazon                    2    1       75          31437        69           8337
 Bonjour                   4    1       0           0            15           1810
 Doubleclick               1    1       84          30190        65           12228
 Google Ads                3    1       103         47136        78           12223
 Google Analytics          4    1       13          3750         15           1711
 Google APIs               3    1       4713        6288091      892          153251
 Google                    3    1       2544        3248915      568          48664
 Google Play               3    1       393         405374       221          20638
 Mozilla                   3    1       117         67446        104          12051
 NetBIOS NS                1    3       0           0            12           936
 NTP                       1    3       3           228          3            228
 OCSP                      3    1       63          6404         71           5247
 OpenX                     1    1       32          8374         27           3507
 Quantcast                 1    1       14          4733         17           2341
 Rapleaf                   3    1       19          6745         19           2288
 Reddit                    3    1       1249        1481150      779          79476
 Scorecard Research        1    1       26          5876         27           2748
 SSDP                      4    1       0           0            32           6400
 SSL                       3    3       226         136435       176          22509
 TCP                       3    1       2910        1694616      2219         455285
 Twitter                   3    4       79          53301        68           7532
 Wikipedia                 3    3       19          3126         28           3873
 YouTube                   1    4       115         32434        119          16137
```

```
XV3-8-EC7708(config)# show application-statistics by-application vlan 1
Applications Count = 79
Application Statistics for VLAN 1
================================================================================
Protocol or Productivity TX TX RX RX
Application Index & Risk Packets Bytes Packets Bytes
--------------------------------------------------------------------------------
-
Ad Analytics 4 1 221 113639 204 27874
Admeta 4 1 20 8577 17 3470
Aggregate Knowledge 4 1 72 25718 67 11423
Amazon 2 1 1245 773227 1307 413188
Amazon Web Services 1 2 2102 2543236 1522 111343
Amp 4 1 163 144673 157 16258
AOL Ads 3 1 21 11459 24 3769
Appier 4 1 39 13552 26 5046
AppNexus 1 1 172 72763 167 62363
Bing 3 1 17 8140 12 1175
Bluekai 1 1 35 13127 23 2856
Bonjour 4 1 0 0 1067 332560
Casale 3 1 97 36559 85 12244
CloudFlare 3 2 31 12537 20 2286
Captive Network Ass 2 1 18 1194 10 918
Connexity 3 1 22 13348 27 3954
Contextweb 4 1 81 41240 100 20963
Criteo 4 1 376 171618 396 60013
Crashlytics 1 1 74 29571 82 10660
Doubleclick 1 1 3549 2691946 2587 759544
DHCP 4 1 52 17212 0 0
Dotomi 4 1 59 21308 64 8324
Drawbridge 4 1 28 6164 23 4780
Facebook 2 1 6053 5188935 4732 1217723
Facebook Messages 2 2 202 71996 150 18393
Facebook Video 2 3 44585 61497202 14049 941942
Flurry 3 1 17 5694 27 15624
Font Awesome 4 1 94 98415 88 5341
gmail 3 1 1351 1057897 1318 155897
Google Ads 3 1 1356 903620 1066 123597
```

```
Google Analytics 4 1 475 165753 407 91298
Google APIs 3 1 5437 2829186 4775 1605169
GoogleDuo 4 1 84 22238 82 23226
Google 3 1 5381 3955811 4385 799374
Google Play 3 1 980 242763 880 254459
Google Video 2 2 0 0 20 23771
hotstar 1 4 100 64443 82 21328
HTTP 3 1 1184 371037 1100 173347
HTTP 2.0 3 1 1410 360603 1271 232993
HTTP VIDEO 3 2 3801 5360601 1841 105901
HWCDN 3 1 213 259756 200 12745
ICICI Bank 2 2 29 33613 21 2025
ICMP 3 4 5 300 1 60
Instagram 1 1 322 330979 242 33346
Krux 1 1 71 31719 53 6993
Lotame 1 1 109 63865 84 10168
MDNS 3 1 0 0 86 21324
Media Innovation Gr 3 1 45 14819 40 5662
Media Math 1 1 25 5413 8 1034
Mixpanel 3 1 451 139375 496 275463
NrData 4 1 371 56753 341 108525
NTP 1 3 1 76 1 76
OpenX 1 1 113 20680 86 12298
Outbrain 3 1 34 16363 46 6344
OwnerIQ 3 1 38 8977 29 5783
Paytm 2 3 2015 2201287 1177 146483
Psiphon 2 2 8562 7869967 6392 983509
PubMatic 3 1 331 103338 262 57072
Quantcast 1 1 47 23413 47 9495
Quic 3 1 0 0 817 1052805
Rapleaf 3 1 66 28602 65 8000
Rubicon Project 1 1 17 9524 24 7846
Scorecard Research 1 1 96 35762 90 12758
Smart AdServer 3 2 35 13345 45 6116
SpotXchange 3 2 59 14418 49 14522
SSDP 4 1 0 0 287 43911
SSL 3 3 6029 4347809 5173 1029629
```

```
Taboola 3 2 2177 2715316 1082 123164
TCP 3 1 169 37436 194 26160
The Trade Desk 3 1 101 67145 67 13168
Turn 1 1 71 31424 81 9438
Twitter 3 4 867 1040706 593 73816
UDP 3 1 0 0 62 10664
Ultrasurf 2 2 31 10286 19 1848
WhatsApp Media Mess 2 2 145 167080 135 10680
WhatsApp 2 2 404 55846 341 34602
Xiaomi 3 1 1244 718018 1376 285219
Yahoo 3 3 204 77608 251 48694
YouTube 1 4 11031 13254451 7129 1156065
```

- **Time fram**e: This gives information about the application seen in last the duration (for example, 1 day).
    - For low-risk numbers, the productivity is high and vice versa. (example, for GitHub (shown in the below figure) the risk index number is 1 and the productive index is 4, this means the application is low risk and more productive).

```
XV3-8-441BCC(config)# show application-statistics by-application time-frame 86000
Applications Count = 24
Application Statistics for All Applications
```

Protocol or Application	Productivity Index	Risk	TX Packets	TX Bytes	RX Packets	RX Bytes
Ad Analytics	4	1	4	220	3	231
Amazon	2	1	75	31437	69	8337
Bonjour	4	1	17	1956	15	1810
Doubleclick	1	1	84	30190	65	12228
Google Ads	3	1	103	47136	78	12223
Google Analytics	4	1	13	3750	15	1711
Google APIs	3	1	4713	6288091	892	153251
Google	3	1	2544	3248915	568	48664
Google Play	3	1	393	405374	221	20638
Mozilla	3	1	117	67446	104	12051
NetBIOS NS	1	3	0	0	12	936
NTP	1	3	3	228	3	228
OCSP	3	1	63	6404	71	5247
OpenX	1	1	32	8374	27	3507
Quantcast	1	1	14	4733	17	2341
Rapleaf	3	1	19	6745	19	2288
Reddit	3	1	1262	1482390	795	82476
Scorecard Research	1	1	26	5876	27	2748
SSDP	4	1	585	259542	36	7200
SSL	3	3	226	136435	176	22509
TCP	3	1	3006	1709704	2311	467655
Twitter	3	4	79	53301	68	7532
Wikipedia	3	3	19	3126	28	3873
YouTube	1	4	128	38033	130	19369

```
XV3-8-EC7708(config)# show application-statistics by-application time-frame 86000
Applications Count = 6
```

```
Application Statistics for All Applications
================================================================================
Protocol or Productivity TX TX RX RX
Application Index & Risk Packets Bytes Packets Bytes
--------------------------------------------------------------------------------
Bonjour 4 1 3599 704477 1067 332560
DHCP 4 1 76 25156 0 0
ICMP 3 4 43 2580 1 60
MDNS 3 1 4414 633504 86 21324
NetBIOS NS 1 3 4785 376002 0 0
UDP 3 1 38944 2648192 62 10664
XV3-8-EC7708(config)#
```

DPI CLI configuration

Users can enable Application Control globally by using the below commands:

To enable DPI support:

```
XV3-8-EC7708(config)# filter global-filter
XV3-8-EC7708(config-global-filter)# application-control
XV3-8-EC7708(config-global-filter)#
```

To disable DPI support:

```
XV3-8-EC7708(config)# filter global-filter
XV3-8-EC7708(config-global-filter)# no application-control
XV3-8-EC7708(config-global-filter)#
```

Global application policy

Per application policy

```
XV3-8-441BCC(config)# filter global-filter
XV3-8-441BCC(config-global-filter)# filter precedence 1
XV3-8-441BCC(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.cn
  914cg                 : 914CG
  9gag                  : 9GAG
  about                 : about.com
  abscbn                : ABS-CBN
  acas                  : ACA Services
  accweath              : accuweather.com
XV3-8-441BCC(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


XV3-8-441BCC(config-global-filter-precedence-1)# ication-control youtube permit

  permit                : Allow this Application
```

Set per category policy

```
XV3-8-EC7708(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
XV3-8-EC7708(config-global-filter-precedence-1)# category-control games permit
XV3-8-EC7708(config-global-filter-precedence-1)#
```

SSID application policy

```
XV3-8-EC7708(config)# filter filter-list 1
XV3-8-EC7708(config-filter-list-1)# filter precedence 1
XV3-8-EC7708(config-list-1-filter-precedence-1)# application-control facebook deny
XV3-8-EC7708(config-list-1-filter-precedence-1)#
XV3-8-EC7708(config-list-1-filter-precedence-1)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# filter-list 1
XV3-8-EC7708(config-wlan-1)#
```

CLI Configuration

```
!
filter  global-filter
  stateful
  application-control
  filter precedence 1
     category-control games permit
     exit

filter  filter-list  1
  filter precedence 1
     application-control facebook deny
     exit
!
lldp
lldp tx-interval 100
power policy sufficient
logging syslog 7
!
XV3-8-441BCC(config-filter-list-1)#
```

Chapter 10: Wireless Intrusion Detection Systems (WIDS) Premium feature

Wireless flood detection

A flood attack happens when a rogue client sends a huge number of packets of a specific type to the AP to disrupt the normal working of the AP. This feature can detect the following five types of flood attacks:

- Association
- Authentication
- Disassociation
- Deauthentication
- Extensible Authentication Protocol over LAN (EAPoL)

CLI configuration:

```
XV3-8-EC7708(config)# wids
association-flood : Detect floods of client associations from clients
authentication-flood : Detect floods of client authentication from clients
deauthentication-flood : Detect floods of clients deauthentications from clients
disassociation-flood : Detect floods of client disassociations from clients
eap-flood : Detect floods of EAP messages from clients
num-of-minutes : Configure time duration for flood detection
num-of-packets : Configure threshold of flood packets
```

Neighbour/Rogue AP detection

The AP can detect all neighbour APs and Rogue APs. To enable Neighbour/Rogue AP detection, refer to Security section.

By default, all Neighbours/Rogue APs in the home channel are detected. To detect Neighbours/Rogue APs in all channels, go to **Radio** > **Basic** > **Off Channel Scan** and click **Enable** checkbox.

Note

Off Channel Scan is not required for XV3-8 platforms because they have inbuilt Radio for monitoring.

Ad Hoc network detection

A wireless Ad Hoc network is a type of Local Area Network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or AP.

CLI configuration:

To enable Ad Hoc network detection

```
XV3-8-EC7708(config)# wids
ad-hoc-detection : Detect ad-hoc networks
```

To display Ad Hoc networks

```
XV3-8-EC7708(config)# show wireless adhoc-networks
```

Chapter 11: Configuring Services

This chapter describes the following topics:

Overview

This chapter gives an overview of Enterprise Wi-Fi AP configurable parameters related to User Groups, Location API, Speed Test, BT Location API, Bonjour Gateway, LACP, and RTLS.

Configuring services

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

User Groups **Premium feature**

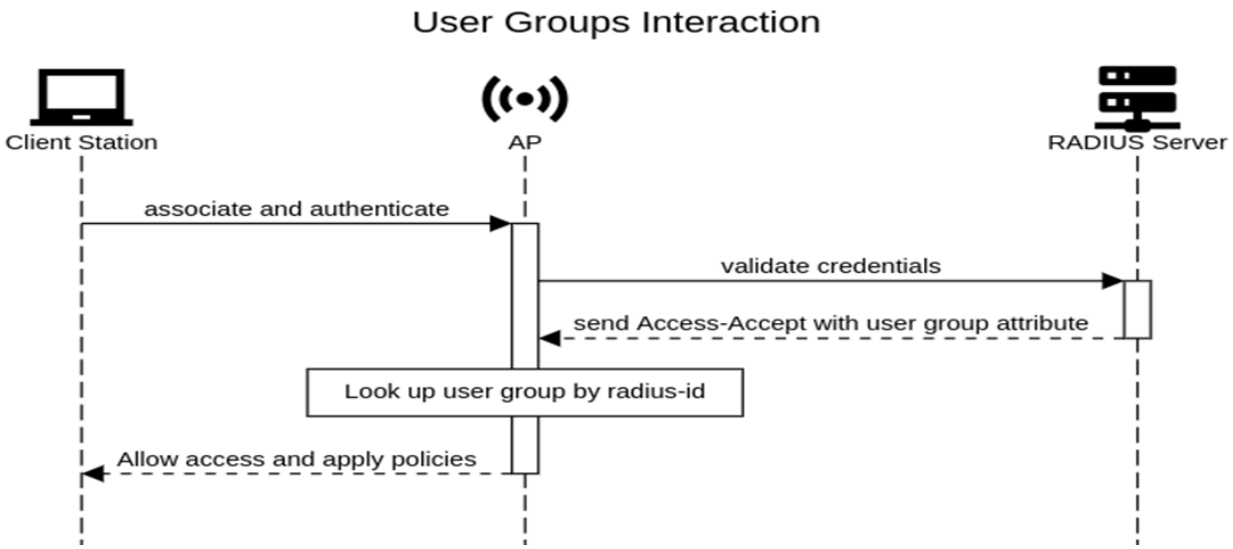
Some policies, like VLAN, require many RADIUS attributes to be sent by the RADIUS server and processed by the AP. Some wireless network administrators do not have administrative access to the RADIUS server, so making changes to wireless policies would require waiting for the RADIUS administrator to make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

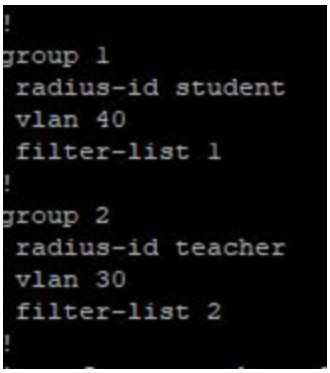
Figure 54: *User Groups interaction*



CLI Configuration:

```
XV3-8-EC7708(config)# group
Specify user group number <1-16>
XV3-8-EC7708(config)# group 1
XV3-8-EC7708(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-EC7708(config-group-1)#
```

Example:



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

Location API

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

Below table lists the fields that are displayed in the **Configuration > Services > Location API** tab.

Table 53: Location API parameters

Parameters	Description	Range	Default
Enable	Provision to enable/disable Location API services.	-	-
Server	Provision to configure HTTP/HTTPS server to send a report with the pot number.	0-65535	-

Parameters	Description	Range	Default
Interval	Provision to configure the custom frequency of information to be shared on server.	2-3600	-
MAC Anonymization	Avoid populating locally administrated MAC addresses in the Location API client list.	-	-

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

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

Figure 55: *Location API parameters*

Note

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

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 APs or between Enterprise Wi-Fi APs and other third-party devices (or PC) that is having zapwireless endpoint running.

Refer to https://code.google.com/archive/p/zapwireless/ to download the zap wireless 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 Enterprise Wi-Fi AP through UI shown below.

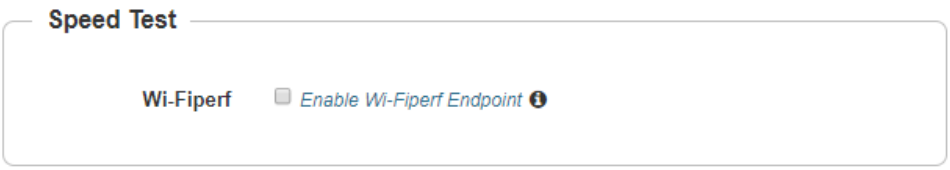
Table 54 lists the fields that are displayed in the **Configuration > Services > Speed Test** tab.

Table 54: 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 56: *Speed Test parameters*



DHCP Option-82

DHCP Option 82 parameter enabled at the device level with VLAN IDs inserts the Option 82 parameters in all the DHCP client packets leaving the configured VLAN interfaces. This device-level configuration precedes the DHCP Option 82 configuration at the WLAN profile or the L3 interface levels.

In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered:

1. Device-level configuration
2. WLAN profile-level configuration
3. L3 interface-level configuration

The device-level configuration is recommended when it is desired to insert the DHCP Option 82 for the following options:

- Guest access enabled wired traffic
- Guest and without guest access enabled wireless DHCP client traffic

To configure the above parameter, navigate to the **Configure > Services > Network** tab and provide the details in the **DHCP Option 82** section:

1. Select the **Enable** checkbox.
2. Select the circuit ID from the **Option 82 Circuit ID** drop-down list.

   Following are the supported values:

   - **None**
   - **All**
   - **Hostname**
   - **APMAC**

- SSID
- VLANID
- SITEID
- Custom

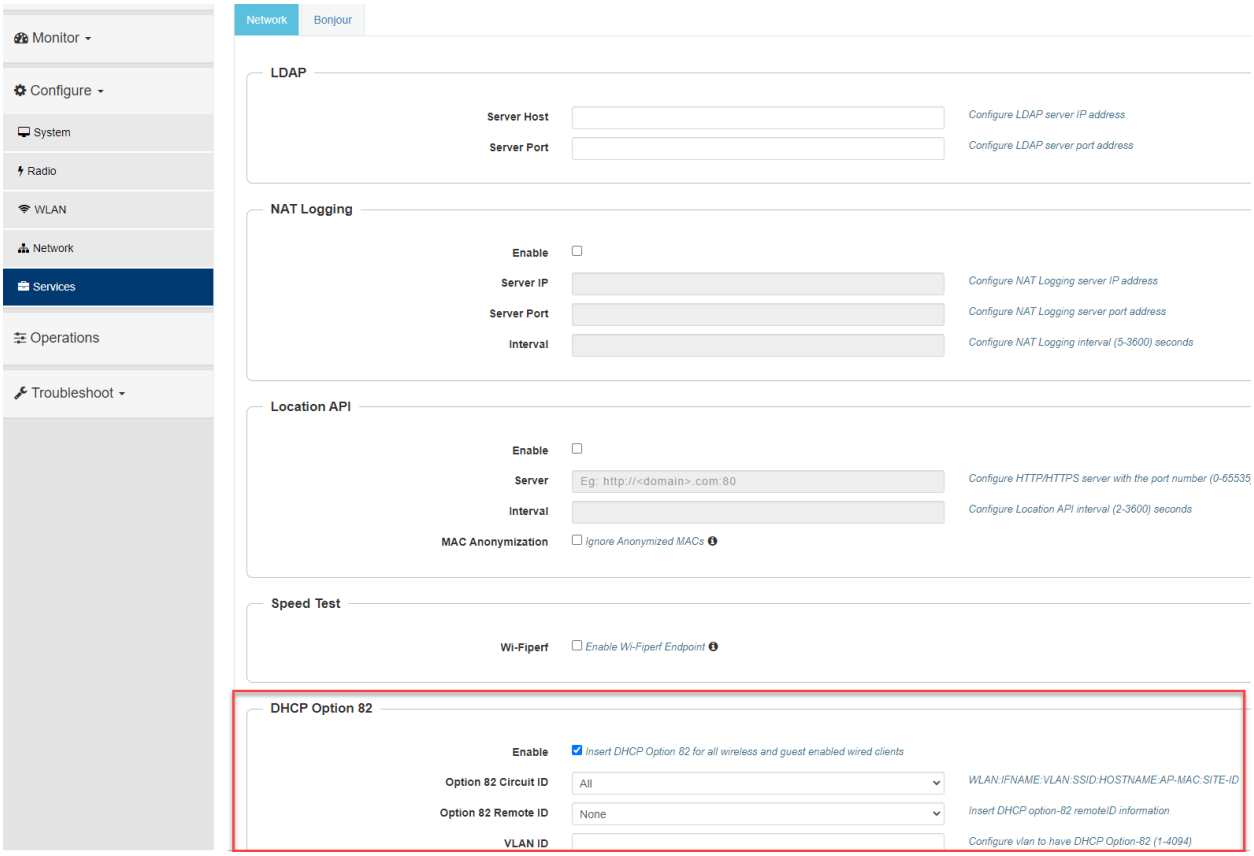
3. Select the remote ID from the **Option 82 Remote ID** drop-down list.

   Following are the supported values:

   - None
   - Hostname
   - APMAC
   - SSID
   - VLANID
   - SITEID
   - Custom

4. Enter the VLAN ID in the **VLAN ID** text box.
5. Click **Save**.

Figure 57: *DHCP Option 82 parameter*



BT location API

XV3-8/XV2-2T APs with an integrated Bluetooth Low Energy (BLE) radio can detect and locate nearby BLE devices. This data is then provided via API to third-party applications. Examples of such devices include smartwatches, battery-based beacons, Apple iBeacons, fitness monitors, and remote sensors.

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

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

Table 55: BT Location API parameters

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

Sending report

After enabling BLE Scanning on AP it will start processing:

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

To configure the BT Location-API in the CLI:

```
XV3-8-EC7708(config)# location-api
ignore-anonymized-mac : Ignore MAC addresses that are anonymized
interval : Configure reporting interval in secs
server : HTTP/HTTPS server to send report to with the port number
```

To disable the BT Location-API:

```
XV3-8-EC7708(config)# no location-bt-api
```

BT Location API data elements

Table 56: BT Location API data elements

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

HTTP POST body format:

```
{
u'ap_mac': '00-04-56-A5-5A-EC',
'version': '2.2',
'ap_name': 'XV3-8-EC7708',
'ble_discoverd_clients':{Array of 0-250 devices}
}
Bluetooth API Data Format
{
bt_rssi': u' -80 dBm ',
bt_mac': 14-8F-21-FD-37-18', u
'bt_uuids': Garmin International, Inc. (0xfe1f)\n',
'bt_timestamp': u' 1.811127'
}
```

Bonjour Gateway

Bonjour enables the automatic discovery of devices such as printers, file servers, and other clients and services on a local network. Bonjour Gateway feature on Wi-Fi AP extends the scope of bonjour service beyond the local network by forwarding bonjour Multicast DNS (mDNS) packet across different VLANS, to make bonjour services/devices available between the different wireless/local networks.

Below table lists the fields that are displayed in the **Configuration > Services > Bonjour** tab.

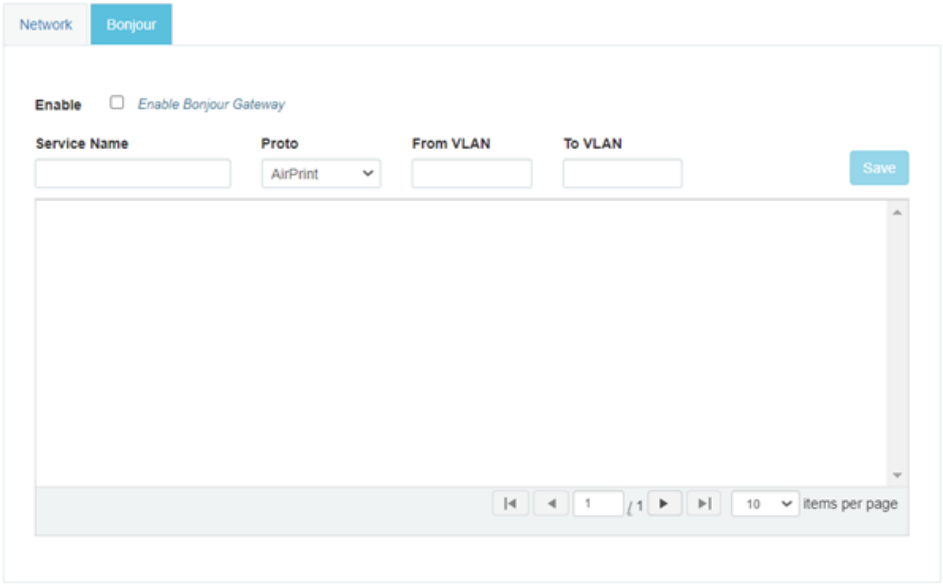
Table 57: Bonjour Gateway parameters

Parameters	Description	Range	Default
Enable	Provision to enable/disable Bonjour Gateway services.	-	-
Service Name	Provision for user-defined bonjour rule name.	-	-
Proto	Select the required mDNS protocol.	-	-
From VLAN	VLAN in which mDNS/Bonjour service is running.	-	-
To VLAN	VLAN in which clients are listening.	-	-

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

1. Select the **Enable** checkbox to enable Bonjour Gateway.
2. Enter the **Service Name** in the textbox.
3. Select **Proto** type from the drop-down list.
4. Select **From VLAN** and **To VLAN** from the drop-down list.
5. Click **Save**.

Figure 58: *Bonjour parameter*



CLI Configuration:

1. Enable Bonjour Gateway on AP.

```
XV3-8-EC7708(config)# bonjour-gw
```

2. To configure Bonjour rule.

```
XV3-8-EC7708(config)# bonjour-fw rules

bonjour-fw rules <sname> <proto> <vidfrom> <vidto>
```

3. To control mDNS repeated packet to WAN side.

```
XV3-8-EC7708(config)# bonjour-fw bonjour-forward-to-wan

all : Forward all bonjour mdns packets queries and response repeated with vlan to
WAN side

queries : Forward bonjour mdns Query packets repeated with vlan to WAN side

responses : Forward bonjour mdns Response packets repeated with vlan to WAN side
```

Note

1. By default, mDNS repeated will not send to the WAN side.
2. WAN side indicates Eth 1 interface, Mesh client interface in case of mesh client mode, tunnel interfaces like L2GRE, and L2TP.

Link Aggregation Control Protocol (LACP)

LACP provides the ability to group multiple physical ports as a logical port. This logical port is referred to as port-channel and supported only on XV3-8 devices. LACP is a dynamic protocol used to form and maintain the Link aggregation between two LACP supported devices.

LACP provides the following benefits:

- Increased Bandwidth: traffic may be balanced across the member ports to provide increased aggregate throughput.
- Link redundancy: the LACP bundle can survive the loss of one or more member links.

Configuration:

To add Ethernet to port channels:

```
XV3-8-EC7708(config)# interface portchannel 1
XV3-8-EC7708(config-portchannel-1)# exit
XV3-8-EC7708(config)# interface eth 1
XV3-8-EC7708(config-eth-1)# channel-group 1
XV3-8-EC7708(config-eth-1)# exit
XV3-8-EC7708(config)# interface eth 2
XV3-8-EC7708(config-eth-2)# channel-group 1
XV3-8-EC7708(config-eth-2)#
```

Port-channel configuration:

```
XV3-8-EC7708(config)# interface portchannel 1
XV3-8-EC7708(config-portchannel-1)#
advertise : Ethernet link speed advertisement
channel-group : Ethernet member channel group
clear : Clear command
duplex : Ethernet link duplex
shutdown : Shutdown interface
speed : Ethernet link speed
switchport : Configure switch port
tunnel-mode : Enable tunnelling of wired traffic over configured tunnel
apply : Apply configuration that has just been set
exit : Exit from interface configuration
no : Disable parameters
save : Save configuration to Flash so it persists across reboots
show : Show command
```

Syntax:

```
XV3-8-EC7708(config)# interface portchannel 1
XV3-8-EC7708(config-portchannel-1)# switchport mode trunk
XV3-8-EC7708(config-portchannel-1)# switchport trunk allowed vlan 1
XV3-8-EC7708(config-portchannel-1)# switchport trunk native vlan 1
XV3-8-EC7708(config-portchannel-1)#
```

Real Time Location System (RTLS)

Stanley AeroScout Location Engine **Premium feature**

The Location Engine delivers accurate and reliable location data for assets and customers with STANLEY Healthcare Wi-Fi tags. It is an integral component of STANLEY Healthcare's AeroScout RTLS solutions. The AeroScout Location Engine determines location using signal strength measurements (RSSI) collected by the Cambium Wi-Fi Access Points, that can simultaneously serve location sensors and provide network access. AeroScout utilizes a location engine to determine the position of Wi-Fi tags.

From Release 6.4 onwards, Bluetooth (BLE) tags are supported on XV3-8 and XV2-2T devices.

CLI Configuration:

```
XV3-8-EC7708(config)# rtls aeroscout
ble-tag : Enable Aeroscout BLE Tag
server : Configure Aeroscout Server IP or FQDN
server-port : Configure Aeroscout Server Port (Default port:12092)
wifi-tag : Enable Aeroscout WiFi Tag
```

Chapter 12: Operations

This chapter describes the following topics:

Overview

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

Firmware upgrade

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 58 lists the fields that are displayed in the **Operations > Firmware** update tab.

Table 58: Firmware update parameters

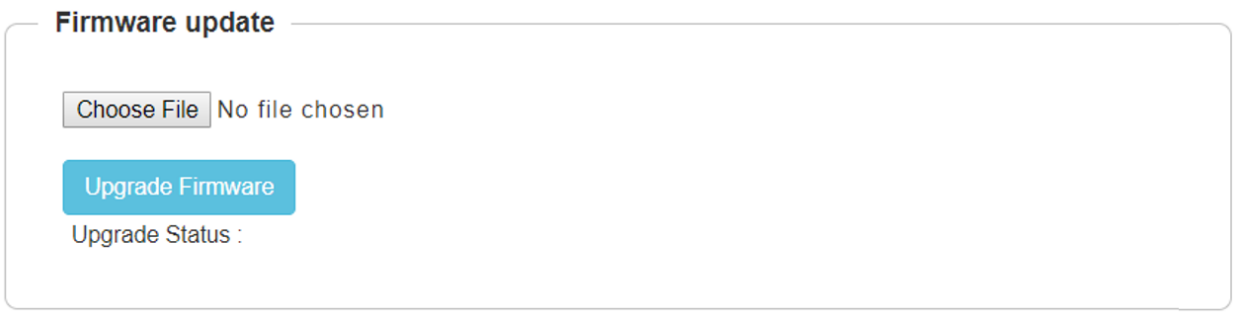
Parameters	Description	Range	Default
Choose File	Provisions to select upgrade files.	–	–
Upgrade Firmware	Provision to initiate upgrade once the file is selected.	–	–

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 the upgrade in the **Upgrade Status** field.

Figure 59: *Firmware update parameters*



System

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

Table 59 lists the fields that are displayed in the **Operations > System** tab:

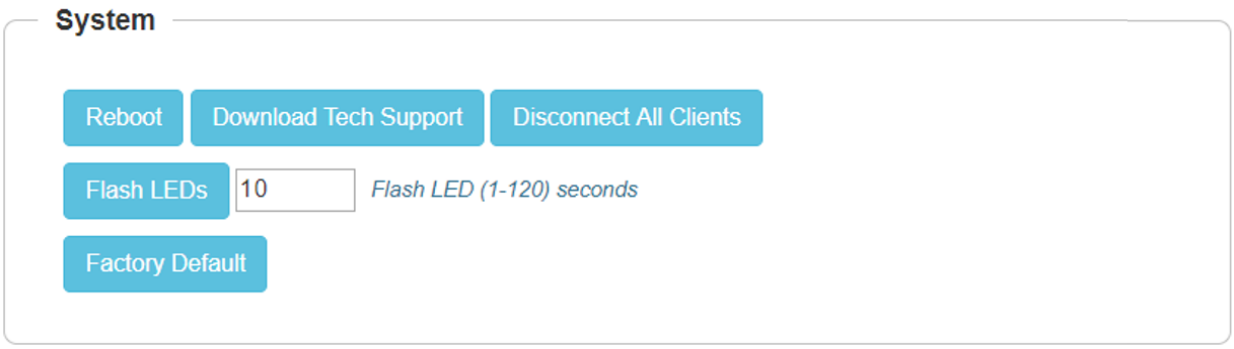
Table 59: System parameters

Parameters	Description	Range	Default
Reboot	Users will be prompted with a Reboot pop-up requesting a reboot. If yes, the device will go for a reboot.	–	–
Download Tech Support	Users will be prompted with permission to download tech support from AP. If yes, the 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 a de-authentication packet to each client connected to the radios.	–	–
Flash LEDs	LEDs on the device will toggle for the configured time period.	1-120	10
Factory Default	A pop-up window appears requesting confirmation for factory defaults. If yes, the device will delete all configurations to factory reset and reboot.	–	–

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

1. Click **Reboot** for rebooting the device.
2. Click **Download Tech Support** to generate tech support 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 configurations on the device.

Figure 60: *System parameters*



LED Test flashing pattern

The LED test flashing pattern for the Enterprise Wi-Fi 6 AP is as follows:

Flashing pattern (For XV3-8, XV2-2, XV2-2T0, XV2-2T1, XE5-8, and XE3-4): **Yellow** -> **Green** -> **Amber** -> **Blue**

Flashing pattern (For XV2-21X, XV2-23T, and XV2-22H): **Green** -> **Amber** -> **Blue**

CLI commands:

```
XV3-8-EC7708(config)# service flash-leds
Number of seconds to flash <1-120> (optional: default 10sec)
XV3-8-EC7708(config)# service test leds
```

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.

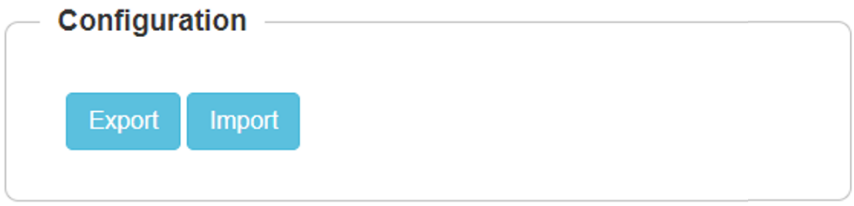
Figure 61: *Configuration parameters*

Parameters	Description	Range	Default
Export	Provision to export the configuration of the device to default download path configured on the system.	–	–
Import	Provision to import the configuration of the 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 62: *Configuration parameters*



Chapter 13: Troubleshoot

Overview

This chapter 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

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

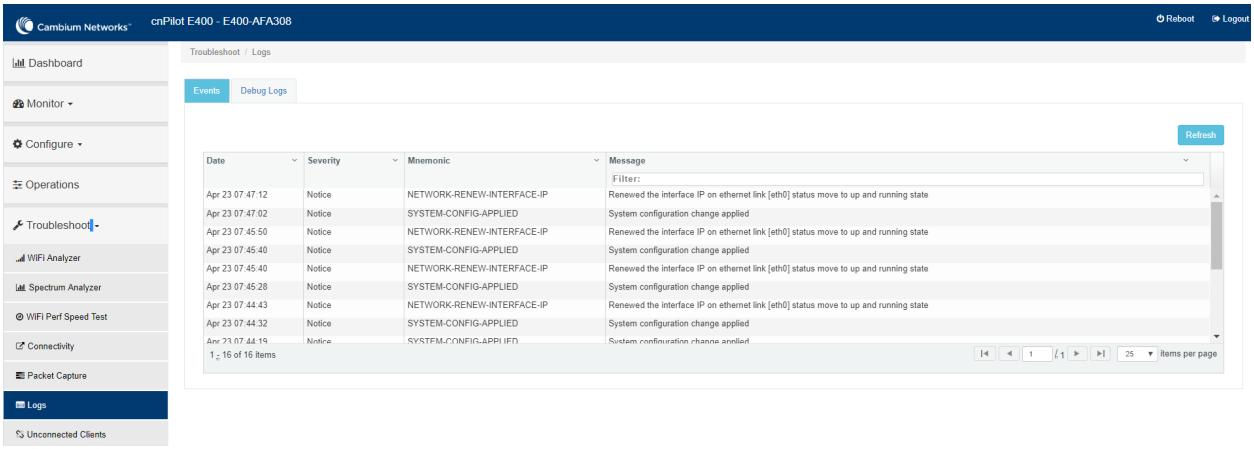
Events

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

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

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

Figure 63: *Events parameters*

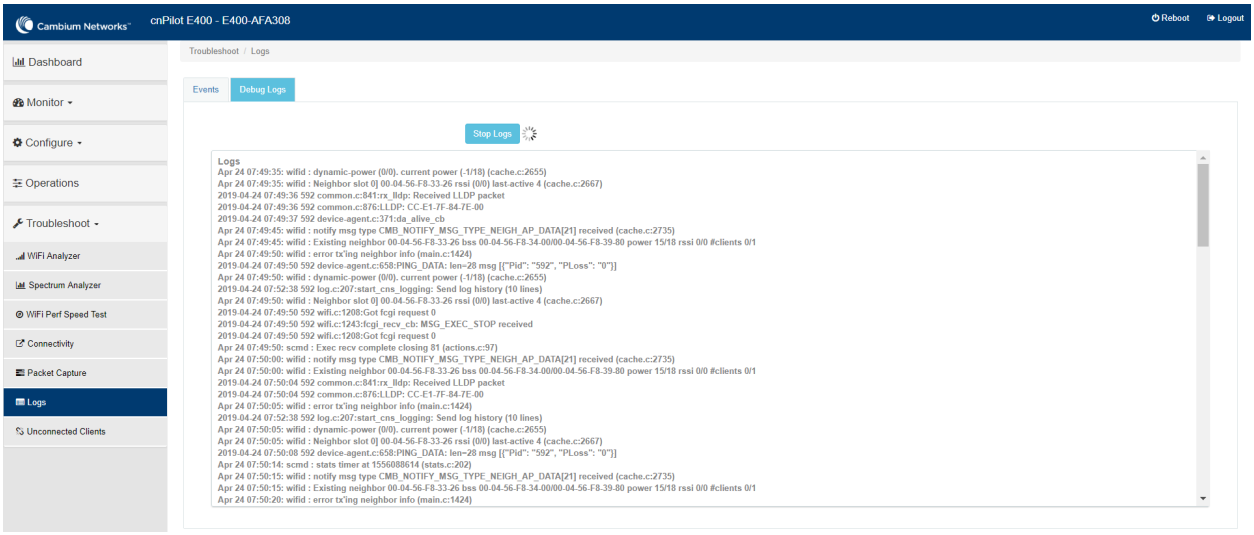


Debug Logs

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 the user clicks **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** tab.

Figure 64: *Debug Logs parameters*



Radio Frequency (RF)

Wi-Fi Analyzer

This tool provisions customers 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 about each channel as below:

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

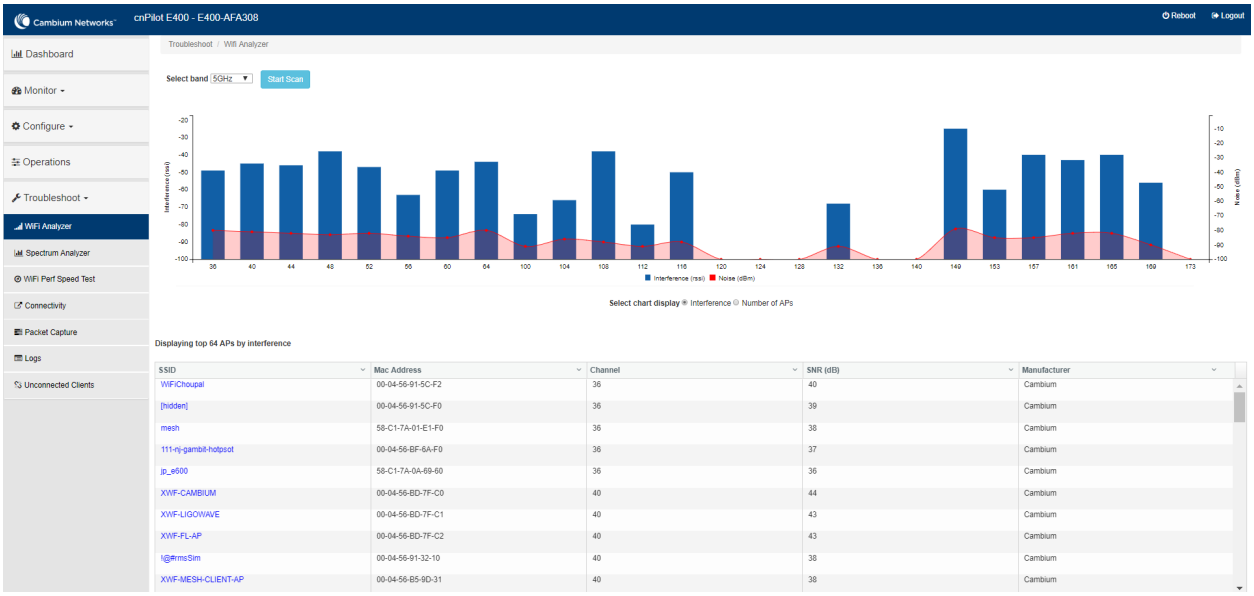
- Number of APs

This tool shares more information about each channel as below:

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

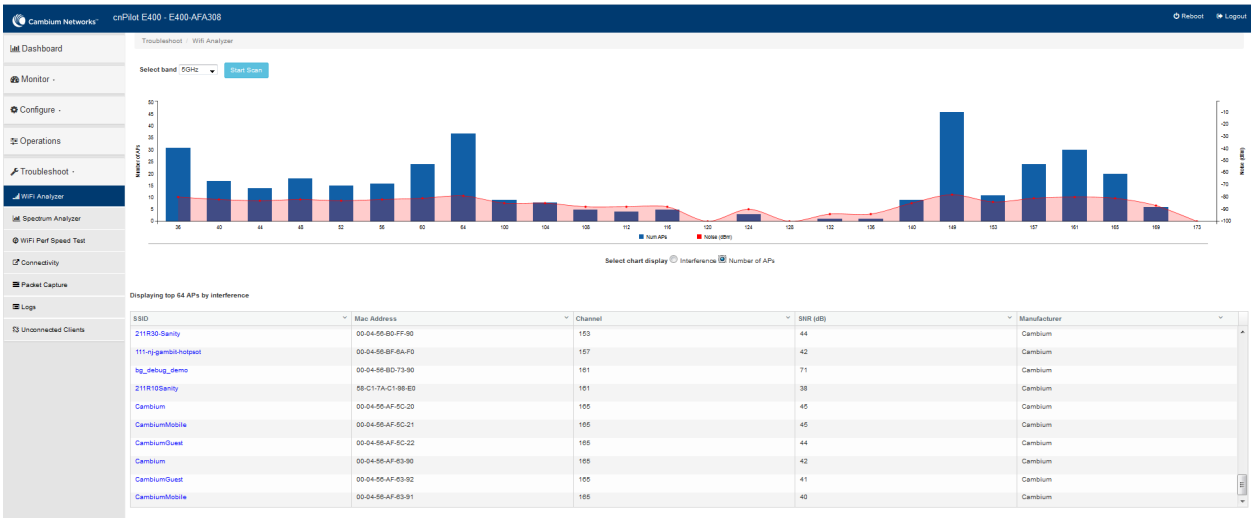
Channel analyzer is available at **Troubleshoot > Wi-Fi Analyzer > Interference Mode**.

Figure 65: *Interference Mode*



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

Figure 66: *Troubleshoot > Wi-Fi Analyzer > Number of APs Mode*



Packet capture

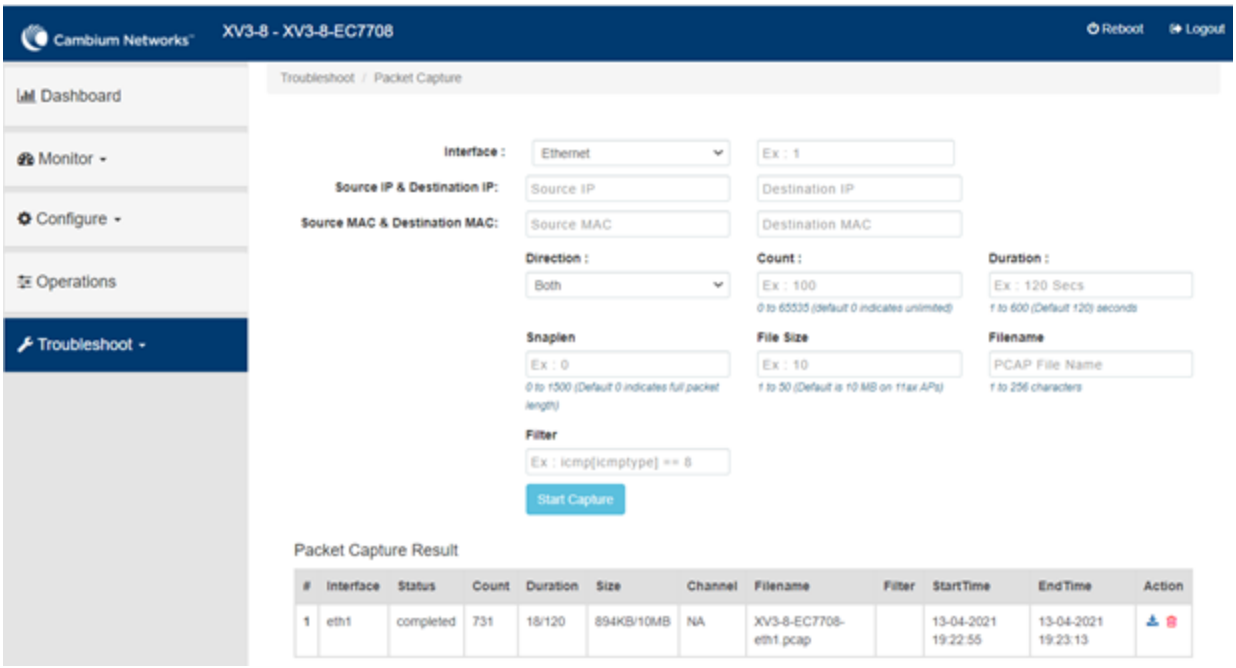
Allows the administrator to capture packets from the APs UI, cnMaestro UI, or XMS-Cloud. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, and port number. The user can trigger packet capture on one or more interfaces, simultaneously view the progress of the capture. The user can also download the captured pcap file on completion.

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

- Ethernet
- Radio
- Wireless LAN
- VLAN
- SSID
- TUNNEL
- BRIDGE

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

Figure 67: *Packet Capture page*



Performance

Speedtest on Access Point

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

Configuration:

Syntax:

```
XV3-8-EC7708(config)# speedtest etsi
<server url> <download MB> <upload MB> [simultaneous connections] [mbps]
```

Example:

```
XV3-8-EC7708(config)# speedtest etsi 10.110.211.19:9000 200 200
Your IP is 10.110.240.202 - private IPv4 access
Latency: 14.5ms Jitter: 1.3ms
Download: 169.53Mbps Upload: 93.93Mbps
```

Connectivity

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

- Ping
- DNS Lookup
- Traceroute

Table 60: Troubleshoot: Connectivity

Parameters	Description	Range	Default
Ping			
IP Address or Hostname	Provide IPv4 address or Hostname to validate the reachability of the destined Host.	-	-
Number of Packets	Provide a number of request packets that are required to be transmitted to validate the reachability of the 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 IPs that are associated with configured Hostname.	-	-
Traceroute			
IP Address or Hostname	Provide IPv4 address or Hostname to validate the reachability of the destined Host.	-	-
Fragmentation	Provision to allow or deny fragment packets.	-	Off
Trace Method	Provision to configure payload mechanism to check the reachability of destined IPv4/Hostname.	-	ICMP Echo
Display TTL	Provision to customize TTL display.	-	On
Verbose	Provision to display the output of traceroute.	-	On
Traceroute Result	Displays the output of the 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 text box.
3. Enter the **Number of Packets** in the text box.
4. Select **Buffer Size** value from the drop-down list.
5. Click **Start Ping**.

To configure **DNS Lookup**:

1. Enter the **Hostname** in the text box.
2. Click **DNS Test**.

To configure Traceroute:

1. Enter **IP address** or **Hostname** in the text box.
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 68: *Connectivity (Ping) parameters*

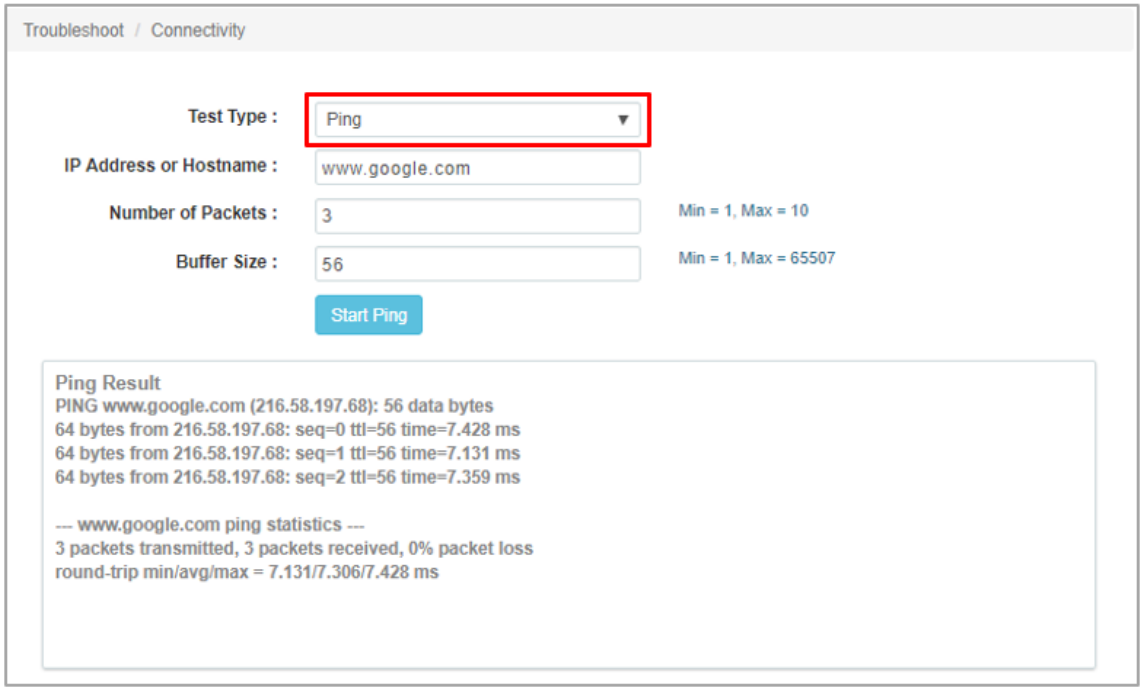


Figure 69: *Connectivity (DNS Lookup) parameters*

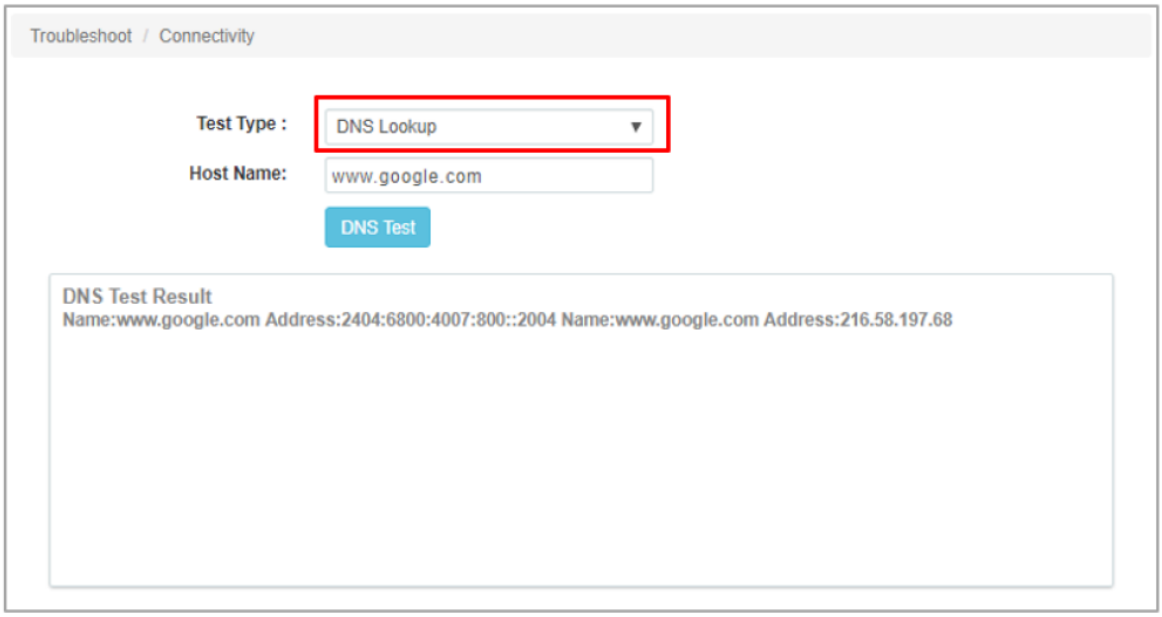
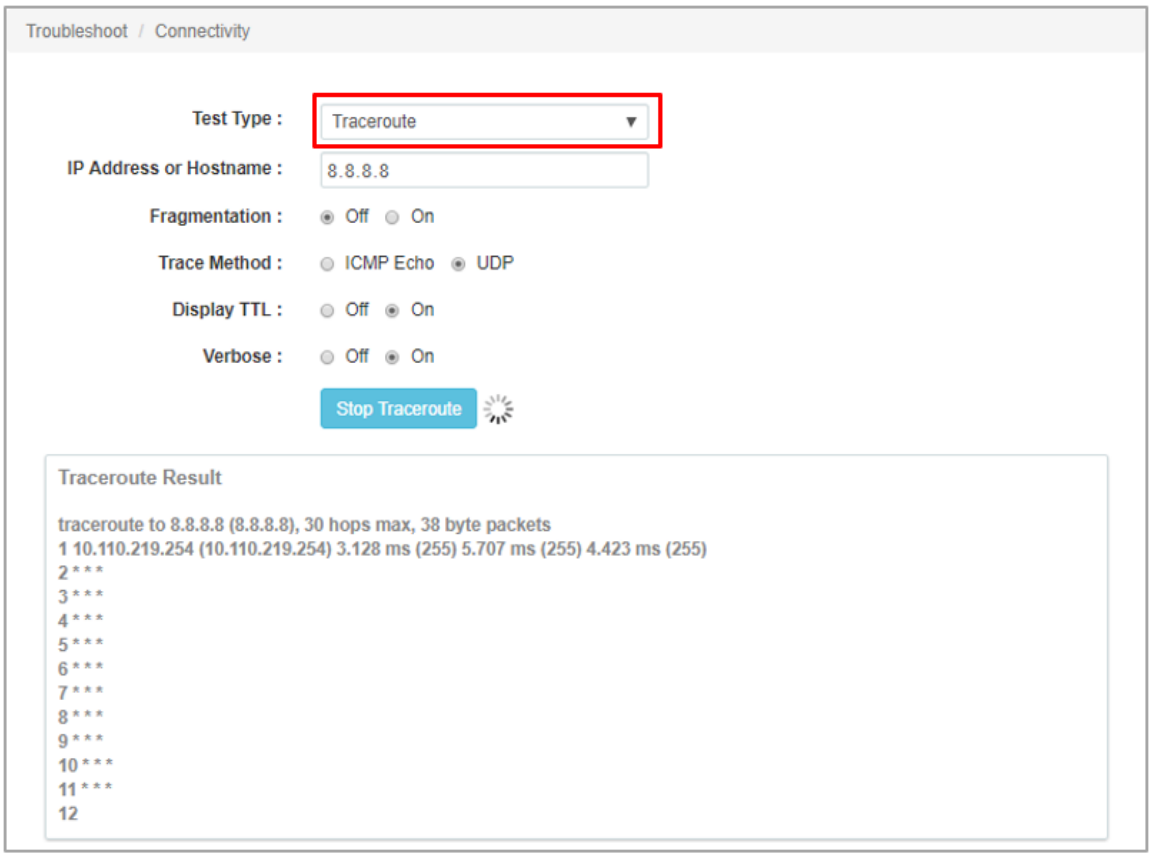


Figure 70: *Connectivity (Traceroute) parameters*



XIRCON tool 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. These are 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 Release 6.2, Enterprise Wi-Fi 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.

XIRCON tool support for Linux 1.0.0.40

XIRCON tool support for Linux 1.0.0.40 has been added which is used to discover APs in the network If the IP address is not known.

Chapter 14: 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

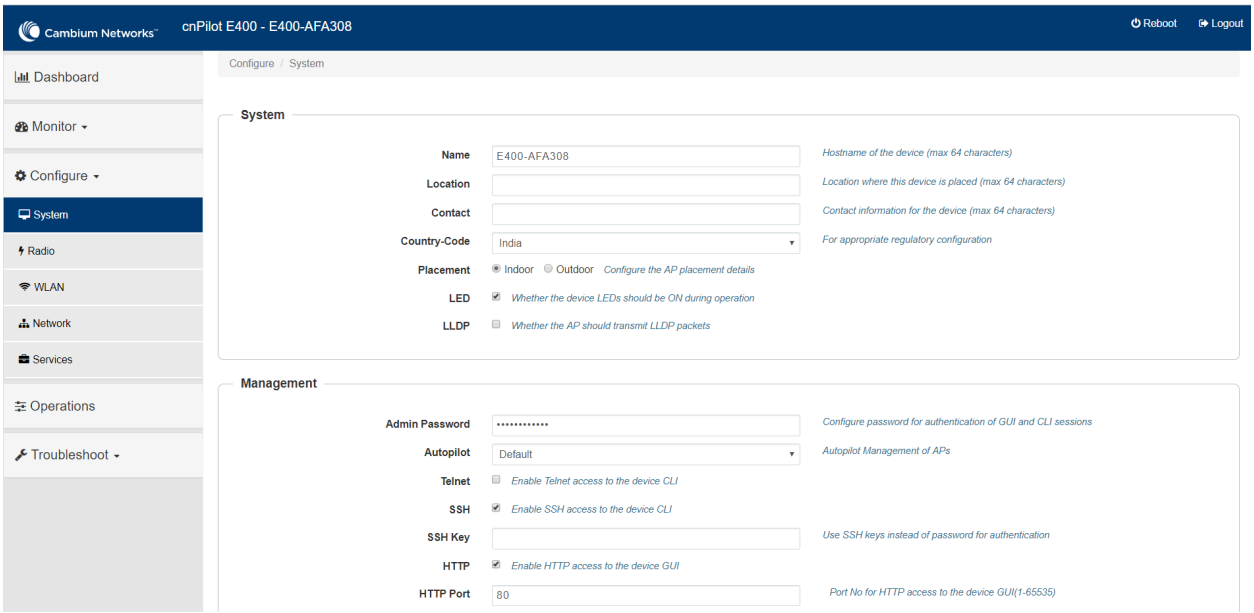
This is the default authentication mode enabled on the device. Only one username is supported which is “admin”. The default password for the “admin” username is “admin”. The user has a provision to configure/update password.

Device configuration

The below figure shows how to configure/update the default password of the admin user.

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

Figure 71: *Configure/update default password of the admin user*



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 users 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

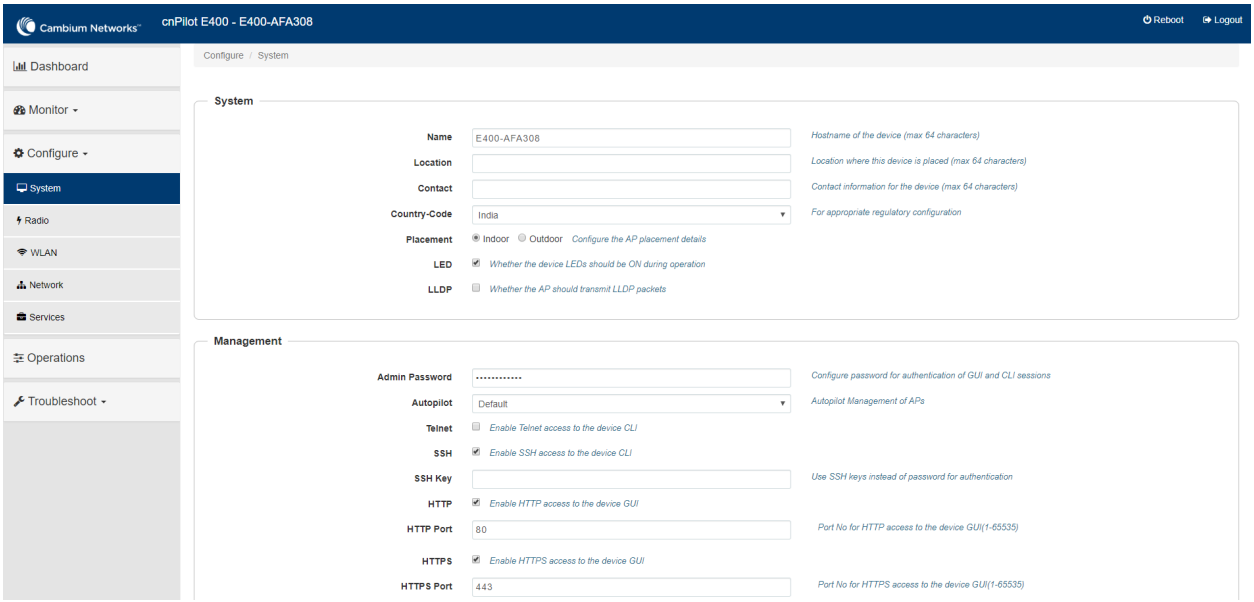
machine of the user and a public key, which is stored to any remote machine (AP) the user wants to connect. So, whenever a user initiates an SSH connection with a remote machine, SSH first checks if the user has a private key that matches any of the public keys in the remote machine and if not, it prompts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

Device configuration

SSH Key-based access method can be configured on the 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 72: *Management parameters*



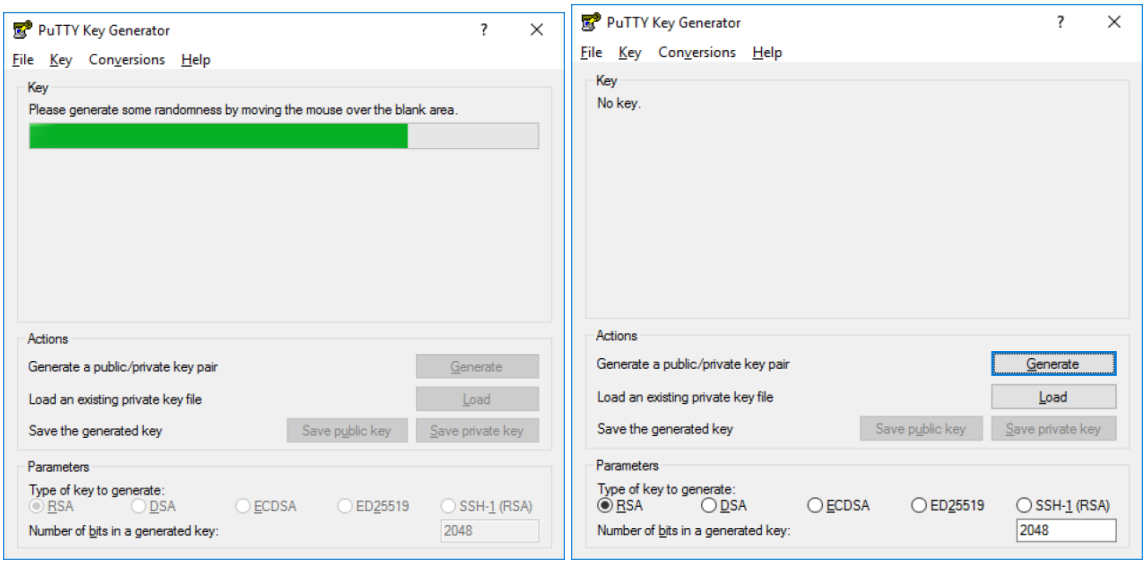
SSH Key generation

Windows

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

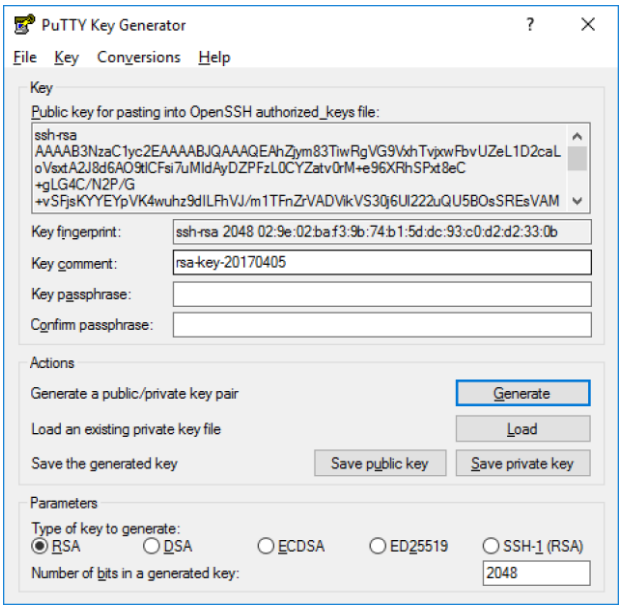
1. Generate a key pair in PUTTY Key Generator as shown in Chapter 14.

Figure 73: *Generating public/private Key*



2. Save the Public key and Private key once the key pair is generated as shown in Chapter 14.

Figure 74: *Public and Private Key*



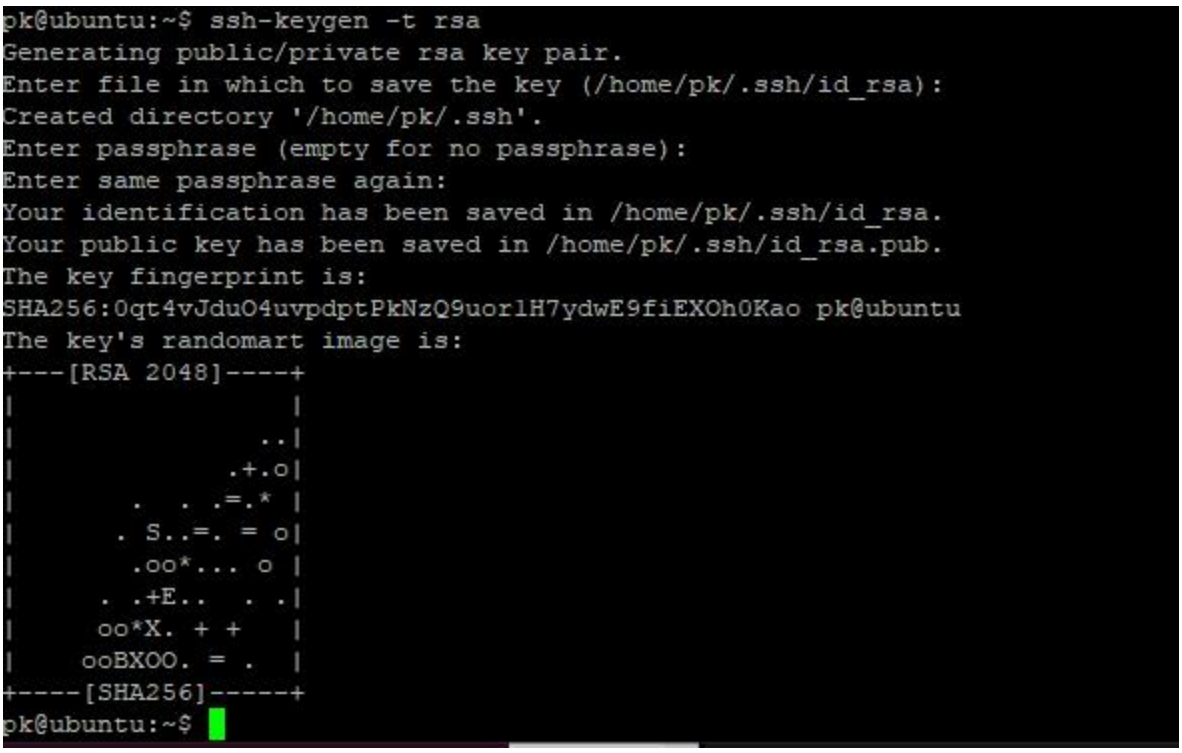
3. Save the Public key generated in the step above as described in Device configuration section.
4. Login to device using Private key generated above with username as “admin”.

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 Chapter 14.

Figure 75: *Public Key location path*



2. The Public key is now located in PATH mentioned in Chapter 14.

   PATH = “Enter the file to which to save the key”

3. The private key (identification) is now saved in PATH as mentioned in Figure 76.

   PATH = “Your identification has saved in <>”

Figure 76: *Private Key saved path*

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

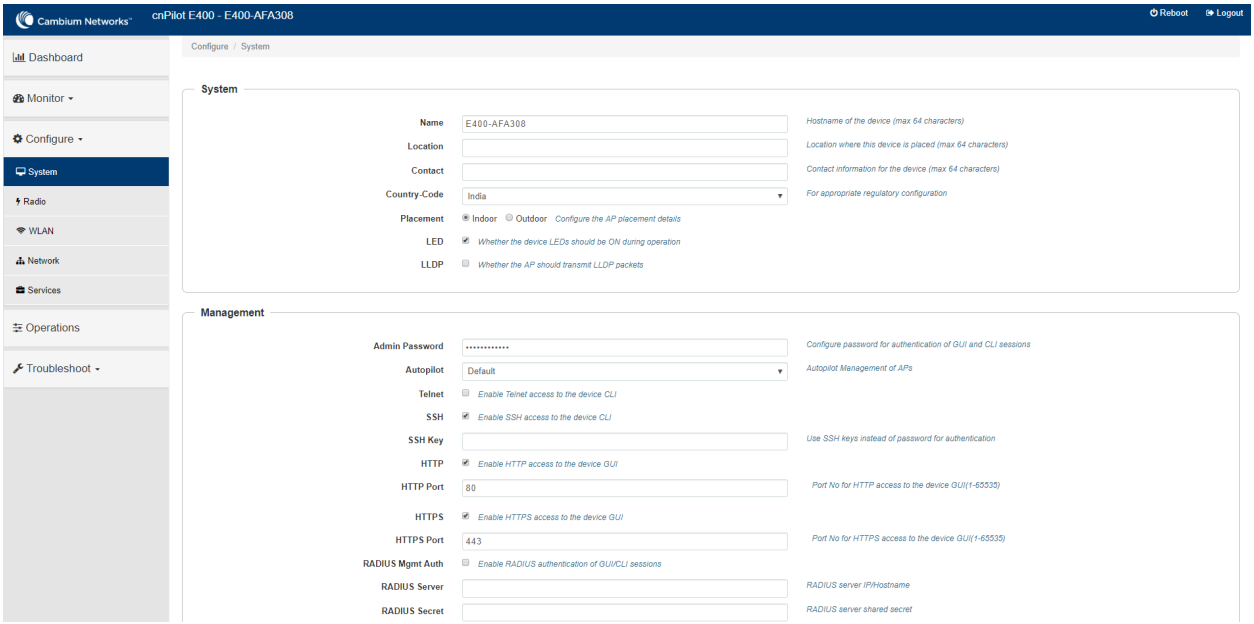
Device management access using RADIUS authentication allows multiple users to access using unique credentials and is secured.

Device configuration

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

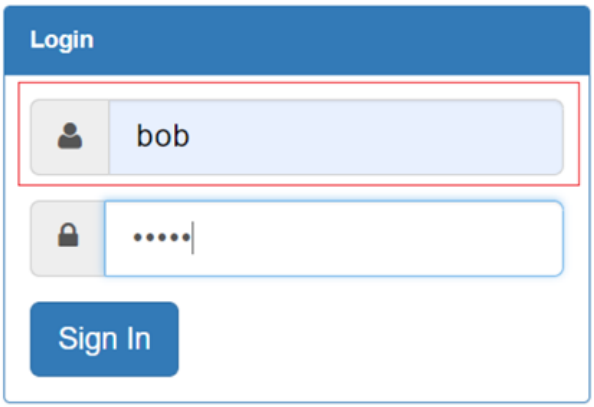
1. Enable **RADIUS Mgmt Auth** checkbox.
2. Configure **RADIUS IPv4/Hostname** and shared secret in **RADIUS Server** and **RADIUS Secret** parameters respectively.
3. Click **Save**.

Figure 77: *RADIUS Server and RADIUS Secret parameters*



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

Figure 78: *UI Login page*



Chapter 15: Mesh

From Release 6.4 onwards, Enterprise Wi-Fi 6 Access Point supports mesh connections between radios. Even though multiple mesh hop is supported in Release 6.4, the suggested maximum hops are two. Mesh links can form between radios of the same band of operation (2.4 GHz, 5 GHz, and 6 GHz), but the two peers of the mesh link do not have to be of the same AP type. For example, a link between Wi-Fi 6 XV2-2 and XV3-8 is supported. Given the larger set of available channels and typically cleaner RF environment, Cambium Networks recommends using the 6 GHz radio for mesh backhaul if the AP is 6 GHz-capable, else use the 5 GHz band.

A mesh link can be created between two radios by configuring one of them as a Base and the other as a Client on the first WLAN of the AP. Typically, the wired connectivity AP would be configured as a Mesh Base (MB). The radio setup for the MB selects a channel and starts transmitting beacons as soon as the AP comes up. The Mesh Client (MC) radio setup scans all available channels, looking for an MB radio to connect with. The SSID in the mesh WLAN is how the client and base radios of a mesh link identify each other, the same SSID should be configured on the MB WLAN as well as the MC WLAN.

In addition to a simple topology between a base and a client, a star or hub-and-spoke mesh topology is also supported; practically a mesh radio can service up to 10-12 Mesh Clients connected to it. When a radio is configured with a mesh WLAN, on that WLAN other clients are allowed to connect, and the radio can service clients on other WLANs mapped to it. Note that a client radio starts rescanning all available channels as soon as it loses connectivity to the base. Other WLANs mapped to it are not operational during this scan period.

The mesh link can also be secured with WPA2/WPA3-Preshared-Keys (PSK). The same passphrase should be configured on both the MB as well as the MC. Standard 802.11 security handshakes and AES-CCM encryption are then used on the mesh link.

For WPA2-PSK, the maximum number of allowed characters is 64 whereas for WPA3-PSK, it is 63.

Deployment scenarios

Enterprise Wi-Fi APs support single and multi-hop mesh connections, although single hop mesh is highly advisable.

Enterprise Wi-Fi APs support the following deployment scenarios:

- Between Wi-Fi 6 APs
- Mixed deployment (between Wi-Fi 6 APs and Wi-Fi 5 APs)
- With third-party APs - TP-Link, Mikrotik, Ligo wave

The following figures illustrate the working scenario of a wireless mesh network.

Figure 79: *Single hop mesh connection in 5 GHz with two Mesh Clients*

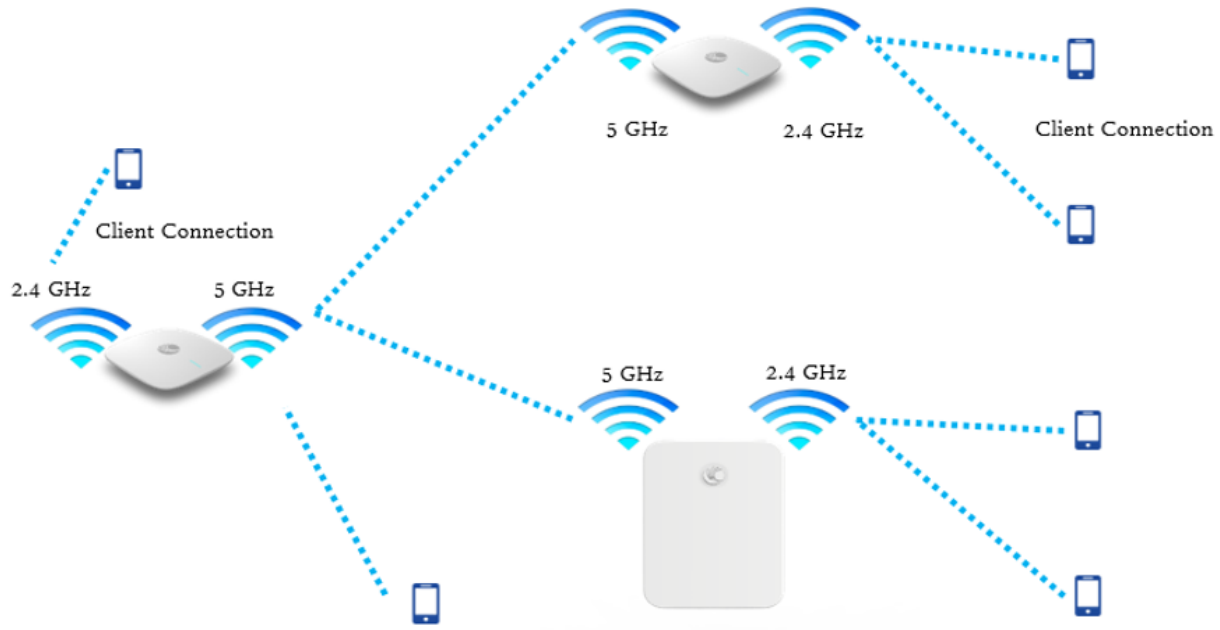


Figure 80: *Single hop mesh connection in 5 GHz with two Mesh Client s and 2.4 GHz and 5 GHz as access*

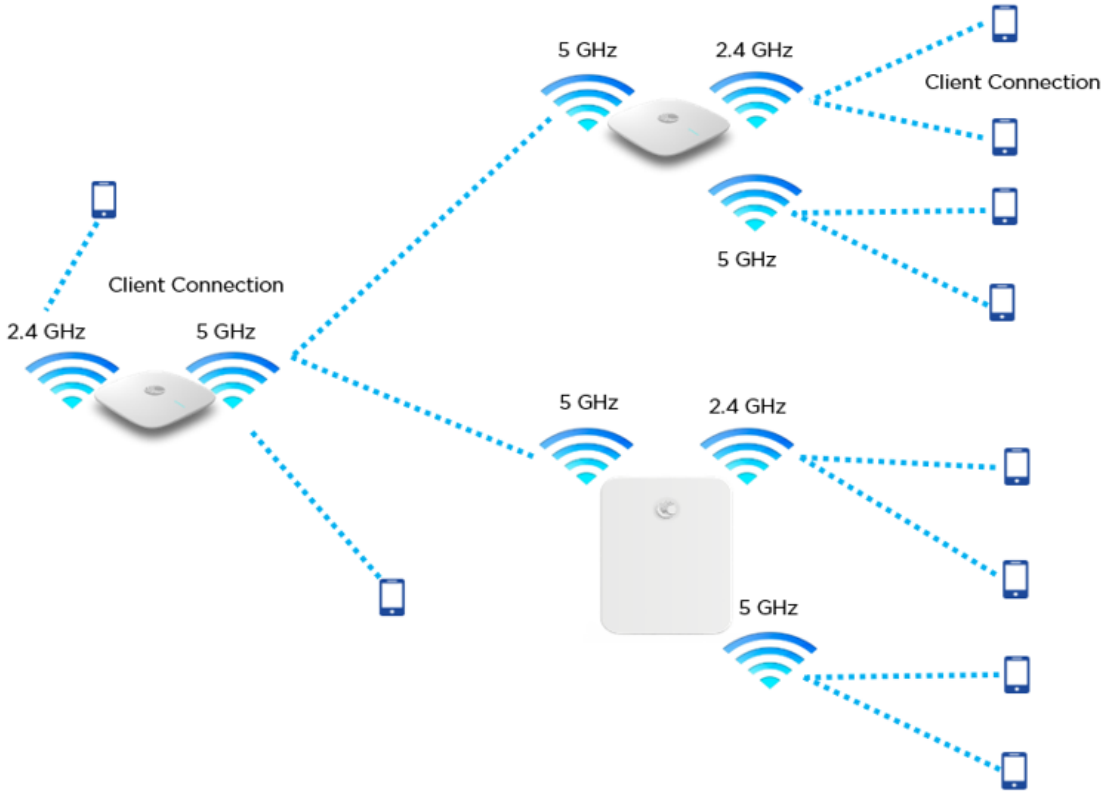
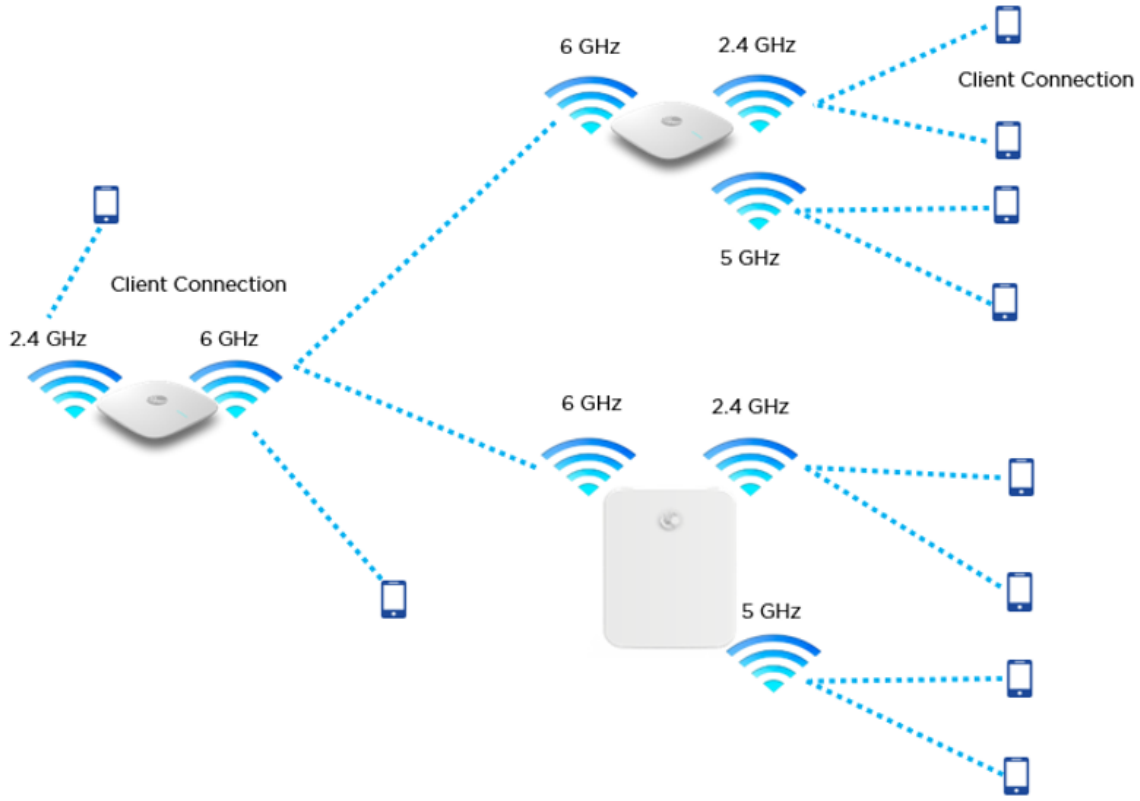


Figure 81: *Single hop mesh Connection in 6 GHz with two Mesh Clients*



For a stable mesh link to be established, Enterprise Wi-Fi mesh is configurable in the following three modes:

- Mesh Base (MB)

  Enterprise Wi-Fi device that operates in MB mode is the key to Mesh topology. MB is usually connected to the wired network. The radio setup for MB selects a channel and starts transmitting beacons as soon as the AP comes up.

- Mesh Client (MC)

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

- Mesh Recovery (MR)

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

  This mode can also help in the Zero Touch Configuration of the Enterprise Wi-Fi device.

Mesh configurable parameters

The below table lists the configurable parameters that are exclusive to mesh:

Table 61: Mesh configurable parameters

Parameter	Description	Range	Default
Mesh	This parameter is required when a mesh connection is established with Enterprise Wi-Fi devices. Four options are available under this parameter: 1. Base A WLAN profile configured with a Mesh Base operates like a normal AP. Its radio beacon is on startup so its SSID can be seen by radios configured as Mesh Clients. 2. Client A WLAN profile configured with a Mesh Client scans all available channels on startup, looking for a mesh-based AP to connect. 3. Recovery A WLAN profile configured as mesh-recovery broadcast pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on the mesh-base device. Mesh Client auto-scan for mesh-recovery SSID upon failure of mesh link.	-	Off
SSID	SSID is the unique network name to which MC connects and establishes mesh links.	-	-
VLAN	Management VLAN to access all devices in a mesh topology.	1-4094	1
Security	For configurable parameters, refer to Chapter 6: Security section.	-	Open
Passphrase	A string that is a key value to generate keys based on the security method configured.	-	12345678
Radios	Each SSID can be configured to be transmitted as per the deployment requirement. For a mesh WLAN profile, options available to configure the band: • 2.4 GHz • 5 GHz • 6 GHz	-	2.4 GHz
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	-	Disabled
SNR-threshold	Mesh Clients trigger a disconnect when SNR is below configured value. This is the applicable configuration on the MB.	1-100	Disabled
Mesh Recovery	Configure the interval for the consecutive ping loss seen after which the mesh link is considered to be down and a reconnect is	5-30 min	30

Parameter	Description	Range	Default
Interval	attempted. One can configure the duration and interval to be the same, in which case the first ping losses trigger the reconnect.		
Mesh Auto Detect Backhaul	1. Single Hop Both Mesh Client and MB profiles are configured on the devices. When enabled, this feature triggers when an MB losses Ethernet connectivity. Mesh Client profile automatically gets enabled and establishes a mesh link with the nearest MB. For the MB profile to get auto-disabled, uncheck Mesh Multi-Hop. 2. Multi-Hop Consider Mesh Client AP is connected to an MB AP which has an Ethernet backhaul connection. In case MB which has the backhaul connection loses the Ethernet connectivity, both APs disconnect from the network. When Auto detected Backhaul is enabled on the MB, it automatically enables the MC profile and connects to the nearest MB ensuring the connectivity for self as well as the client behind. Mesh Multi-Hop check should be enabled for this feature to be active. 3. Mesh Monitored Host This parameter is exclusive to Mesh Client devices when Auto-Detect Backhaul is enabled with an extended network via the Ethernet of the device. Configure IP or Hostname to check the link status.	-	Disabled
Mesh Client Monitor	1. Duration Duration in minutes of ping failure after which mesh connectivity is re-established. 2. Host Configure a server to monitor with ping to decide if mesh connectivity needs to be re-established.	-	-
Mesh Vlan Tagging	Enable the VLAN tagging over the mesh link. This applies only to the Cambium mesh topology.	-	Enabled

Order of Mesh profile configuration

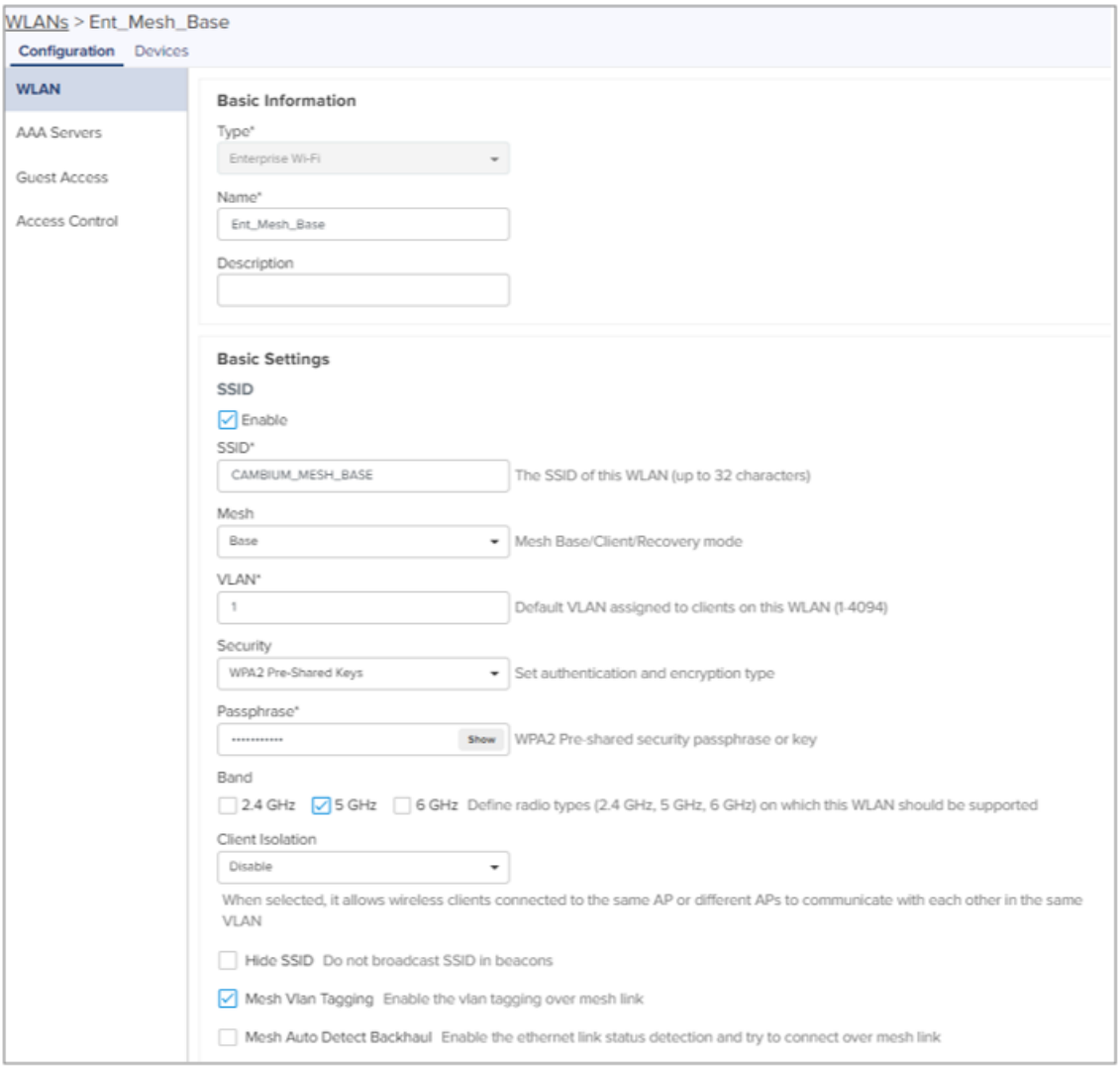
If a device is configured as Mesh Base/client/recovery, the recommended order of WLAN configuration should be as follows:

- WLAN profile 1: Mesh Base
- WLAN profile 2: Mesh Client
- WLAN profile 3: Mesh Recovery

Mesh Base (MB)

To configure the MB:

cnMaestro configuration:



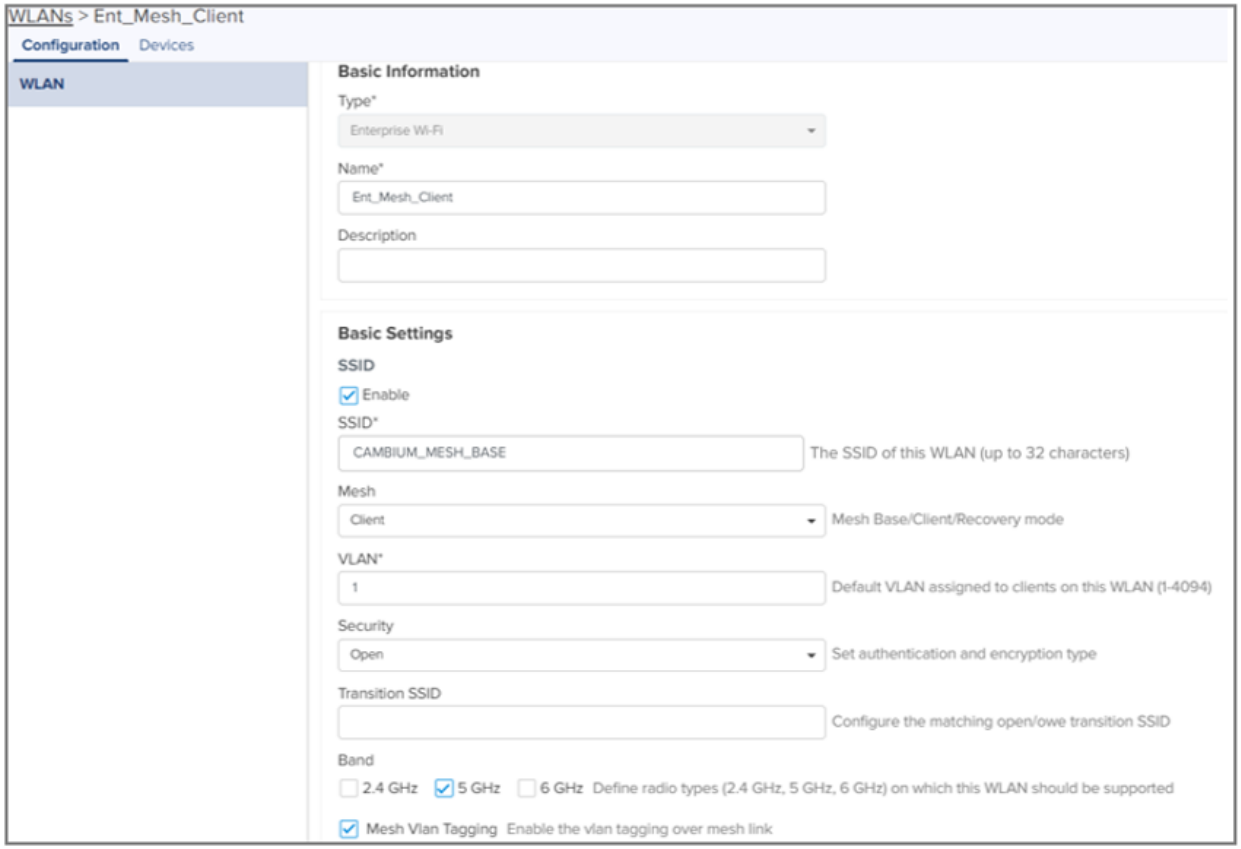
CLI configuration:

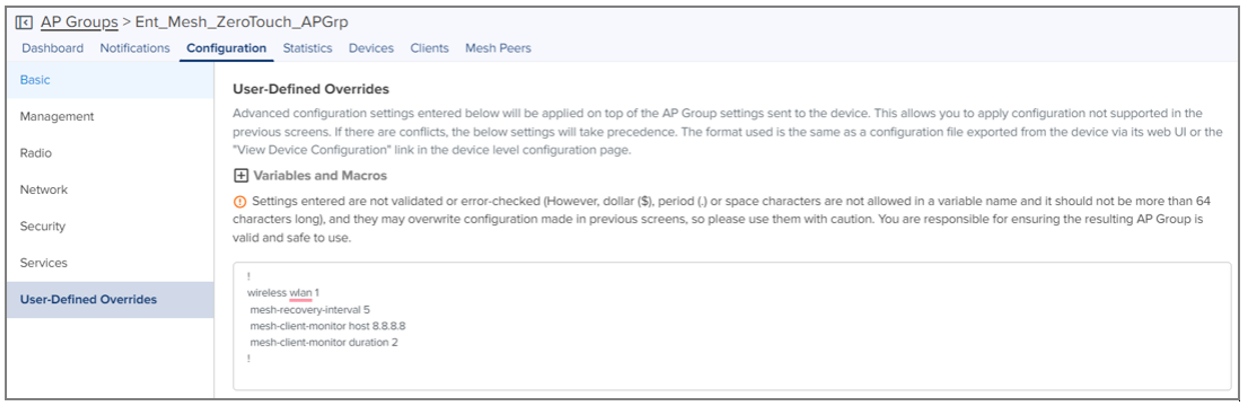
```
XV3-8-EC7708(config-wlan-1)# Mesh Base
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# VLAN 1
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

Mesh Client (MC)

To configure the MC:

cnMaestro configuration:





CLI configuration:

```
XV3-8-EC7708(config)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# mesh client
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-1)# vlan 1
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

```
XV3-8-EC7708(config-wlan-1)# mesh-recovery-interval 30
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor duration 5
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor host 8.8.8.8
```

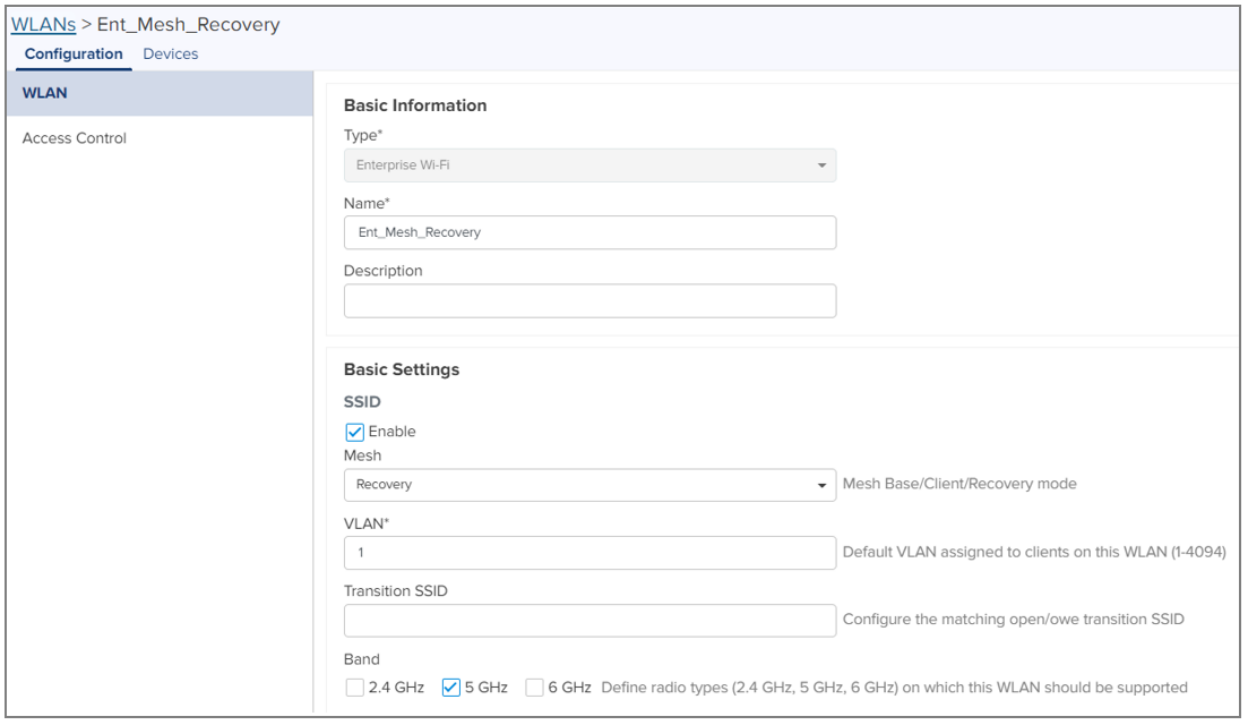
Mesh Recovery (MR)

To support plug and play Mesh deployment model, suggest configuring the MR profile on the MB AP. As a result, factory reset APs/New APs can establish a mesh connection to the MB right away (out of the box).

A recovery profile is also useful when an MC loses connectivity to a base due to misconfiguration or a bad connection that causes frequent drops.

To configure the MR:

cnMaestro configuration:



CLI configuration:

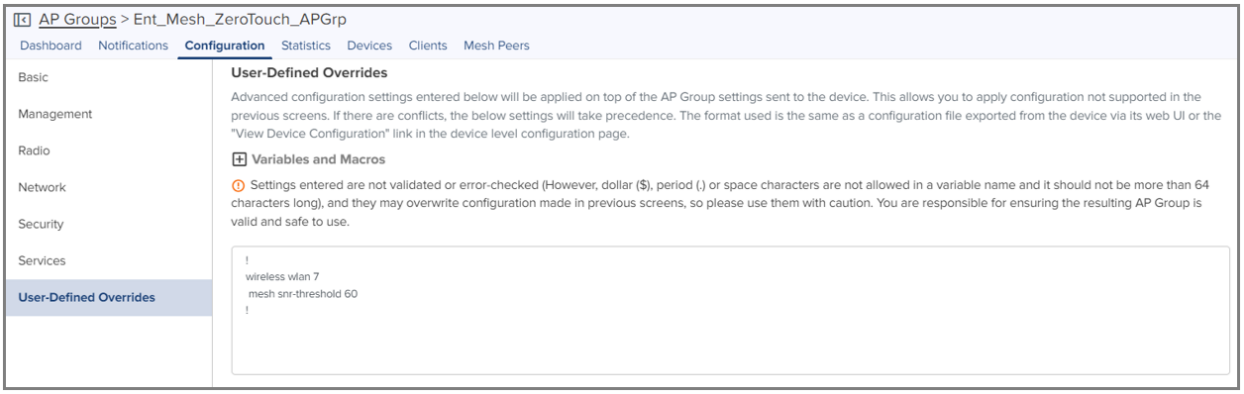
```
XV3-8-EC7708(config-wlan-1)# mesh recovery
XV3-8-EC7708(config-wlan-1)# vlan 1
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

Please refer to the Cambium Zero touch White paper on mesh for more information on Zero touch Mesh.

Mesh SNR-threshold

SNR-threshold configuration parameter is supported via CLI and can also be provisioned via cnMaestro on the MB WLAN profile. This parameter helps in maintaining the quality of the mesh link by denying MCs which has a low SNR value than the configured threshold.

cnMaestro configuration:



CLI configuration:

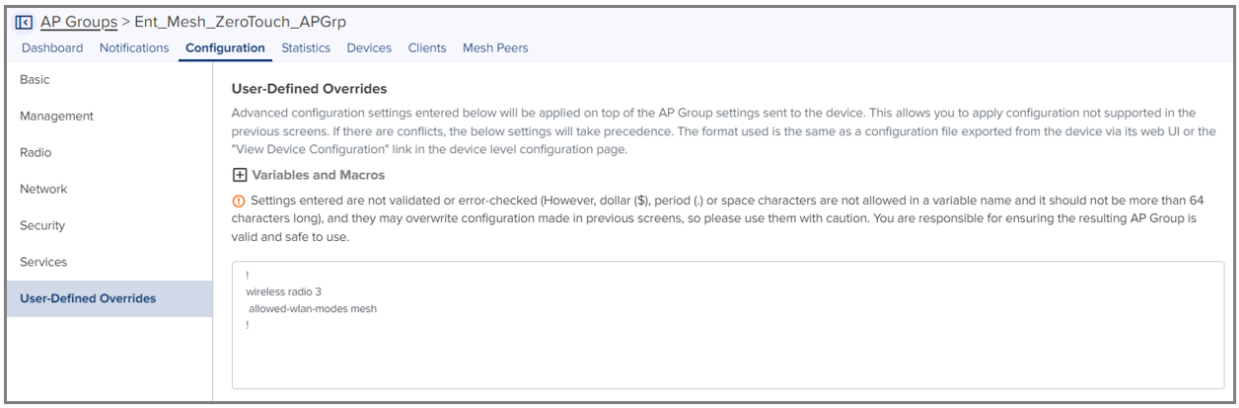
```
XV3-8-EC7708(config-wlan-1)# mesh snr-threshold 60
```

Mesh Mode

Enterprise Wi-Fi 6 APs support multi-radio, and by default channel distribution, is enabled. When channel distribution is enabled, each radio is mapped with a group of channels that it can operate.

When a device operates in MC, it will scan channels that are supported by the radio. Hence, there is a high possibility that MC will never connect to MB. Mesh mode configuration is supported at the RADIO level. To maintain the consistent link, the user has provision exclusively to configure mode on the radio to ensure that Mesh Clients are always connected to the network. To configure the Mesh mode:

cnMaestro configuration:



CLI configuration:

```
XV3-8-EC7708(config-radio-1)# allowed-wlan-modes mesh
```

Mesh ACL

ACL can be used to make sure that the Mesh Client connecting to the base AP is a known AP. The Mesh Client radio MAC address can be added to the Mesh Base AP to achieve this.

Following are the various modes of MAC authentication supported by Enterprise Wi-Fi APs:

- Allow

To enable this mode, add the list of MAC addresses either to be allowed or denied under “mac-authentication list <Radio MAC of Mesh Client>” and configure the device as below:

cnMaestro configuration:

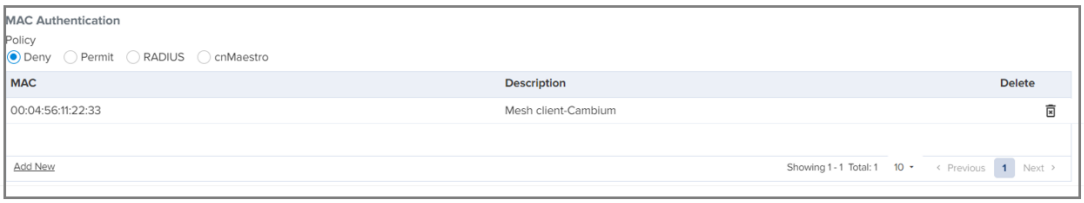
CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mac-authentication policy allow
```

- Deny

  To enable this mode, add the list of MAC addresses either to be allowed or denied under “mac-authentication list <Radio MAC of Mesh Client>” and configure the device as below:

  cnMaestro configuration:



  CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mac-authentication policy deny
```

- RADIUS

  To enable this mode, configure the device (described in Chapter 7: Radius server section) on the MB WLAN profile as below:

  cnMaestro configuration:

  CLI configuration:

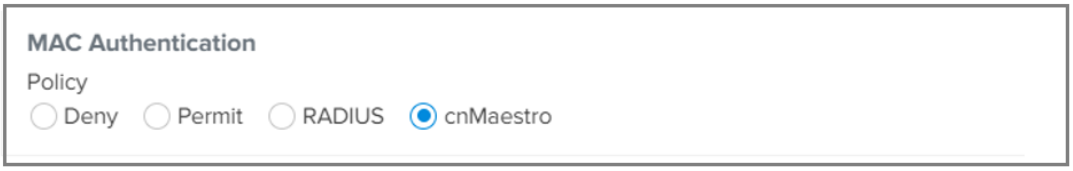
```
XV3-8-EC7708(config-wlan-1)# mac-authentication policy radius
```

- cnMaestro

  To enable this mode, define the MAC addresses allowed or denied as described in the cnMaestro On-Premises User Guide Association ACL section and configure the device on

the MB WLAN profile as below:

cnMaestro configuration:



CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mac-authentication policy cnMaestro
```

Mesh Auto Detect Backhaul

Mesh Auto Detect backhaul is a mechanism to enable MB or MC WLAN profile based on the status of ethernet of a device that is operating in mesh mode. Enterprise Wi-Fi 6 APs are multi-radio and multi-ethernet supported, hence there are multiple ways of configuring this feature based on the number of ethernet ports of a device.

In general, customers use a single AP group to configure any mesh devices in a network. When this feature is enabled, the device is intelligent enough to decide whether it has to operate in MB or MC mode. Below are different scenarios (AP2), where this feature can trigger a change in the mesh mode of the device.

Scenario 1

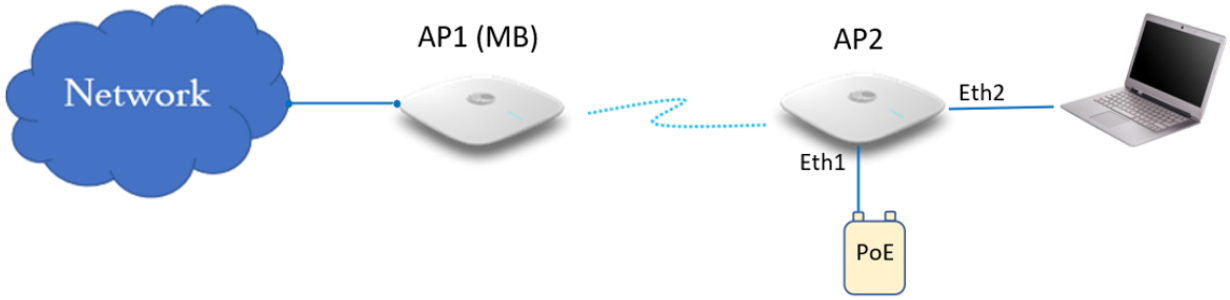
When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 and eth2 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

Based on eth1 and eth2 physical link and reachability to 8.8.8.8 determines the state of mesh mode of AP2. Below is a matrix that explains AP2 behavior:

Eth 1	Eth 2	8.8.8.8 Reachability	MB	MC
• Connected • No data enabled	Connected with no network reachability	No	Disabled	Enabled
• Connected • No data enabled	Connected with network reachability	Yes	Enabled	Disabled
• Connected • Data-enabled	Connected with no network reachability	No	Disabled	Enabled
• Connected	Connected with no network reachability	Yes	Enabled	Disabled

Eth 1	Eth 2	8.8.8.8 Reachability	MB	MC
• Data-enabled				
• Connected • Data-enabled	Connected with network reachability	Yes	Enabled	Disabled

Figure 82: *Deployment Scenario 1*

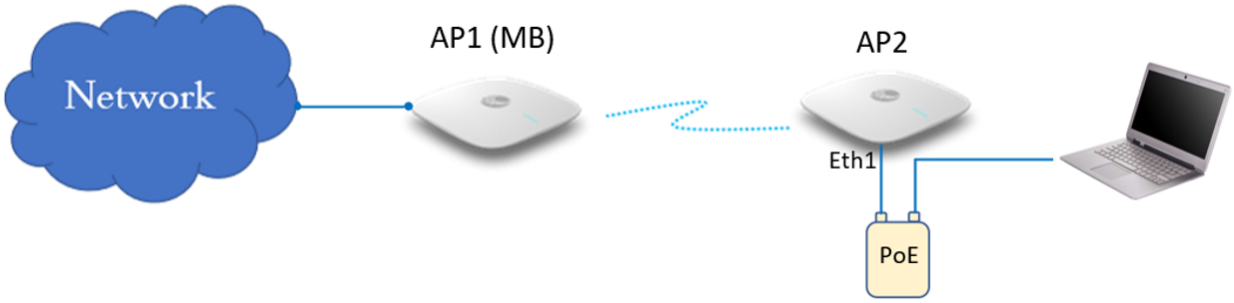


Scenario 2

When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

Eth 1	8.8.8.8 Reachability	MB	MC
• Connected • No data enabled	No	Disabled	Enabled
• Connected • Data-enabled	No	Disabled	Enabled
• Connected • Data-enabled	Yes	Enabled	Disabled

Figure 83: *Deployment Scenario 2*

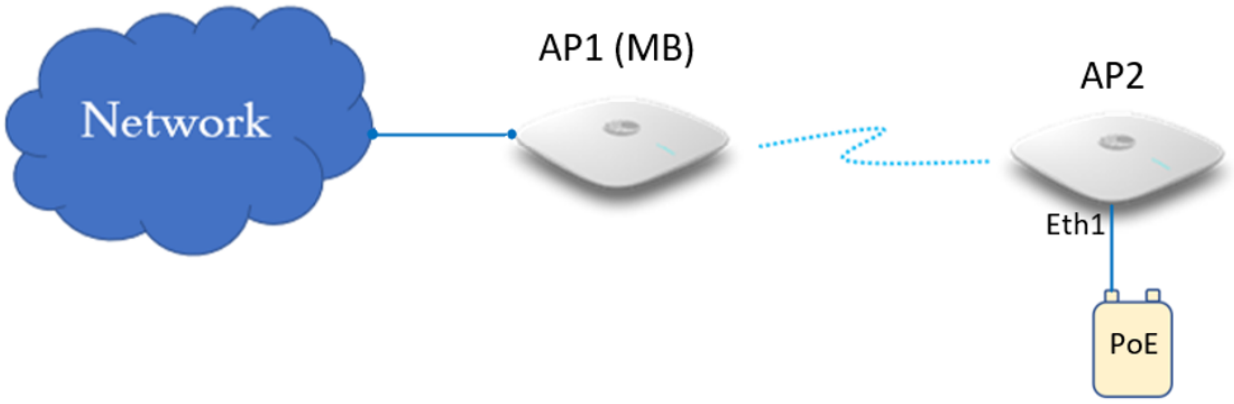


Scenario 3

When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

Eth 1	8.8.8.8 Reachability	MB	MC
Connected	No	Disabled	Enabled

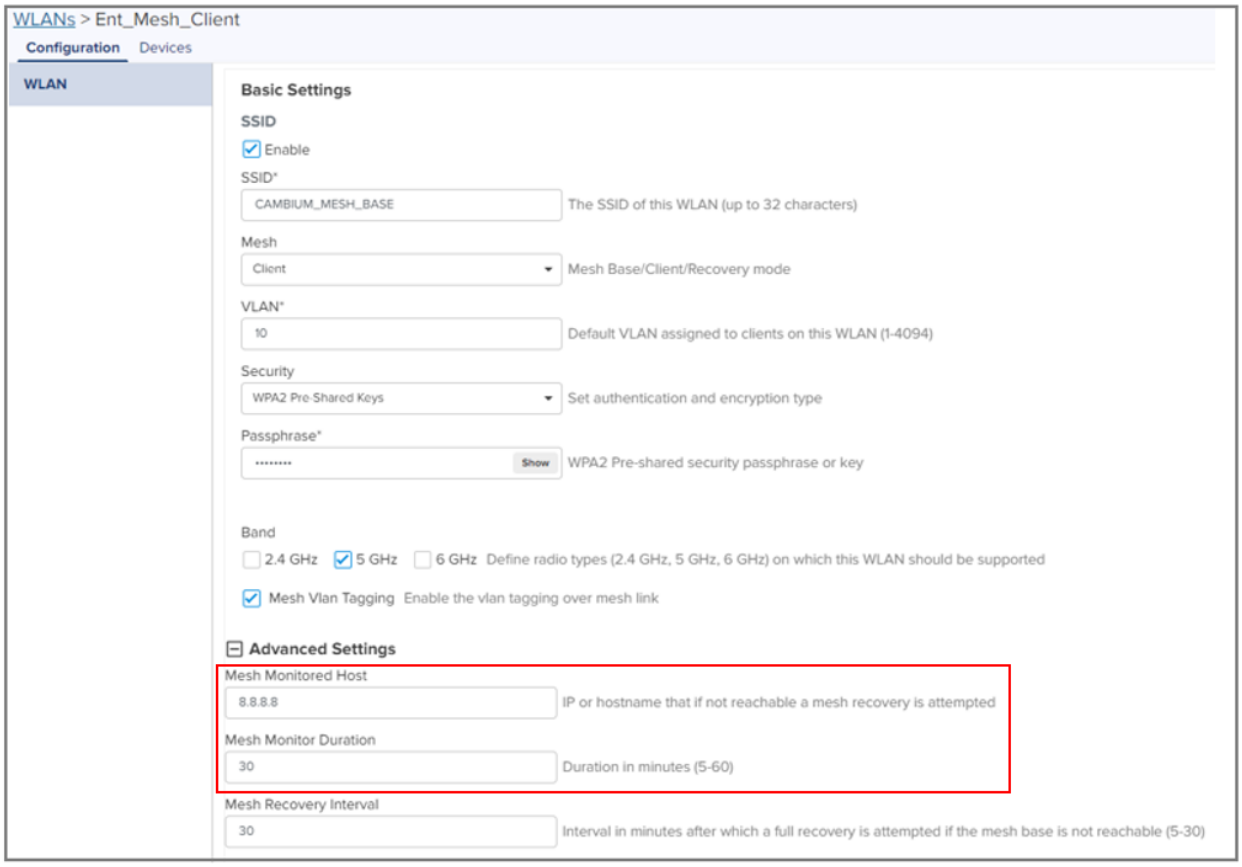
Figure 84: *Deployment Scenario 3*



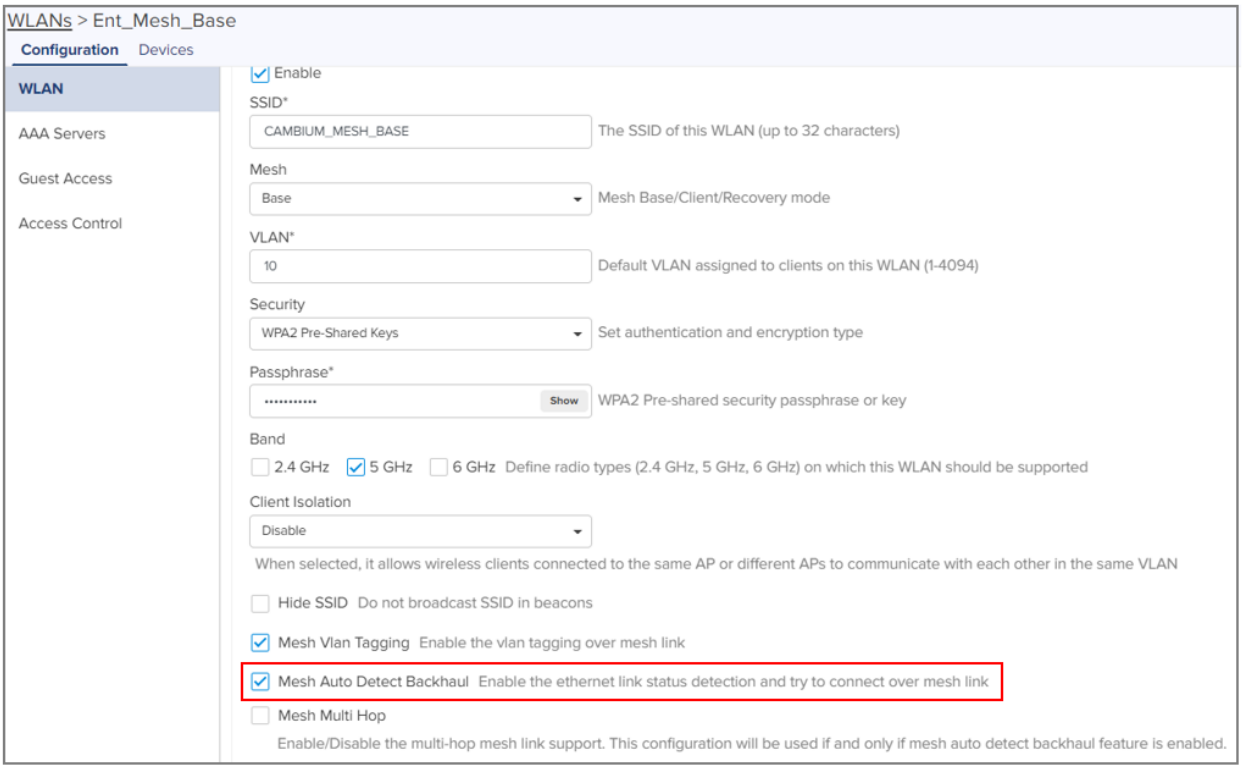
To enable this configuration either from cnMaestro or CLI, follow the below guidelines:

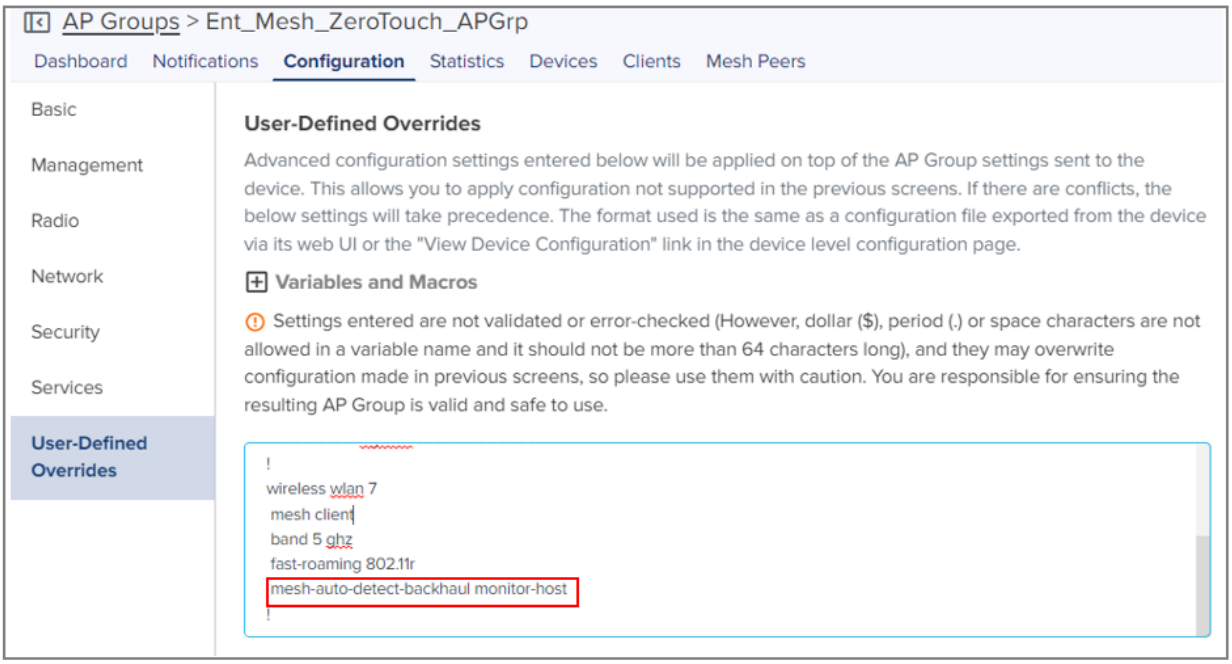
cnMaestro configuration:

Mesh Client



Mesh Base





CLI configuration:

Mesh Client

```
XV3-8-EC7708(config-wlan-1)# mesh client
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
```

```
XV3-8-EC7708(config-wlan-1)# vlan 1
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# band 5GHz
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor duration 5
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor host 8.8.8.8
```

Mesh Base

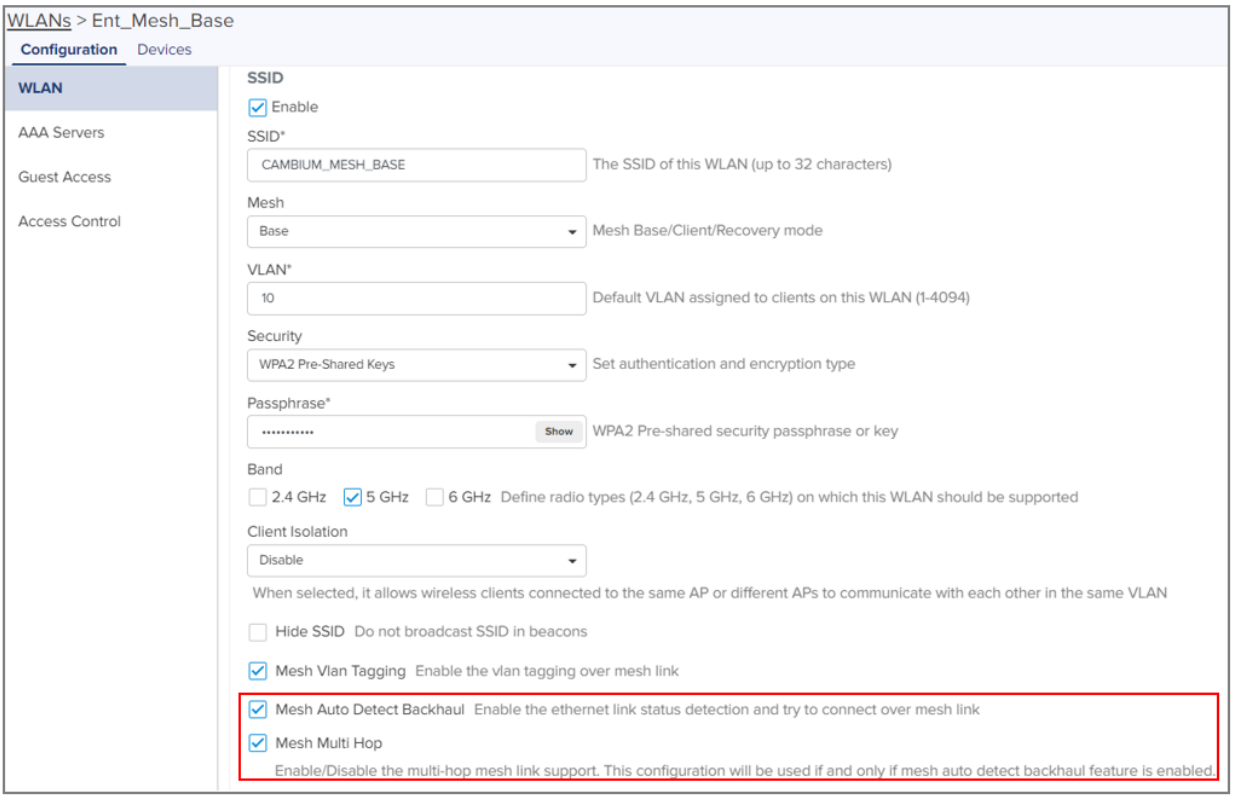
```
XV3-8-EC7708(config-wlan-7)# mesh base
XV3-8-EC7708(config-wlan-7)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-7)# vlan 1
XV3-8-EC7708(config-wlan-7)# security wpa2-psk
XV3-8-EC7708(config-wlan-7)# passphrase 12345678
XV3-8-EC7708(config-wlan-7)# band 5GHz
XV3-8-EC7708(config-wlan-7)# mesh-auto-detect-backhaul
XV3-8-EC7708(config-wlan-7)# mesh-auto-detect-backhaul monitor-host
```

Mesh Muti-Hop

This topology is not a recommended solution but can be deployed in foreseen situations. In this type of deployment, intermediate devices (AP2) in mesh links require both MB and MC to be enabled.

Figure 85: *Multi-Hop deployment Scenario*

cnMaestro configuration:



CLI configuration:

```
XV3-8-EC7708(config-wlan-7)# mesh base
XV3-8-EC7708(config-wlan-7)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-7)# vlan 1
XV3-8-EC7708(config-wlan-7)# security wpa2-psk
XV3-8-EC7708(config-wlan-7)# passphrase 12345678
XV3-8-EC7708(config-wlan-7)# band 5GHz
XV3-8-EC7708(config-wlan-7)# mesh-auto-detect-backhaul
XV3-8-EC7708(config-wlan-7)# mesh-auto-detect-backhaul monitor-host
XV3-8-EC7708(config-wlan-7)# mesh-auto-detect-backhaul multi-hop
```

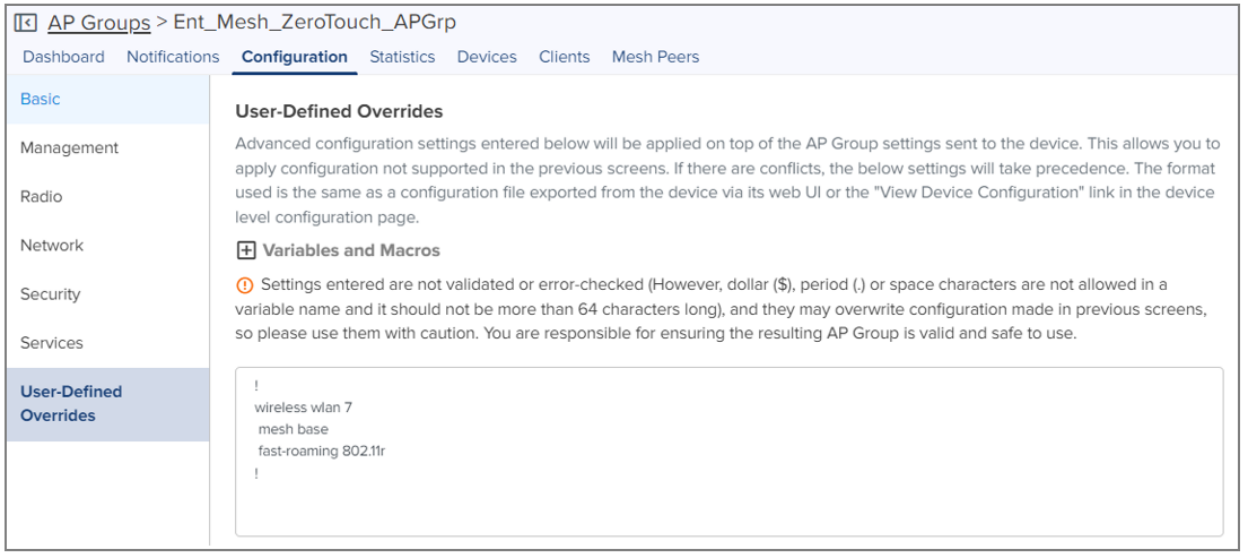
Mesh Roaming

From Release 6.4 onwards Enterprise Wi-Fi 6 APs support mesh roaming. For this functionality to be active, enable the below parameters (MB and MC) on mesh devices.

Mesh Base configuration

Enable 802.11r on the MB WLAN profile to support MC roaming.

cnMaestro configuration:



CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# fast-roaming 802.11r
```

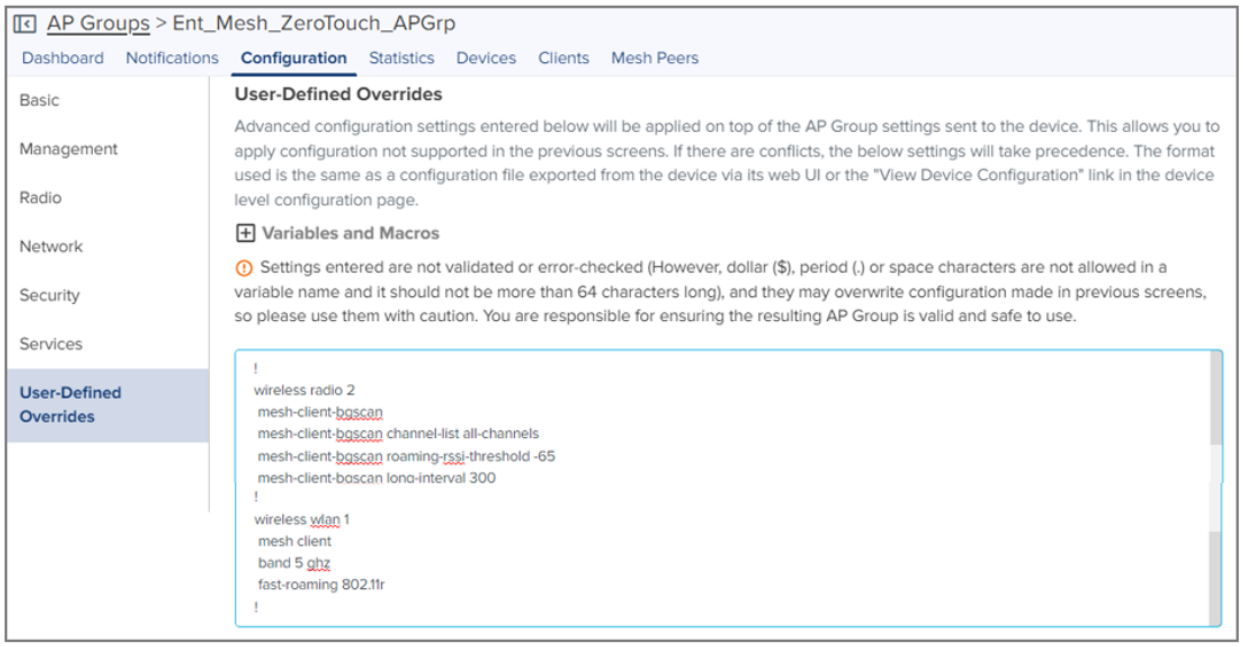
Mesh Client configuration

For Mesh Client roaming to be operational, enable or configure the below parameters on the radio where the mesh client is enabled.

Table 62: Mesh Client configuration parameter

Parameters	Description	Range	Default
mesh-client-bgscan	Provision to enable the Mesh Client background scan.	-	Disabled
mesh-client-bgscan channel-list	The list of channels the Mesh Client needs to scan to look for AP.	-	-
mesh-client-bgscan long-interval	Once APs RSSI goes above this value, scan intervals are every configured interval.	1-600 seconds	300
mesh-client-bgscan roaming-rssi-threshold	APs RSSI threshold to initiate a scan and roam.	-100-0 dBm	-65
mesh-client-bgscan short-interval	Once AP's RSSI drops below this value, the immediate scan will be triggered and follows the scan interval.	1-300 seconds	60

cnMaestro configuration:



CLI configuration:

```
XV3-8-EC7708(config-radio-2)# mesh-client-bgscan
XV3-8-EC7708(config-radio-2)# mesh-client-bgscan channel-list all-channels
XV3-8-EC7708(config-radio-2)# mesh-client-bgscan roaming-rssi-threshold -65
XV3-8-EC7708(config-radio-2)# mesh-client-bgscan long-interval 300
XV3-8-EC7708(config-radio-2)# mesh-client-bgscan short-interval 60
```

Mesh link-Sample configuration

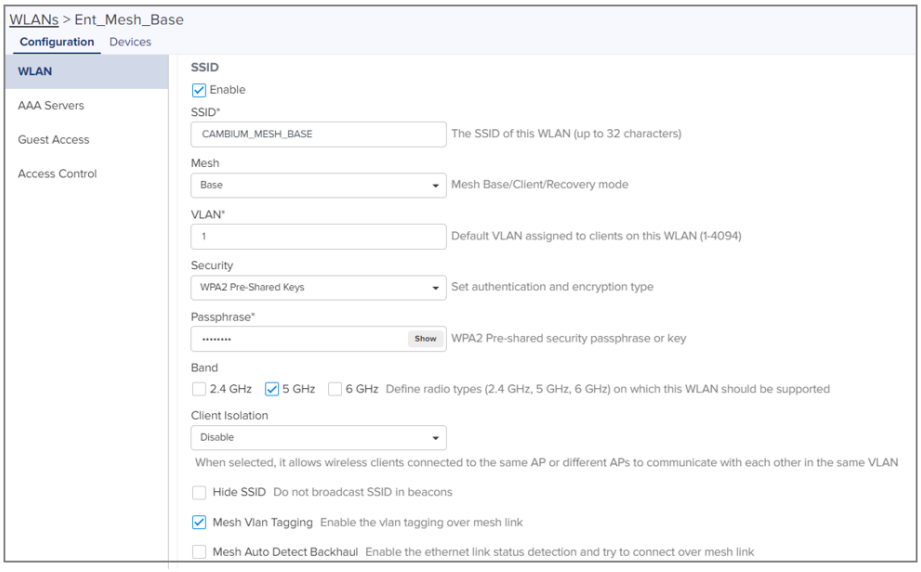
This section briefs about the configuration of the device to get a mesh link established with different deployment scenarios.

VLAN 1 as the management interface

Follow the below CLI commands to establish a mesh link with VLAN 1 as the management interface:

1. To configure MB and MR, following are the commands:
    - WLAN MB profile

      cnMaestro configuration:

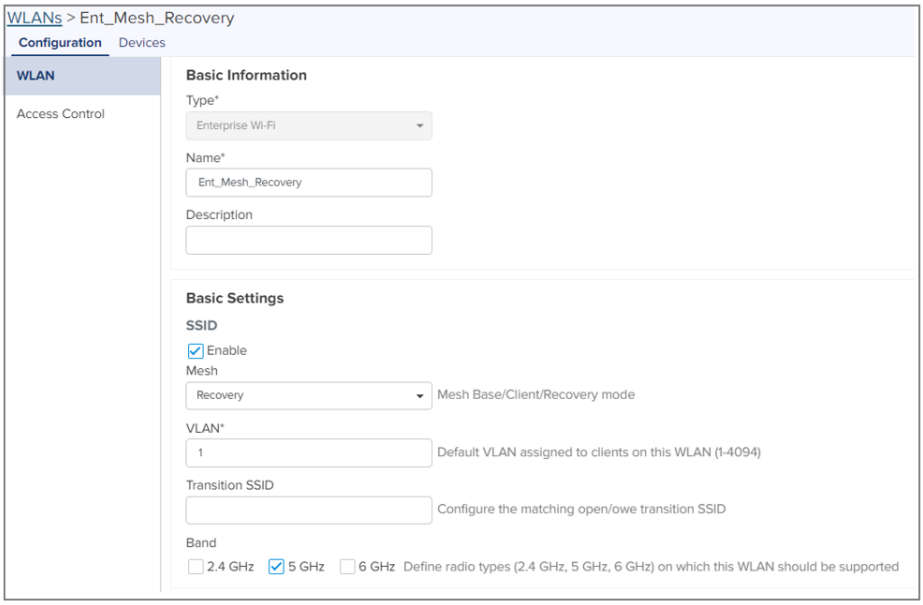


CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mesh base
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# VLAN 1
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

- WLAN MR profile

  cnMaestro configuration:

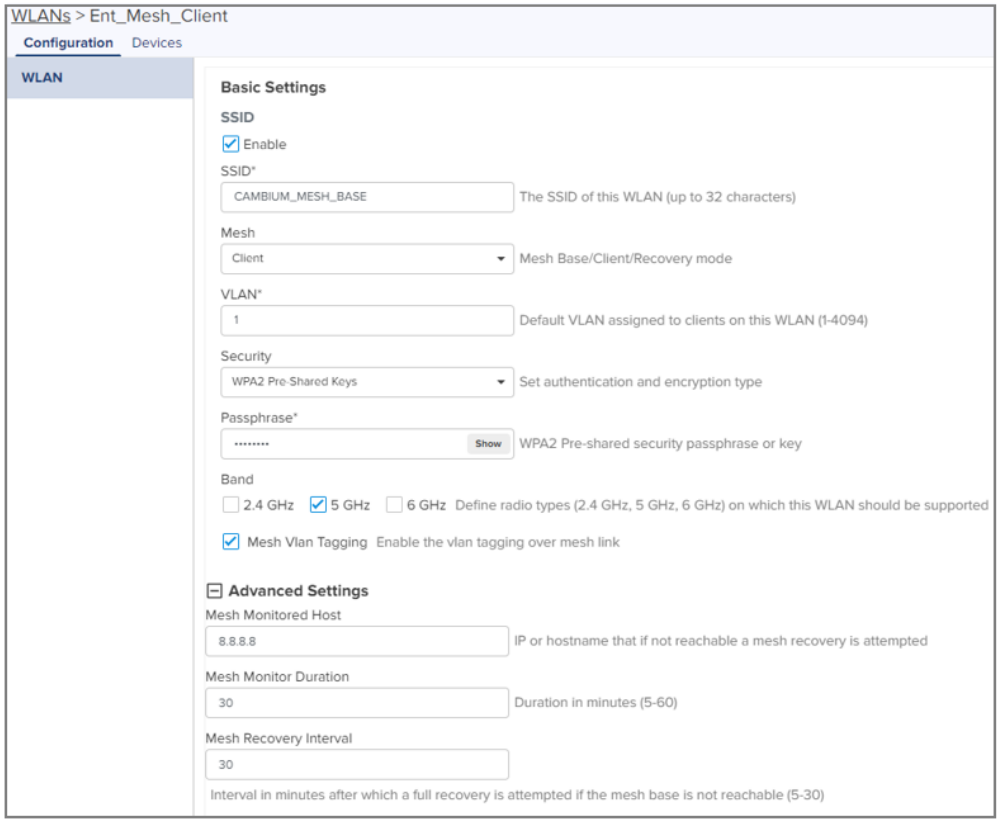


CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mesh recovery
XV3-8-EC7708(config-wlan-1)# vlan 1
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

2. To configure MC, following are the commands:

   cnMaestro configuration:

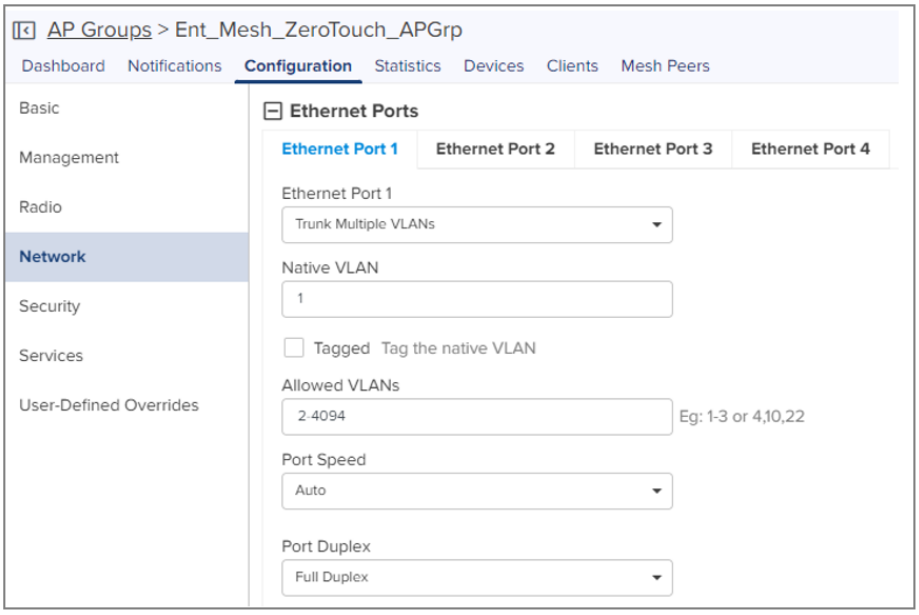


CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mesh client
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-1)# vlan 1
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# band 5GHz
XV3-8-EC7708(config-wlan-1)# mesh-recovery-interval
XV3-8-EC7708(config-wlan-1)# mesh-recovery-interval 30
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor duration 5
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor host 8.8.8.8
```

3. To configure the Management VLAN interface, following are the commands:

   cnMaestro configuration:



CLI configuration:

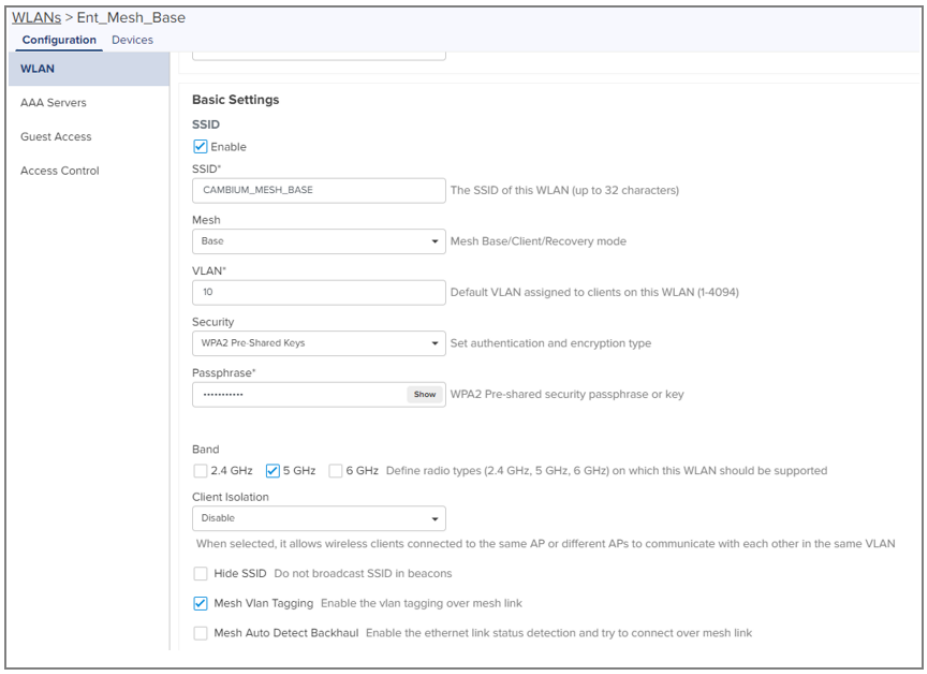
```
XV3-8-EC7708(config)# interface vlan 1
XV3-8-EC7708(config-vlan-1)# ip address dhcp
XV3-8-EC7708(config-vlan-1)# exit
XV3-8-EC7708(config)# interface eth 1
XV3-8-EC7708(config-eth-1)# switchport mode trunk
XV3-8-EC7708(config-eth-1)# switchport trunk native vlan 1
XV3-8-EC7708(config-eth-1)# switchport trunk allowed vlan 2-4094
```

Non-VLAN 1 as the management interface

Follow the below CLI commands to establish a mesh link with non-VLAN 1 as the management interface:

1. To configure MB and MR, following are the commands:
    - WLAN MB profile

      cnMaestro configuration:

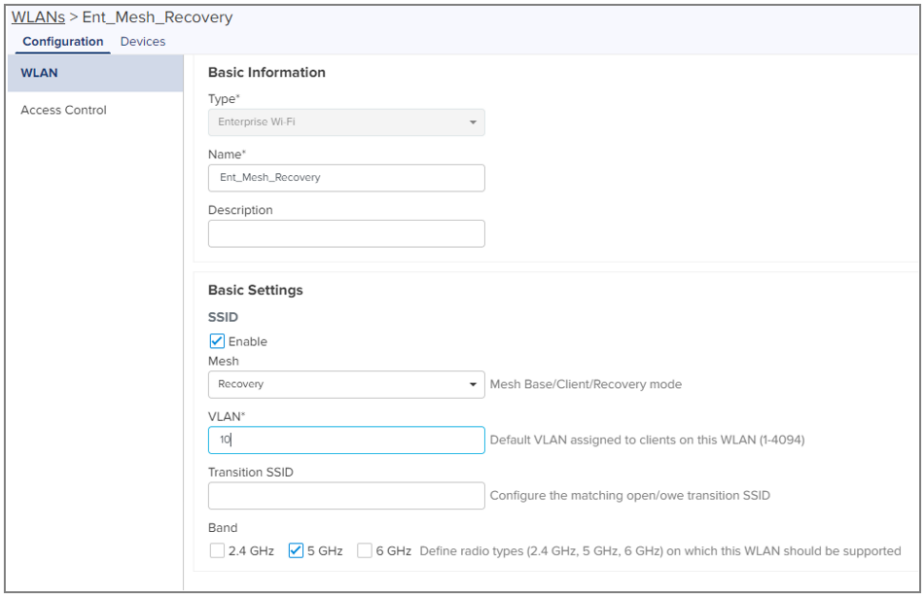


CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mesh base
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# VLAN 10
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

- WLAN MR profile

  cnMaestro configuration:

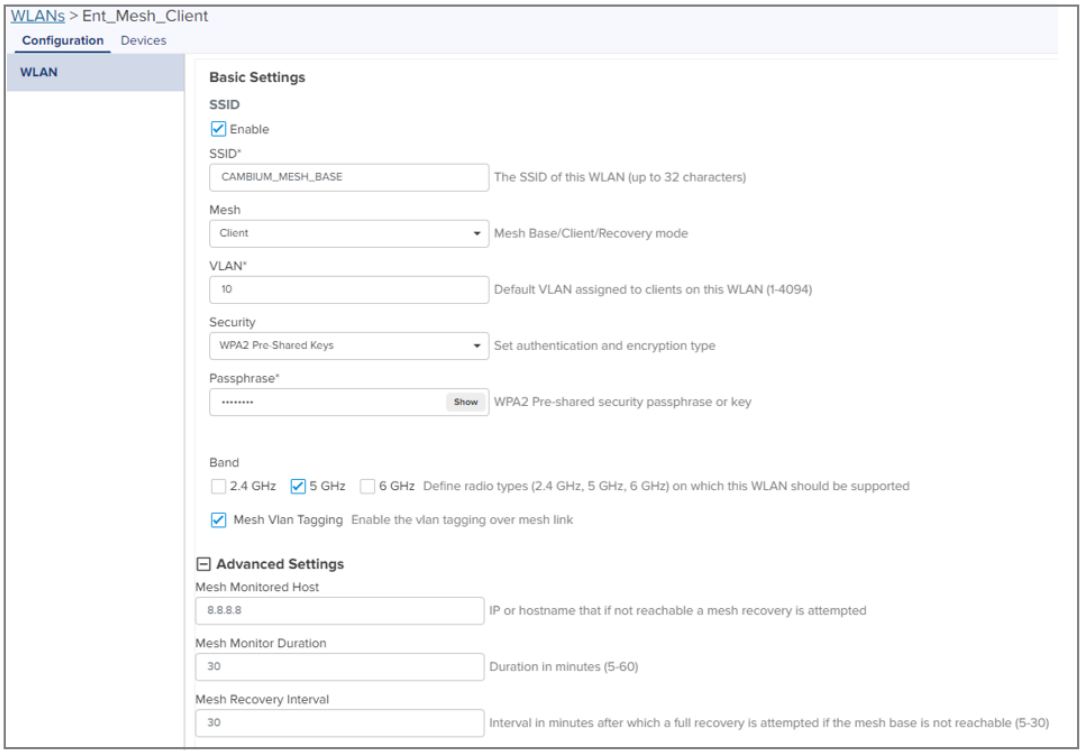


CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mesh recovery
XV3-8-EC7708(config-wlan-1)# vlan 10
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

2. To configure MC, following are the commands:

   cnMaestro configuration:

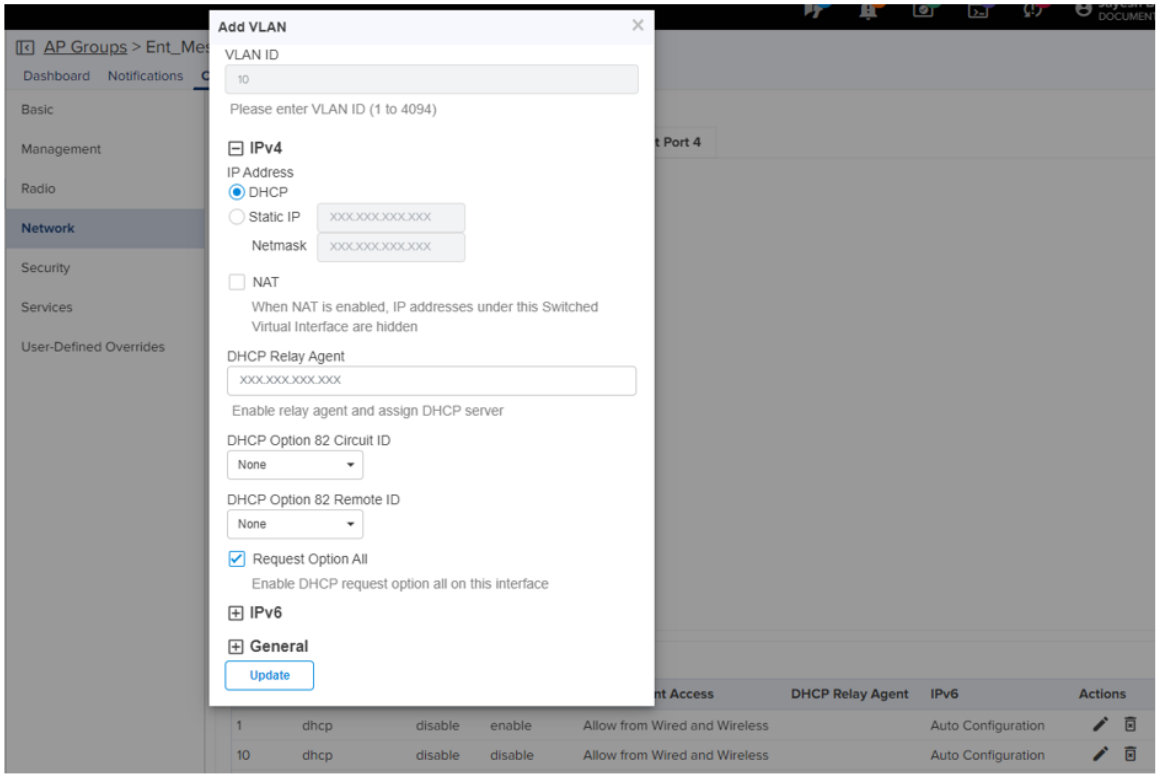


CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# mesh client
XV3-8-EC7708(config-wlan-1)# ssid CAMBIUM_MESH_BASE
XV3-8-EC7708(config-wlan-1)# vlan 10
XV3-8-EC7708(config-wlan-1)# security wpa2-psk
XV3-8-EC7708(config-wlan-1)# passphrase 12345678
XV3-8-EC7708(config-wlan-1)# band 5GHz
XV3-8-EC7708(config-wlan-1)# mesh-recovery-interval
XV3-8-EC7708(config-wlan-1)# mesh-recovery-interval 30
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor duration 5
XV3-8-EC7708(config-wlan-1)# mesh-client-monitor host 8.8.8.8
```

3. To configure the Management non-VLAN interface, the following are the commands:

   cnMaestro configuration:



CLI configuration:

```
XV3-8-EC7708(config)# interface vlan 10
XV3-8-EC7708(config-vlan-10)# ip address dhcp
XV3-8-EC7708(config-vlan-10)# ip dhcp request-option-all
XV3-8-EC7708(config)# interface eth 1
XV3-8-EC7708(config-eth-1)# switchport mode trunk
XV3-8-EC7708(config-eth-1)# switchport trunk native vlan 1
XV3-8-EC7708(config-eth-1)# switchport trunk allowed vlan 2-4094
```

Typical use-cases

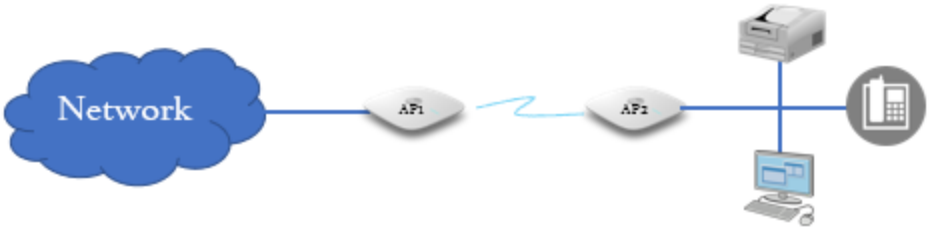
- Wi-Fi access in areas with no cable run
    - Add an AP indoor/outdoor APs for the areas that are difficult to reach
- Small retail location with one AP near an Ethernet outlet, and another in the middle of the lobby that has no easy cable run.
- Resolving coverage issues.
    - Plug coverage holes

- Extend range outdoors
    - An XV2-2T Hotspot in a parking lot outside a building, with XV2-2s providing Wi-Fi within the building

Additional mesh topology supported

Note

The following topology supports zero touch provisioning and single AP group configuration.



Wired devices behind mesh client AP

In this scenario, when wired devices are connected to the mesh client AP (AP2), the AP will support zero touch provisioning and both base and client APs will have the same configuration (AP group). Mesh AP must have the capability to connect a separate LAN segment (containing wired devices) to the WLAN.

When an AP, with factory default configuration, is connected in the above scenario, the device waits for 180 seconds to obtain the IP address from the wired side. If the device does not receive any IP address from the wired side, then mesh recovery is triggered. If the device restarts, the device waits for 360 seconds to obtain the IP address from the wired side. If the device does not receive any IP address from the wired side, then mesh recovery is triggered.

Chapter 16: Guest Access Portal - Internal

Introduction

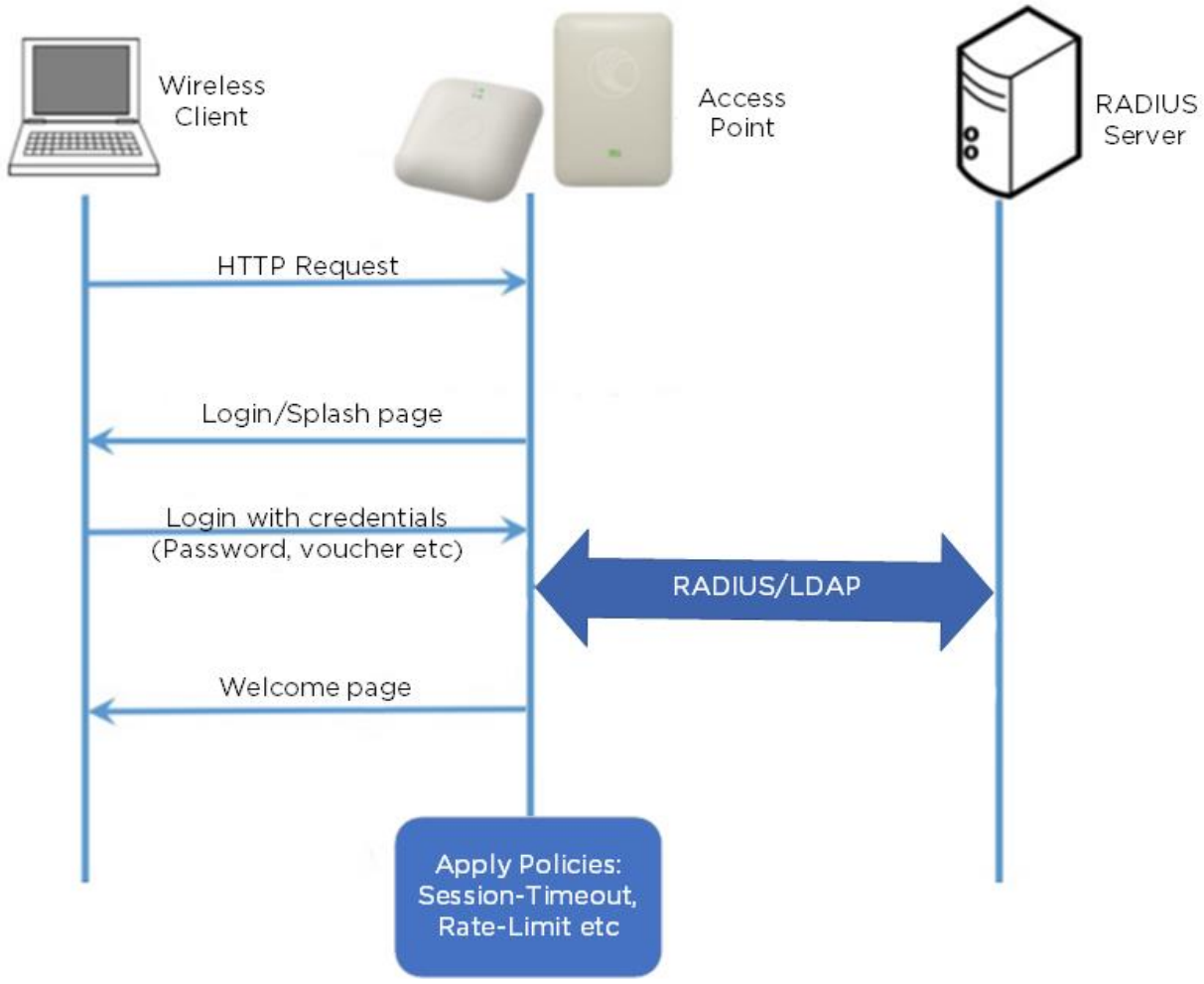
Guest Access Portal services offer a simple way to provide secure access to the internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browser's session to a captive portal login 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 the access point and is local to the AP.
- **External Access**: Enterprise Wi-Fi AP is integrated with multiple third-party Captive Portal services vendors. Based on the vendor, the device needs to be configured. For more information, see Guest Access Portal - External.
- **cnMaestro**: Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login, and Paid login are supported. For more information, see Guest Access – cnMaestro.
- **EasyPass**: EasyPass Access Services enable you to easily provide secure and controlled access to users and visitors on your Wi-Fi network.

This chapter describes about Internal Captive Portal services supported by Enterprise Wi-Fi APs. The following figure displays the basic topology of testing the Internal Captive Portal Service.

Figure 86: *Topology*



Configurable parameters

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

Figure 87: *Guest Access Internal Access Point parameter*

Access policy

Click through

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

Splash page

Title

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

Contents

You can configure the contents of the 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 is supported.

Background image

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

Redirect parameters

Redirect hostname

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

Success action

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

- Internal logout Page

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

- Redirect users to external URL

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

- Redirect users to the Original URL

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

Figure 88: *Success action*

Redirect

By default, captive portal redirection is triggered when the user accesses either HTTP or HTTPS WWW. If enabled, redirection to Captive Portal Splash Page is triggered when an HTTP WWW is accessed by end-user.

Figure 89: *Redirect*

Redirect Mode

There are two redirect modes available:

- **HTTP Mode**

  When enabled, AP sends an 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

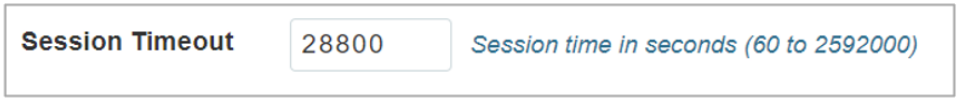
Figure 90: *Success Message*

Timeout

Session

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

Figure 91: *Session timeout*



Inactivity

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

Figure 92: *Inactivity timeout*

Whitelist

Provision to configure either Ips or URLs to bypass traffic, therefor users 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

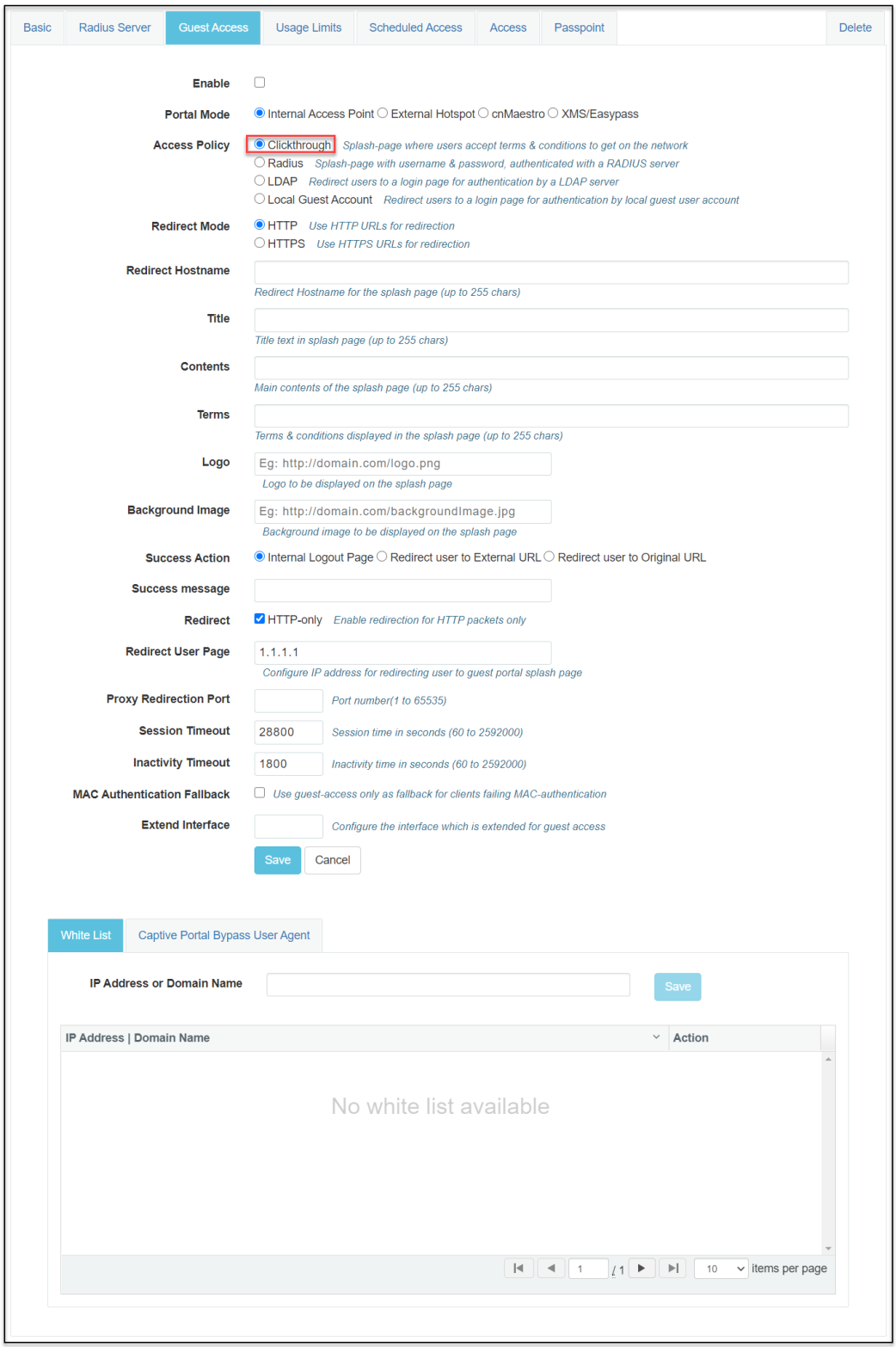


Figure 93: *Authentication – redirected splash page*

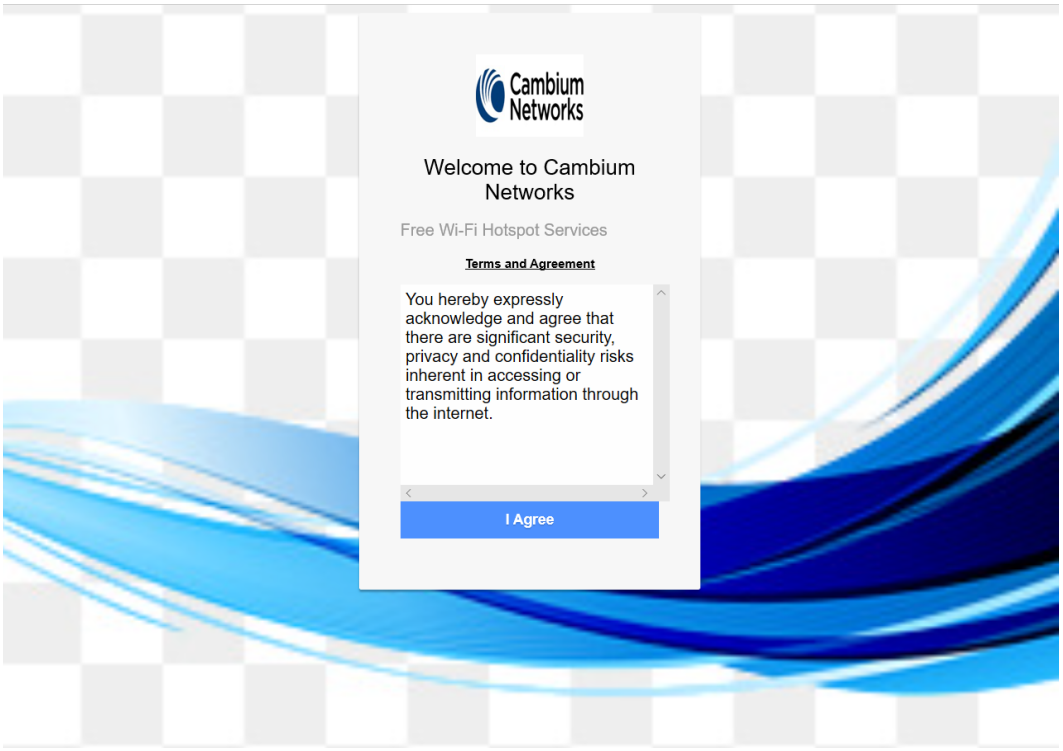
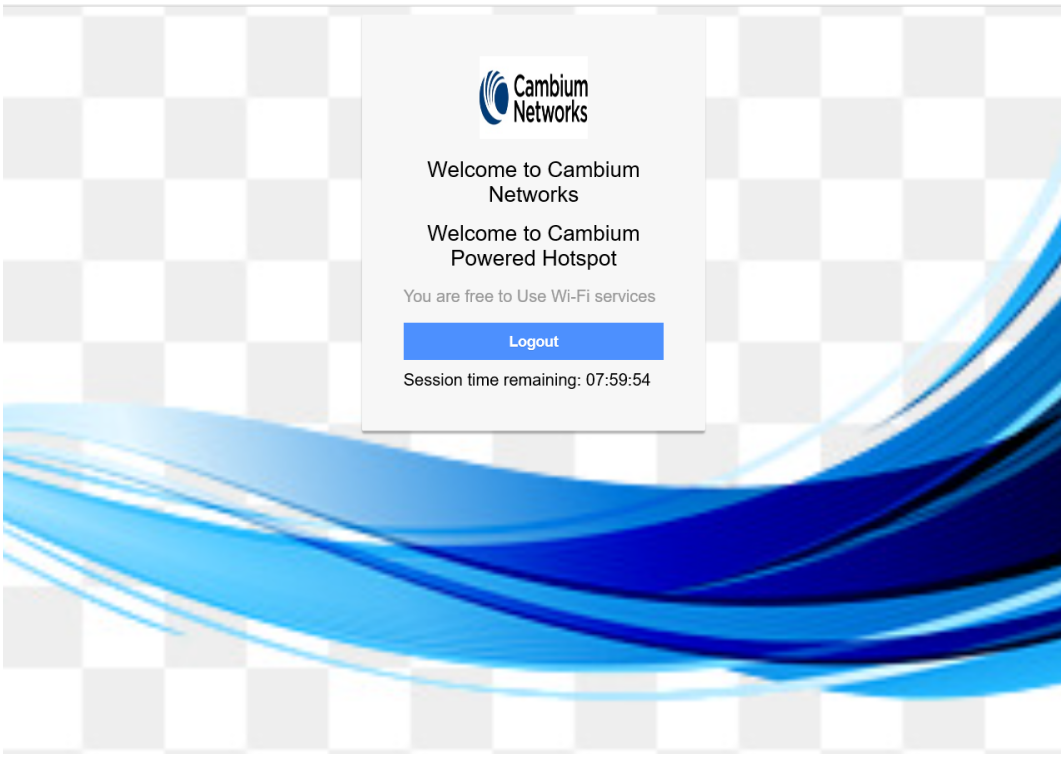


Figure 94: *Successful login – redirected splash page*



Chapter 17: Guest Access Portal - External

Introduction

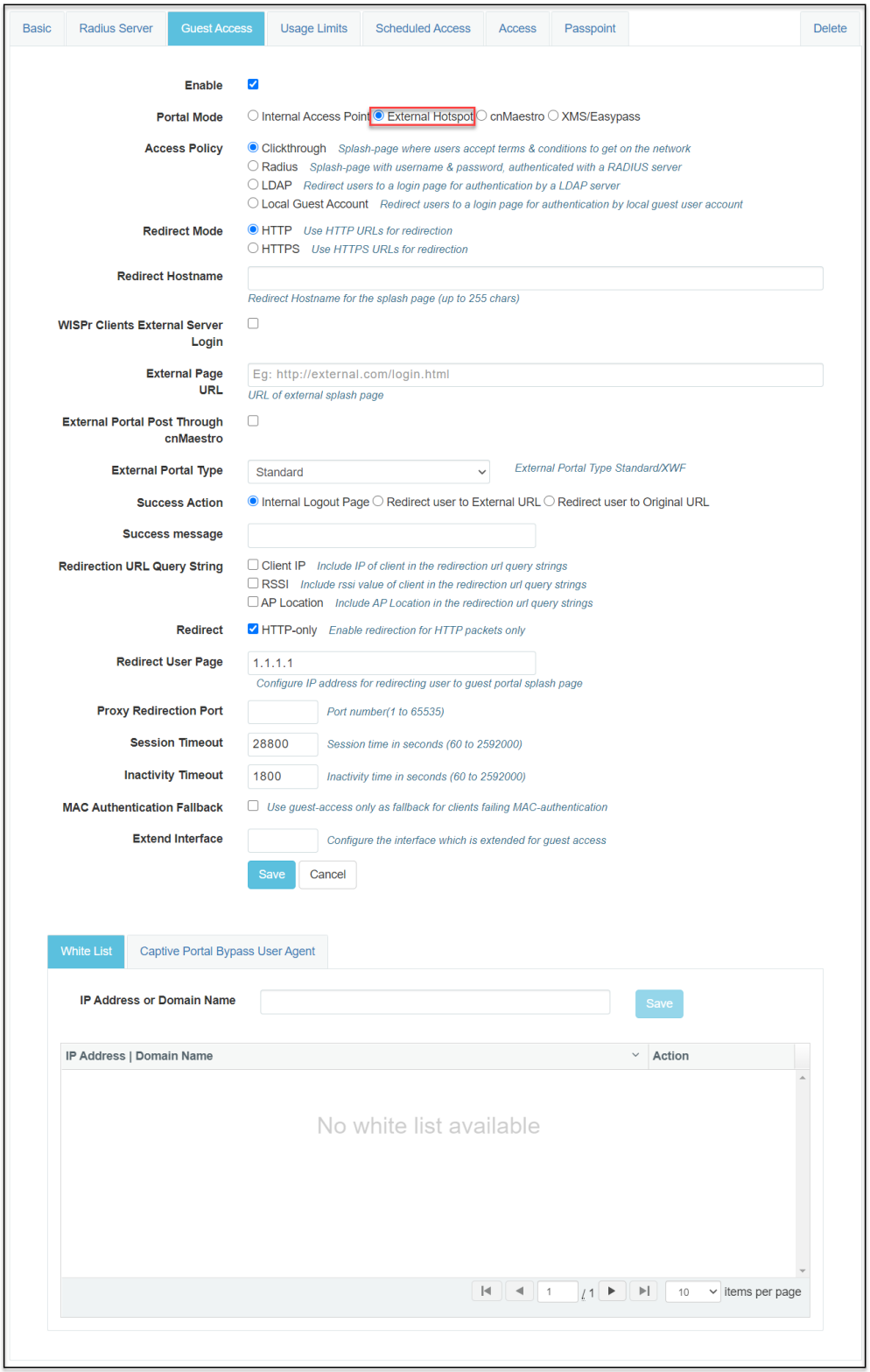
Guest access WLAN is designed specifically for BYOD (Bring Your Own Device) setup, where large organizations have both staff and guests running on the same WLAN or similar WLANs. Cambium Networks provides different options to the customers to achieve this based on where the captive portal page is hosted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

External Hotspot is a smart Guest Access provision supported by Enterprise Wi-Fi AP devices. This method of Guest Access provides the 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 95 displays multiple configurable parameters supported for External Guest Access hosted on AP.

Figure 95: *External Access Point parameter*



Access policy

Clickthrough:

When this policy is selected, the user will get a login page to accept **Terms and Conditions** to get access to the 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 an external guest access portal. This option when enabled minimizes certification. The certificate is required to install only in cnMaestro.

External portal type

Only standard mode configuration is 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. Users can configure three modes of redirection URL:

- Internal logout Page

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

- Redirect users to external URL

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

- Redirect users to the original URL

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

Figure 96: *Success action*

Redirect

By default, captive portal redirection is triggered when the user accesses either HTTP or HTTPS WWW. If enabled, redirection to Captive Portal Splash Page is triggered when an HTTP WWW is accessed by end-

user.

Figure 97: *Redirect*

Redirect mode

There are two redirect modes available:

- HTTP Mode

  When enabled, AP sends an 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

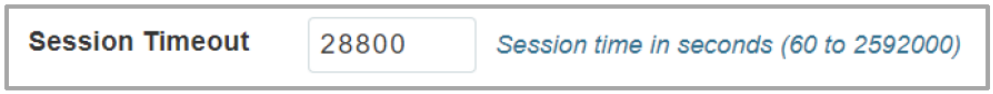
Figure 98: *Success Message*

Timeout

Session

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

Figure 99: *Session timeout*



Inactivity

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

Figure 100: *Inactivity timeout*

Whitelist

Provision to configure either Ips or URLs to bypass traffic, therefor users 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

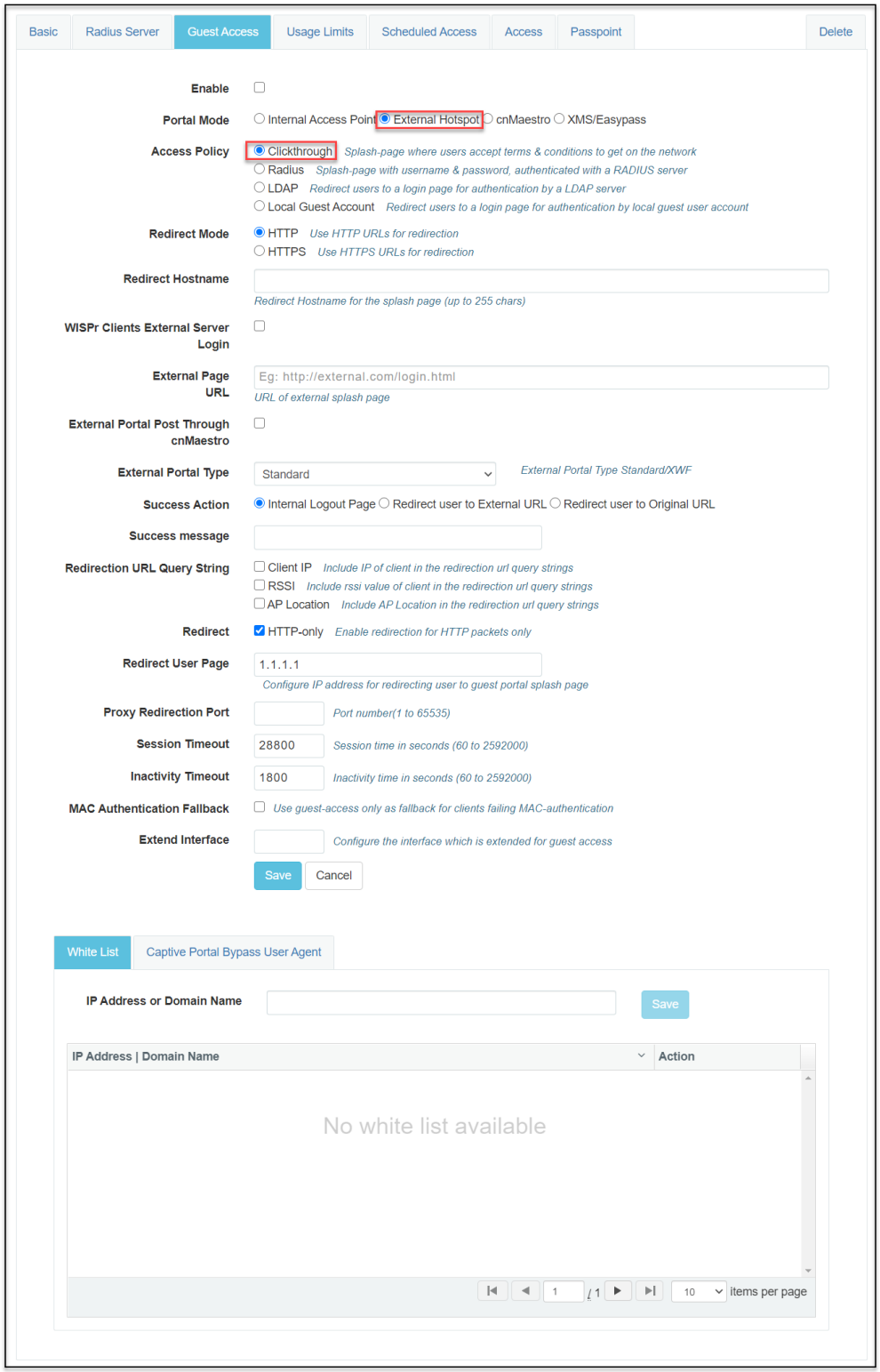


Figure 101: *Authentication – redirected splash page*

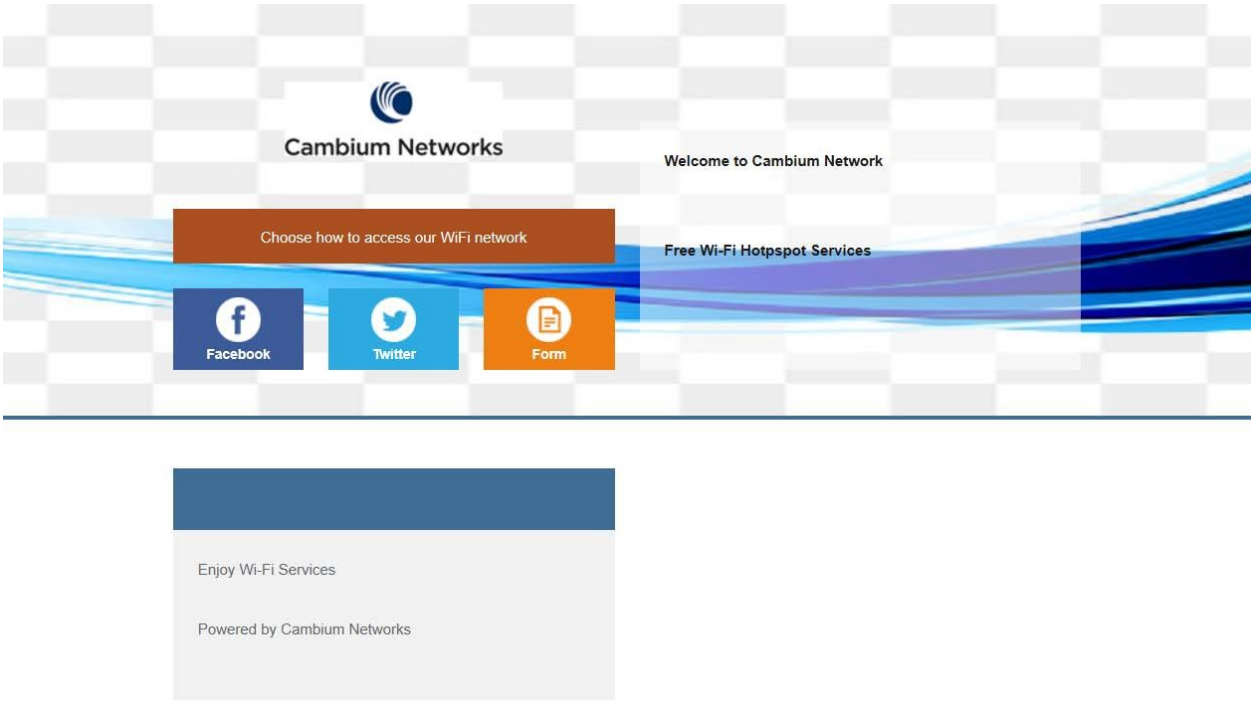
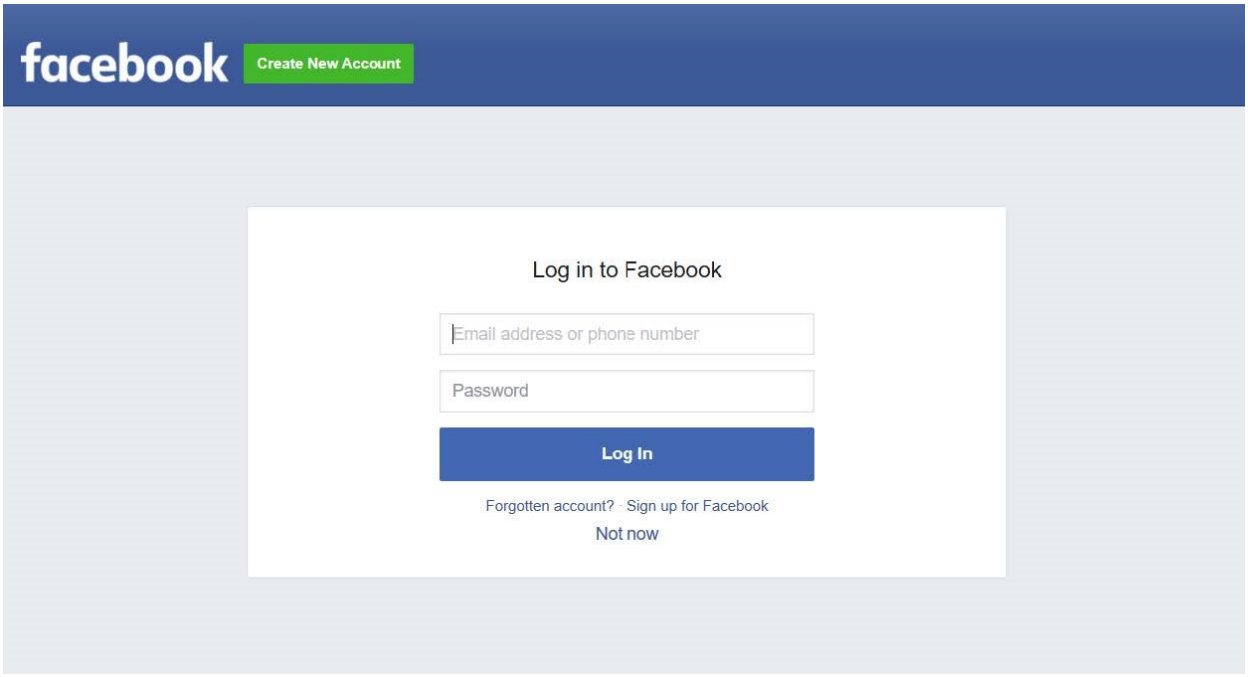


Figure 102: *Successful Login – redirected splash page*



Chapter 18: Guest Access – cnMaestro

Cambium supports end-to-end Guest Access Portal services with a combination of Enterprise Wi-Fi AP and cnMaestro. cnMaestro supports various types of authentication mechanisms 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 the latest *cnMaestro On-Premises User Guide.*
- For cnMaestro Cloud, go to cnMaestro Cloud User Guide.

Chapter 19: Auto VLAN

The Auto VLAN is intended to support zero-touch detection and configuration for connected Enterprise Wi-Fi APs. New Cambium vendor-specific LLDP TLVs are introduced starting with cnMatrix Release 3.1 to support “pushing” PBA policy data from Enterprise Wi-Fi APs to cnMatrix. The new PBA TLVs are implemented as an extension to the LLDP standard, using its flexible extension mechanism.

From a functional perspective, cnMatrix, acting as the upstream device, includes the PBA authentication TLV in the regularly generated LLDPDUs for a port. The downstream device receives the PBA authentication TLV, and, if policy action data (for example VLANs) is present to be pushed to cnMatrix, a PBA device settings TLV is constructed and added to the LLDPDU for the port.

The below table lists the fields that are required for configuring Auto-VLAN:

Table 63: Configuring Auto-VLAN parameters

Parameters	Description	Range	Default
lldp pba	New PBA TLVs is shared with cnMatrix switch.	–	Enabled
lldp pba-auth-key	The shared private key used during PBA TLV authentication can be updated or reset from its default value (by using the ‘no’ option).	–	Enabled with default key

Note

lldp pba-auth-key default value cannot be shared due to security concerns.

CLI configuration:

Syntax:

```
XV3-8-EC7708(config)# lldp
XV3-8-EC7708(config)# lldp pba-auth-key
```

Example:

```
XV3-8-EC7708(config)# lldp pba
XV3-8-EC7708(config)# lldp pba-auth-key 123456789
```

Chapter 20: Device Recovery Methods

Factory reset via 'RESET' button

Table 64: Factory reset via RESET button

Access Point	Procedure	LED Indication
XV3-8	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE5-8	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2T0	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2T1	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE3-4	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE3-4TN	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-21X	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-23T	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-22H	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber

Boot partition change via power cycle

Table 65: Boot partition change via power cycle

Access Point	Procedure
XV3-8	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XE5-8	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2T0	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2T1	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)

Access Point	Procedure
XE3-4	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XE3-4TN	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-21X	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-23T	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-22H	Follow power ON and off 9 times with an interval of 120 Sec (ON) and 5 Sec (OFF)

Disable factory Reset Button

User can disable the physical Reset Button on the device by using the below CLI command:

```
XV3-8-EC7708(config)# no system hw-reset
```

Warning

Please keep in mind that the **Reset Button** is a key recovery option in situations when an AP gets misconfigured and you are not able to connect to the AP so by disabling the Reset Button, you lose the ability to recover the AP in such a scenario.

Chapter 21: Command-Line Interface (CLI)

The Enterprise Wi-Fi products support Command-Line Interface (CLI) which helps in configuring as well as monitoring the devices.

Show commands

The below table provides **Show commands** supported in Enterprise Wi-Fi AP:

Table 66: Show commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
Deep Packet Inspection (DPI)		
1	`show application-statistics by-application`	Displays statistics of each application that is accessed by the station connected to the AP.
2	`show application-statistics by-category`	Displays statistics of application category that is accessed by the station connected to the AP.
Network Information		
3	`show arp`	Displays list of ARP entries learned by AP.
4	`show conntrack`	Displays current connection track entries along with application ID Mapping.
5	`show route`	Displays IP route information.
6	`show dhcp-pool <Index number>`	Displays the DHCP pool configuration.
7	`show interface brief`	Displays interface details such as IP, Netmask, and traffic statistics.
8	`show ip dhcp-client-info`	Displays the DHCP options learned by device across all interfaces.
9	`show ip domain-name`	Displays learned domain name information.
10	`show ip gw-source-precedence`	Displays the Precedence of gateway sources.
11	`show ip interface`	Displays IP interface parameters.
12	`show ip name-server`	Displays DNS server information.
13	`show ip neighbour`	Displays IPv4 neighbour entries.
14	`show ip route`	Displays IP route information.
15	`show ipv6 dhcp-client-info`	Displays learned DHCPv6 client information.
16	`show ipv6 domain-name`	Displays learned domain name information.

SL No	CLI Command	Description
17	`show ipv6 gw-source-precedence`	Displays the precedence of gateway sources.
18	`show ipv6 interface brief`	Displays IPv6 interface parameters.
19	`show ipv6 name-server`	Displays DNS server information.
20	`show ipv6 neighbour`	Displays neighbour entries.
21	`show ipv6 route`	Displays IP route information.
Radio Information		
22	`show auto-rf channel-info`	Displays Auto-RF channel information.
23	`show auto-rf history`	Displays Auto-RF history.
24	`show wireless band-steer client-cache`	Displays band steered client cache.
25	`show wireless mesh ipv6`	Displays IPv6 address of associated mesh clients .
26	`show wireless mesh-xtnded-list`	Displays mesh extended device list for 2.4 GHz when **mesh-xtnded-dev-list** is enabled.
27	`show wireless neighbors 2.4GHz`	Displays 2.4 GHz wireless neighbors.
28	`show wireless neighbors 5GHz`	Displays 5G Hz wireless neighbors.
29	`show wireless neighbors 6GHz`	Displays 6 GHz wireless neighbors.
30	`show wireless neighbors autocell`	Displays Auto-cell neighbors.
31	`show wireless radios channels`	Displays supported channels.
32	`show wireless radios mu-mimo-statistics`	Displays MU-MIMO statistics of Radios.
33	`show wireless radios multicast-to-unicast`	Displays multicast-to-unicast configuration.
34	`show wireless radios ofdma-statistics`	Displays OFDMA statistics of Radios.
35	`show wireless radios rf-statistics`	Displays statistics of Radios.
36	`show wireless radios statistics`	Displays statistics of Radios.
37	`show wireless wlans aggregate-statistics`	Displays aggregate statistics of wireless LANs.
38	`show wireless wlans interface`	Displays wireless WLAN interface details.

SL No	CLI Command	Description
39	`show wireless wlans monitor-host`	Displays monitor host information for wireless LANs.
40	`show wireless wlans statistics`	Displays statistics of wireless LANs.
Bonjour Information		
41	`show bonjour-services`	Displays Bonjour services available.
42	`show bonjour-statistics`	Displays Bonjour rule statistics.
System Information		
43	`show upgrade-status`	Displays last upgrade status.
44	`show version`	Displays device firmware information.
45	`show timezones`	Displays list of timezone locations.
46	`show management details`	Displays management status in detail.
47	`show mfgrom`	Displays manufacturing ROM details.
48	`show country-codes`	Displays a list of supported countries and corresponding country codes.
49	`show boot`	Displays device firmware active-backup versions.
50	`show cambium-id`	Displays configured Cambium-ID (if any).
51	`show clock`	Displays system time.
52	`show config all`	Displays current configuration including defaults.
53	`show config dhcp-pools all`	Displays DHCP pools configuration including defaults.
54	`show config filter`	Displays Filter configuration.
55	`show config wireless all`	Displays wireless configuration including defaults.
56	`show config system all`	Displays infra configuration including defaults.
57	`show config system interfaces`	Displays network interface configuration.
58	`show events`	Displays recent event messages.
Guest Access		
59	`show ext-guest clients`	Displays information of ext-guest clients.
Filters		
60	`show filter-statistics`	Displays filter statistics.
LLDP		
61	`show lldp chassis`	Displays local chassis data.

SL No	CLI Command	Description
62	`show lldp configuration`	Displays configuration.
63	`show lldp interfaces`	Displays interfaces data.
64	`show lldp neighbors`	Displays neighbors data.
65	`show lldp statistics`	Displays statistics.
66	`show power`	Displays power conditions.
67	`show packet-capture status`	Displays status of packet capture.
Real-Time Location System		
68	`show rtls aeroscout ble-tag-summary`	Displays AeroScout BLE-tag summary.
69	`show rtls aeroscout configuration`	Displays AeroScout Wi-Fi-tag configuration.
70	`show rtls aeroscout wifi-tag-summary`	Displays AeroScout Wi-Fi-tag summary.
Tunnel		
71	`show tunnel-statistics`	Displays tunnel statistics.
72	`show tunnel-status details`	Displays tunnel parameters.
73	`show ip pppoe-client-info`	Displays learned PPPoE client information.
74	`show pppoe-status`	Displays PPPoE status.

Service commands

Service show

The below table provides **Service show commands** supported in Enterprise Wi-Fi AP:

Table 67: Service show commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
1	`service show bridge`	Displays AP bridge table entries.
2	`service show client-cache`	Displays current client status and history of clients connected and respective parameters.
3	`service show config`	Displays configuration from data base.
4	`service show cores`	Displays process cores (if any).
5	`service show debug-logs <Process Names>`	Displays debug logs of various processes.
6	`service show df`	Displays flash status.

SL No	CLI Command	Description
7	`service show dmesg`	Displays system kernel logs.
8	`service show epsk`	Displays ePSK information.
9	`service show ethtool`	Displays information and statistics w.r.t Ethernet interfaces.
10	`service show guest-portal whitelist wlan <wlan index>`	Displays whitelist entries either configured or auto-selected by a device in a guest portal WLAN profile.
11	`service show ifconfig`	Displays status and statistics of all interfaces configured and supported on the device.
12	`service show iperfd-logs`	Display IPERF logs when iperfd daemon is enabled on device.
13	`service show iwconfig`	Displays status and statistics of all Wireless interfaces configured on the device.
14	`service show last-reboot-reason`	Displays the reason for the last reboot of the AP.
15	`service show last-reboot-state watchdog`	Displays if the last reboot reason is due to watchdog.
16	`service show mcastsnoop`	Displays multicast-snoop tables.
17	`service show mdnsd-statistics`	Displays mDNS packet stats on mdnsd.
18	`service show memory`	Displays memory information.
19	`service show netstat`	Displays network socket connections.
20	`service show ps`	Displays a list of processes.
21	`service show ps-restart-history`	Displays history of process restart on the AP.
22	`service show route`	Displays routing table.
23	`service show top`	Displays process activity status.

Service system

The below table provides **Service system** commands supported in Enterprise Wi-Fi AP:

Table 68: Service system commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
1	`service boot backup-firmware`	Helps to boot to other partition.
2	`service clear-cores`	Clear system core files (if any).
3	`service clear-dhcp-pool`	Clear DHCP pool allocated addresses.

SL No	CLI Command	Description
4	`service debug <process name>logging-level <logging-level>`	Commands to enable debugging of processes at various logging levels.
5	`service flash-leds`	Flash system LEDs help identify this device visually.
6	`service radio apstats`	Displays aggregate statistics of all wireless interfaces.
7	`service radio athstats`	Displays aggregate Radio traffic statistics.
8	`service radio iwpriv`	Displays supported iwpriv commands.
9	`service radio thermaltool`	Displays radio current operating temperature.
10	`service schedule reload`	Reboot AP at the specified time.
11	`service ssh host add`	Add a host and key to the known hosts list.
12	`service ssh host del`	Delete a host and key from the known hosts list.
13	`service system-trace`	Start a trace session for troubleshooting.
14	`service test leds`	Displays test LEDs.
15	`service test radio`	Displays status and configured Radio.

Chapter 22: cnMaestro X Assurance

Note:

This feature is available from cnMaestro 4.1.0 and later versions only.

The cnMaestro X Assurance feature provides enhanced visibility into the health of Wi-Fi client connections, including root cause analysis of failures with possible recommended actions. It also provides analytics on aggregated data that can help to improve clients connectivity in the Wi-Fi network.

Note:

This feature is currently available as a free trial to all cnMaestro X customers. In future, this feature will require a separate paid subscription.

The cnMaestro X Assurance feature analyzes the Wi-Fi client connection events and helps to troubleshoot common network connectivity and performance issues such as the following:

- Connectivity—Association, authentication, and network connectivity services, such as DHCP and DNS transaction failures.
- Poor Performance—Low RSSI, low data rate, AAA, DHCP, DNS transaction latency.

For more information, refer to the *cnMaestro User Guide*.

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.
BT	Bluetooth
DFS	See Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol defined in RFC 2131. The 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	The 32-bit binary number identifies a network element by both network and host. See also Subnet Mask.
IPv4	The traditional version of Internet Protocol, defines 32-bit fields for data transmission.
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.
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.

Term	Definition
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.
PoE	Power over Ethernet.
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	A 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 are 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.

Appendix

This appendix contains the following topics:

- Supported RADIUS Attributes
- Supported DFS channels
- Supported 6 GHz countries

Supported RADIUS Attributes

This topic lists the following RADIUS override attributes that are supported on Enterprise Wi-Fi APs:

- WISPr VSAs (Vendor ID: 14122)
- Cambium VSAs (Vendor ID: 17713)
- Standard RADIUS attributes
- RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security
- Supported CoA messages

WISPr VSAs (Vendor ID: 14122)

Table 69 lists the WISPr vendor-specific attributes (VSAs) supported on Enterprise Wi-Fi APs.

Table 69: WISPr VSAs

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
2	WISPr-Location-Name	string	Yes	-NA-	No	Yes	Yes	Yes	Yes	Yes
7	WISPr-Bandwidth-Max-Up	integer	No	No	Yes	No	No	No	Yes	Yes
8	WISPr-Bandwidth-Max-Down	integer	No	No	Yes	No	No	No	Yes	Yes
9	WISPr-Session-Terminate-Time	string	No	No	Yes	No	No	No	Yes	Yes

Table 70 lists the WISPr VSAs supported on Enterprise Wi-Fi APs with CoA support.

Table 70: WISPr VSAs with CoA

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
2	WISPr-Location-Name	string	Yes	-NA-	No	Yes	Yes	Yes	-NA-	-NA-
7	WISPr-Bandwidth-Max-Up	integer	No	No	Yes	No	No	No	Yes	Yes
8	WISPr-Bandwidth-Max-Down	integer	No	No	Yes	No	No	No	Yes	Yes
9	WISPr-Session-Terminate-Time	string	No	No	Yes	No	No	No	Yes	Yes

Cambium VSAs (Vendor ID: 17713)

Table 71 lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs.

Table 71: Cambium VSAs

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
151	Cambium-Wi-Fi-Quota-Up	integer	No	No	Yes	No	No	No	-NA-	Yes
152	Cambium-Wi-Fi-Quota-Down	integer	No	No	Yes	No	No	No	-NA-	Yes
155	Cambium-Wi-Fi-Quota-Total	integer	No	No	Yes	No	No	No	-NA-	Yes
153	Cambium-Wi-Fi-Quota-Up-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes
154	Cambium-Wi-Fi-Quota-Down-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
156	Cambium-Wi-Fi-Quota-Total-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes
157	Cambium-VLAN-Pool-ID	string	No	No	Yes	No	No	No	Yes	No
159	Cambium-Traffic-Classes-Acct	TLV								
159.2	Cambium-Acct-Input-Octets	integer	No	No	No	No	Yes	Yes		
159.3	Cambium-Acct-Output-Octets	integer	No	No	No	No	Yes	Yes		
159.4	Cambium-Acct-Input-Packets	integer	No	No	No	No	Yes	Yes		
159.5	Cambium-Acct-Output-Packets	integer	No	No	No	No	Yes	Yes		
161	Cambium-ePSK	TLV							-NA-	Yes
161.1	Cambium-ePSK-Anonce	octet	Yes	-NA-	No				-NA-	Yes
161.2	Cambium-ePSK-M2	octet	Yes	-NA-	No				-NA-	Yes
161.3	Cambium-ePSK-BSSID	octet	Yes	-NA-	No				-NA-	Yes
161.4	Cambium-ePSK-AP-MAC	octet	Yes	-NA-	No				-NA-	Yes
161.5	Cambium-ePSK-SSID	string	Yes	-NA-	No				-NA-	Yes
161.6	Cambium-ePSK-PMK	string	No	-NA-	Yes				-NA-	Yes

Table 72 lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs with CoA.

Table 72: Cambium VSAs with CoA

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
151	Cambium-Wi-Fi-Quota-Up	integer	No	No	Yes	No	No	No	Yes	
152	Cambium-Wi-Fi-Quota-Down	integer	No	No	Yes	No	No	No	Yes	
155	Cambium-Wi-Fi-Quota-Total	integer	No	No	Yes	No	No	No	Yes	
153	Cambium-Wi-Fi-Quota-Up-Gigaword	integer64	No	No	Yes	No	No	No	Yes	
154	Cambium-Wi-Fi-Quota-Down-Gigaword	integer64	No	No	Yes	No	No	No	Yes	
156	Cambium-Wi-Fi-Quota-Total-Gigaword	integer64	No	No	Yes	No	No	No	Yes	
157	Cambium-VLAN-Pool-ID	string	No	No	Yes	No	No	No		
159	Cambium-Traffic-Classes-Acct	TLV								
159.2	Cambium-Acct-Input-Octets	integer	No	No	No	No	Yes	Yes		
159.3	Cambium-Acct-Output-Octets	integer	No	No	No	No	Yes	Yes		
159.4	Cambium-Acct-Input-Packets	integer	No	No	No	No	Yes	Yes		
159.5	Cambium-Acct-Output-Packets	integer	No	No	No	No	Yes	Yes		
161	Cambium-ePSK	TLV							-NA-	-NA-
161.1	Cambium-ePSK-Anonce	octet	Yes	-NA-	No				-NA-	-NA-

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
161.2	Cambium-ePSK-M2	octet	Yes	-NA-	No				-NA-	-NA-
161.3	Cambium-ePSK-BSSID	octet	Yes	-NA-	No				-NA-	-NA-
161.4	Cambium-ePSK-AP-MAC	octet	Yes	-NA-	No				-NA-	-NA-
161.5	Cambium-ePSK-SSID	string	Yes	-NA-	No				-NA-	-NA-
161.6	Cambium-ePSK-PMK	string	No	-NA-	Yes				-NA-	-NA-

Standard RADIUS attributes

Table 73 lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs.

Table 73: Standard RADIUS attributes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
11	Filter-Id (text) - Group-ID	text	No	-NA-	Yes	No	No	No	Yes	
24	State	string	Yes	Yes	No				Yes	-NA-
25	Class	string	No	-NA-	Yes	Yes	No	No	Yes	Yes
27	Session-Timeout	integer	No	-NA-	Yes	No	No	No	Yes	Yes
28	Idle-Timeout	integer	No	-NA-	Yes	No	No	No		Yes
64	Tunnel-Type	enum	No	-NA-	Yes	No	No	No	Yes	Yes
65	Tunnel-Medium-Type	enum	No	-NA-	Yes	No	No	No	Yes	Yes
81	Tunnel-Private-Group-Id	text	No	-NA-	Yes	No	No	No	Yes	Yes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			WPA2 / WPA3 - Enterprise Authentication Support	Guest Access Support
			Request	Response / Challenge	Accept	Start	Interim	Stop		
85	Acct-Interim-Interval	integer	No	-NA-	Yes	No	No	No	Yes	Yes
	Disconnect		RADIUS packet							
40	Disconnect-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	-NA-	-NA-
41	Disconnect-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
42	Disconnect-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
43	CoA-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
44	CoA-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		
45	CoA-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-		

Table 74 lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs with CoA support.

Table 74: Standard RADIUS attributes with CoA

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
11	Filter-Id (text) - Group-ID	text	No	-NA-	Yes	No	No	No	Yes	Yes
24	State	string	Yes	Yes	No					Yes

Attribute Value	Attribute Description	Attribute Type	RADIUS Message Types			Accounting Messages			CoA Support with Guest Access	CoA Support with WPA2 / WPA3 - Enterprise Authentication
			Request	Response / Challenge	Accept	Start	Interim	Stop		
25	Class	string	No	-NA-	Yes	Yes	No	No	-NA-	-NA-
27	Session-Timeout	integer	No	-NA-	Yes	No	No	No	-NA-	-NA-
28	Idle-Timeout	integer	No	-NA-	Yes	No	No	No	-NA-	-NA-
64	Tunnel-Type	enum	No	-NA-	Yes	No	No	No	-NA-	-NA-
65	Tunnel-Medium-Type	enum	No	-NA-	Yes	No	No	No	-NA-	-NA-
81	Tunnel-Private-Group-Id	text	No	-NA-	Yes	No	No	No	No	Yes
85	Acct-Interim-Interval	integer	No	-NA-	Yes	No	No	No		
	Disconnect		RADIUS packet							
40	Disconnect-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
41	Disconnect-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
42	Disconnect-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
43	CoA-Request	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
44	CoA-ACK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes
45	CoA-NAK	-	RADIUS packet	-NA-	-NA-	-NA-	-NA-	-NA-	Yes	Yes

RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security

Table 75 lists the RADIUS attributes supported in authentication and accounting packets with WPA2-Enterprise security.

Table 75: RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
1	User-Name	string	Yes	No	Yes	Yes	Yes	Yes
2	User-Password	string	Yes	No	No	No	No	No
4	NAS-IP-Address	ipv4addr	Yes	No	No	Yes	Yes	Yes
5	NAS-Port	integer	Yes	No	No	Yes	Yes	Yes
6	Service-Type	enum	Yes	No	No	Yes	Yes	Yes
8	Framed-IP-Address	ipv4addr	No	No	No	Yes	Yes	Yes
12	Framed-MTU	integer	Yes	No	No	Yes	Yes	Yes
24	State	string	Yes	Yes	No	No	No	No
25	Class	string	No	No	Yes	Yes	Yes	Yes
27	Session-Timeout	integer	No	No	Yes	No	No	No
28	Idle-Timeout	integer	No	No	Yes	No	No	No
30	Called-Station-Id	string	Yes	No	No	Yes	Yes	Yes
31	Calling-Station-Id	text	Yes	No	No	Yes	Yes	Yes
32	NAS-Identifier	string	Yes	No	No	Yes	Yes	Yes
40	Acct-Status-Type	enum	No	No	No	Yes	Yes	Yes
41	Acct-Delay-Time	integer	No	No	No	Yes	Yes	Yes
42	Acct-Input-Octets	integer	No	No	No	No	Yes	Yes

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
43	Acct-Output-Octets	integer	No	No	No	No	Yes	Yes
44	Acct-Session-Id	text	Yes	No	No	Yes	Yes	Yes
45	Acct-Authentic	enum	No	No	No	Yes	Yes	Yes
46	Acct-Session-Time	integer	No	No	No	No	Yes	Yes
49	Acct-Terminate-Cause	enum	No	No	No	No	No	Yes
50	Acct-Multi-Session-Id	text	Yes (Empty)	No	No	Yes	Yes	Yes
52	Acct-Input-Gigawords	integer	No	No	No	No	No	No
53	Acct-Output-Gigawords	integer	No	No	No	No	No	No
55	Event-Timestamp	time	No	No	No	Yes	Yes	Yes
61	NAS-Port-Type	integer	Yes	No	No	Yes	Yes	Yes
77	Connect-Info	text	Yes	No	No	Yes	Yes	Yes
79	EAP-Message	concat	Yes	Yes	Yes	No	No	No
80	Message-Authenticator	string	Yes	Yes	Yes	No	No	No
85	Acct-Interim-Interval	integer	No	No	Yes	No	No	No
87	NAS-Port-Id	text	Yes	No	No	Yes	Yes	Yes

Supported CoA messages

Table 76 lists the supported CoA messages.

Table 76: CoA messages

CoA Message	Supported by MAB (Wired Clients)	Supported by the AP
Disconnect client	Yes	Yes
Update VLAN	Yes	Yes
Session Timeout	No	Yes
Accounting Interval	Yes	Yes
Quota Limit	No	Yes

Note

Following are the mandatory parameters to be included in the CoA message:

- When sent through cnMaestro—User-Name, Calling-Station-Id, and Session ID
- When sent directly through the AP—User-Name, Calling-Station-Id, and NAS-Identifier

Supported DFS channels

Table 77 lists the DFS channel support for various platforms in conformance with FCC standards.

Table 77: DFS channel support for FCC

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XE3-4TN	Yes	Yes	Yes
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	Yes
XV3-8	Yes	Yes	Yes
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

Table 78 lists the DFS channel support for various platforms in conformance with IC standards.

Table 78: DFS channel support for IC

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XE3-4TN	Yes	Yes	Yes
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	Yes
XV3-8	Yes	Yes	Yes
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

Table 79 lists the DFS channel support for various platforms in conformance with CE standards.

Table 79: DFS channel support for CE

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XE3-4TN	Yes	Yes	Yes
XV2-22H	Yes	Yes	Yes

AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	No
XV3-8	No	Yes	No
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

Supported 6 GHz countries

Table 80 lists the countries where 6 GHz band is available and the frequencies supported.

Note

Availability of these channels is subjected to respective country regulations.

6 GHz frequency is supported only on the following Enterprise Wi-Fi APs: XE3-4, XE3-4TN, and XE5-8.

Table 80: List of countries where 6 GHz band is supported

Country	XE3-4		XE5-8			
	Frequencies Supported	Channels Supported	Frequencies Supported	Channels Supported (No Channel Distribution)	Channels Supported (With Channel Distribution Enabled)	
					Radio 2	Radio 3
Australia (AU)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Brazil (BR)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	129-233
Canada (CA)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	97-233
Colombia (CO)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	129-233
France (FR)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Germany (DE)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Ireland (IE)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93

Country	XE3-4		XE5-8			
	Frequencies Supported	Channels Supported	Frequencies Supported	Channels Supported (No Channel Distribution)	Channels Supported (With Channel Distribution Enabled)	
					Radio 2	Radio 3
Italy (IT)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Jordan (JO)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
South Korea (KR)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	97-233
Netherlands (NL)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
New Zealand (NZ)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
South Africa (ZA)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Spain (ES)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
Sweden (SE)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
United Kingdom (GB)	5945-6425 MHz	1-93	5945-6425 MHz	1-93	1-61	65-93
United States (US)	5945-7125 MHz	1-233	5945-7125 MHz	1-233	1-93	129-233

Priority Order for Parameters

This section provides information on the order of priority for the following parameters:

- **Session timeout and inactivity timeout**—Following priority is considered when configuring session timeout and inactivity timeout:

    a. Configured from the RADIUS server

    b. Configured from the AP

Note

- Inactivity timeout is triggered when there is no data packets from the client to the AP.
- A five minute static idle time is configured from the driver, which is triggered when there are no wireless packets from the client.

- **VLAN assignment**—Following priority is considered when assigning VLANs to clients:
    a. RADIUS dynamic VLAN for guest access clients
    b. RADIUS dynamic VLAN (Filter-ID/RADIUS-ID)
    c. RADIUS dynamic VLAN
    d. RADIUS-based ePSK
    e. RADIUS-based dynamic VLAN Pool
    f. Local ePSK VLAN setting
    g. VLAN pool (Static)
    h. SSID/WLAN profile VLAN
- **User group filter**—Following priority is considered for assigning policy:
    a. Global policy
    b. User Group policy
    c. Device Group policy
    d. SSID/WLAN policy

Best Practices for Wireless Clients Seamless Roaming across APs

Note

- Inactivity timeout is triggered when there is no data packets from the client to the AP.
- A five minute static idle time is configured from the driver, which is triggered when there are no wireless packets from the client.

This appendix explains the recommended configuration for Cambium Networks APs and external network to facilitate a seamless roaming across the APs for the wireless clients. Additionally, this appendix also lists the recommended network best practices for minimizing broadcast and multicast packets processing.

This appendix contains the following topics:

External network recommendations

The Cambium APs work in the distributed architecture mode and it is important to facilitate AP-to-AP communication for the wireless clients seamless roaming. The APs uses the Cambium propriety XRP

protocol to exchange clients information with the neighboring APs.

Following are the recommendations:

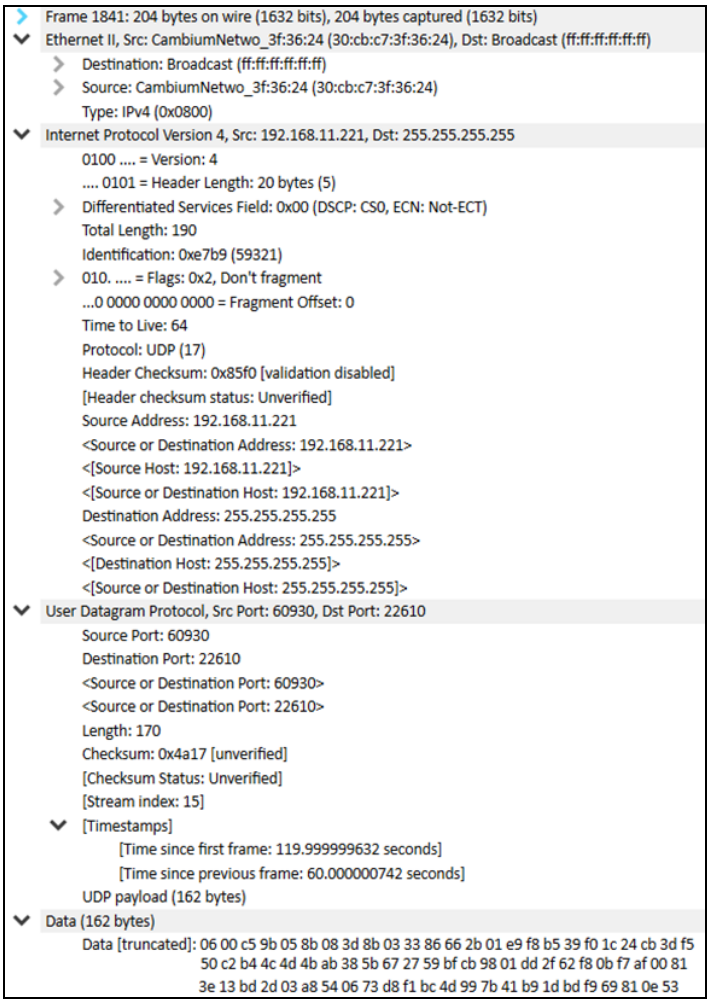
- The intermediate network switches, to which the APs are connected, must not block the following XRP messages:

  XRP message packet information

  - Source MAC—APs ethernet MAC
  - Destination MAC—Ethernet broadcast
  - Source IP Address—APs exit interface IP address
  - Destination IP Address—255.255.255.255 Broadcast IP address
  - Protocol—UDP with a random source port and a fixed destination port

  A sample pcap capture of the XRP message is displayed in Figure 103.

  Figure 103: *Sample XRP message*



- APs send the XRP messages on the ethernet port's native VLAN.

- All the APs must be part of the same native VLAN.
- Make sure that the APs have the L3 interface for the native VLAN with a valid IP address.

AP WLAN profile configuration recommendations

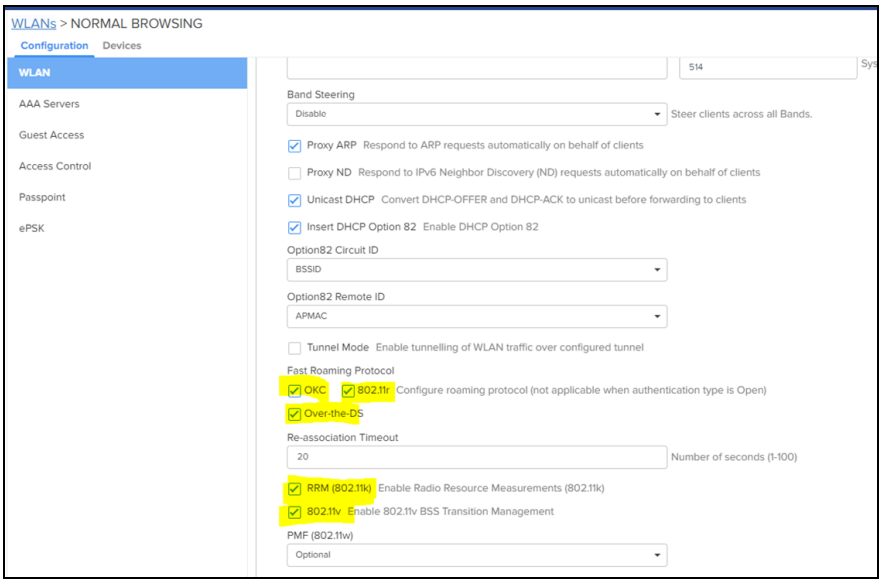
If the WLAN profile is configured with WPA2 and WPA3 security, it is recommended to enable the following:

- 802.11r fast roaming
- OKC

Note

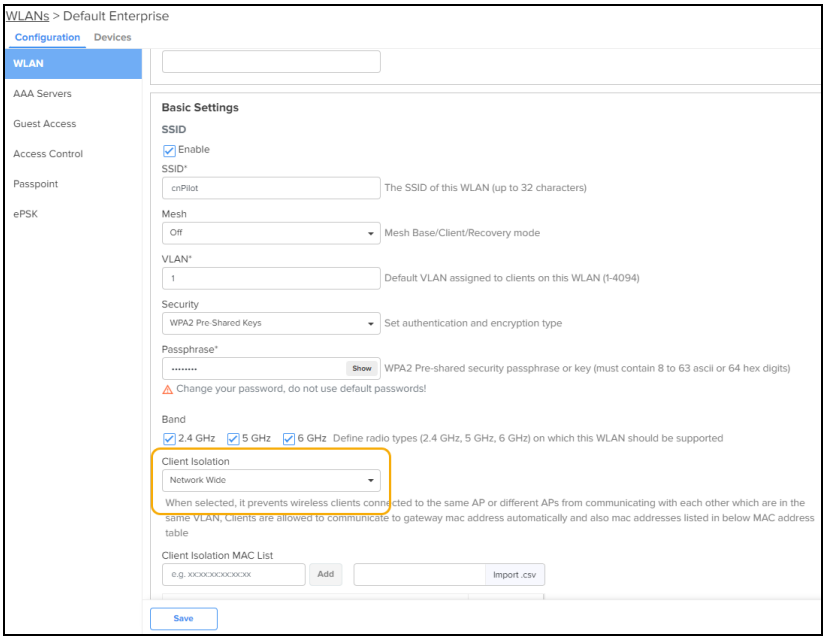
A few clients use 802.11k and 802.11v protocols for fast roaming. We can enable the same.

Figure 104: *Enabling OKC and 802.11r*



- Enable client isolation with the **Network Wide** option to prevent clients communicating with other clients on the same L2 network.

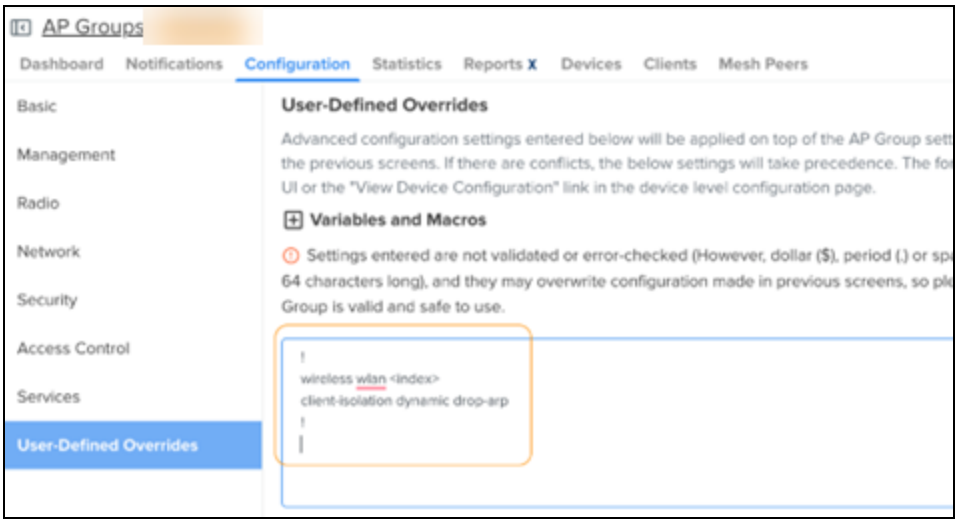
Figure 105: *Enabling Client Isolation*



Note

From AP version 6.6.0.2, the AP drops the ARP packets when the client isolation feature is enabled. To enable this in APs running firmware version lesser than 6.6.0.2, execute the `client-isolation dynamic drop-arp` CLI command from the AP group **User-Defined Overrides** section.

Figure 106: *Enabling Client Isolation in User-Defined Overrides*



AP group configuration recommendations

- In large public Wi-Fi and campus deployments, it is common to see large number of network discovery protocols, such as mDNS, LLMNR, SSDP and other service discovery packets coming

from the wireless clients.

Disable these packets using **Access Control Policy**.

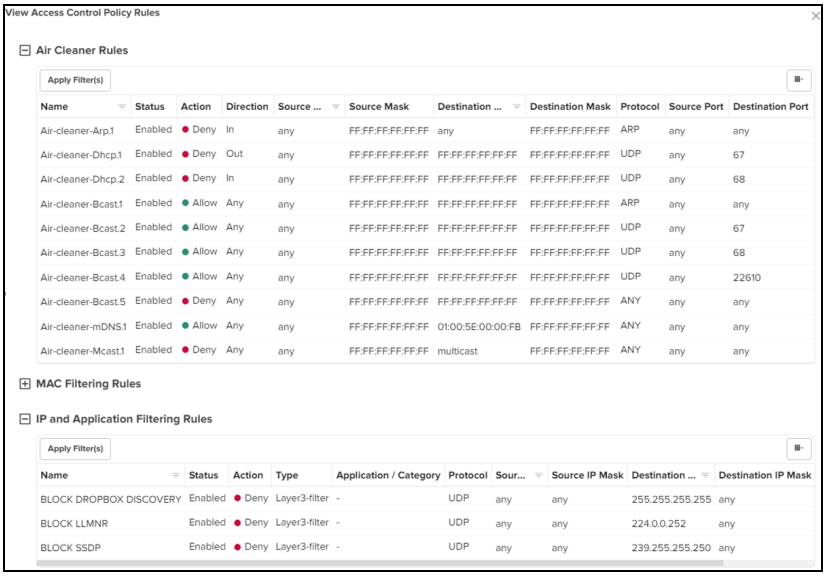
- If IPv6 is not required, disable IPv6 packets from the wireless clients using **Access Control Policy**.
- Use **Air Cleaner Rules** to:
    - prevent unauthorized rogue DHCP server from wireless clients
    - prevent unwanted DHCP client packets from wired network side
    - drop L2 broadcast packets
    - drop IPv4 and IPv6 multicast packets
    - drop ARP discovery packets from one SSID to another SSID interface
    - disable mDNS packets in the default Air Cleaner rules

Note

Allow the mDNS packet to enable bonjour discovery service to work.

- Sample AP group policy with **Air Cleaner Rules**.

Figure 107: *Sample AP group policy with Air Cleaner Rules*



Sample user-defined rule for blocking IPv6 traffic and allowing the rest of the traffic.

```
!
filter global-filter
filter precedence 14
```

```
enable
layer3-filter deny proto6 any any any any any any //BLOCK IPv6 TRAFFIC
exit
filter precedence 15
enable
layer3-filter permit ip any/any any/any any //ALLOW TRAFFIC
exit
!
```

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Support website	https://support.cambiumnetworks.com
Support enquiries	
Technical training	https://learning.cambiumnetworks.com/learn
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
User Guides	http://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Cambium Networks™

www.cambiumnetworks.com