



USER GUIDE

Enterprise Wi-Fi Access Point

System Release 6.5.3



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

## **Restrictions**

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

## **License Agreements**

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

## **High Risk Materials**

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

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

---

<b>Contents</b> .....	<b>3</b>
<b>About This User Guide</b> .....	<b>10</b>
Overview of Enterprise Wi-Fi AP products .....	10
Intended audience .....	10
Purpose .....	10
Related documents .....	10
Existing hardware platforms .....	11
Premium feature list .....	12
<b>Chapter 1: Quick Start – Device Access</b> .....	<b>13</b>
Powering up the device .....	13
PoE switches (802.3af/802.3at/802.3bt) .....	13
PoE adapter .....	14
DC Power supply .....	15
Accessing the device .....	15
Device access using default/fallback IP .....	16
Device access using zeroconf IP .....	17
Device access using DHCP IP address .....	18
LED Status .....	18
<b>Chapter 2: Onboarding the Device</b> .....	<b>20</b>
Overview .....	20
Device Onboarding and provisioning .....	20
cnMaestro .....	20
XMS-Cloud .....	20
Swift .....	20
<b>Chapter 3: Using the UI</b> .....	<b>22</b>
Logging into the UI .....	22
Viewing the Home page (dashboard) .....	23
Monitor .....	25

Configure .....	26
Operations .....	26
Troubleshoot .....	26
<b>Chapter 4: Configuring the System .....</b>	<b>27</b>
Basic .....	27
Power over Ethernet (PoE) in .....	29
Power over Ethernet (PoE) Out port .....	31
Link Layer Discovery Protocol (LLDP) .....	31
Management .....	33
Administrator Access .....	33
HTTPS Proxy server configuration .....	36
Time settings .....	36
Event logging .....	37
SNMP .....	38
<b>Chapter 5: Configuring the Radio .....</b>	<b>40</b>
Overview .....	40
Configuring Radio parameters .....	40
Basic .....	40
Software Define Radio (SDR) capabilities .....	47
Enhanced Roaming .....	49
BSS Coloring .....	50
Target Wake Time (TWT) .....	50
Receive sensitivity configuration .....	50
Multicast-snooping and Multicast-to-Unicast conversion .....	50
<b>Chapter 6: Configuring the Wireless LAN .....</b>	<b>52</b>
Overview .....	52
Configuring the WLAN parameters .....	52
Basic .....	52
WLAN VLAN allowed list .....	65
ICMPv6 Router advertisement (RA) unicast conversion .....	66

802.11k/v .....	66
Radius server .....	66
Guest Access .....	70
Usage Limits .....	86
Scheduled Access .....	86
Access .....	88
Passpoint .....	91
Radius attributes .....	93
enhanced PSK (ePSK) .....	94
RADIUS based ePSK Premium feature .....	95
Groupwise Transient Key (GTK) per VLAN .....	96
<b>Chapter 7: Configuring the Network .....</b>	<b>97</b>
Overview .....	97
Configuring Network parameters .....	97
IPv4 network parameters .....	97
Routes .....	102
IPv6 network parameters .....	105
General network parameters .....	109
Ethernet Ports .....	109
General network parameters .....	110
Security .....	111
DHCP .....	112
Tunnel .....	114
Point-to-Point Protocol over Ethernet (PPPoE) .....	117
VLAN Pool .....	119
Wireless Wide Area Network (WWAN) .....	121
<b>Chapter 8: Managing Filters .....</b>	<b>123</b>
Overview .....	123
Filter list .....	123
Filters .....	123

Configuring filter CLI .....	123
Device class filter .....	127
Wi-Fi Calling support .....	128
Air cleaner .....	128
Application control Premium feature .....	130
Deep Packet Inspection (DPI) .....	130
<b>Chapter 9: Wireless Intrusion Detection Systems (WIDS)Premium feature .....</b>	<b>143</b>
Wireless flood detection .....	143
Neighbour/Rogue AP detection .....	143
Ad Hoc network detection .....	143
<b>Chapter 10: Configuring Services .....</b>	<b>145</b>
Overview .....	145
Configuring services .....	145
User Groups Premium feature .....	145
Location API .....	147
Speed Test .....	148
BT location API .....	149
Bonjour Gateway .....	150
Link Aggregation Control Protocol (LACP) .....	152
Real Time Location System (RTLS) .....	153
<b>Chapter 11: Operations .....</b>	<b>154</b>
Overview .....	154
Firmware upgrade .....	154
System .....	155
LED Test flashing pattern .....	156
Configuration .....	156
<b>Chapter 12: Troubleshoot .....</b>	<b>158</b>
Overview .....	158
Logging .....	158
Events .....	158

Debug Logs .....	159
Radio Frequency (RF) .....	159
Wi-Fi Analyzer .....	159
Packet capture .....	161
Performance .....	162
Speedtest on Access Point .....	162
Connectivity .....	162
XIRCON tool support .....	166
XIRCON tool support for Linux 1.0.0.40 .....	166
<b>Chapter 13: Management Access .....</b>	<b>167</b>
Local authentication .....	167
Device configuration .....	167
SSH Key authentication .....	167
Device configuration .....	168
SSH Key generation .....	168
RADIUS authentication .....	170
Device configuration .....	171
<b>Chapter 14: Mesh .....</b>	<b>172</b>
Deployment scenarios .....	172
Mesh configurable parameters .....	174
Order of Mesh profile configuration .....	176
Mesh Auto Detect Backhaul .....	182
Scenario 1 .....	182
Scenario 2 .....	183
Scenario 3 .....	184
Mesh Muti-Hop .....	187
Mesh Roaming .....	188
Mesh Base configuration .....	188
Mesh Client configuration .....	189
Mesh link-Sample configuration .....	190

VLAN 1 as the management interface .....	190
Non-VLAN 1 as the management interface .....	194
Typical use-cases .....	198
<b>Chapter 15: Guest Access Portal - Internal .....</b>	<b>200</b>
Introduction .....	200
Configurable parameters .....	201
Access policy .....	202
Splash page .....	203
Redirect parameters .....	203
Success message .....	204
Timeout .....	204
Whitelist .....	205
Configuration examples .....	205
Access Policy - Clickthrough .....	206
<b>Chapter 16: Guest Access Portal - External .....</b>	<b>208</b>
Introduction .....	208
Configurable parameters .....	208
Access policy .....	210
WISPr .....	210
External portal post through cnMaestro .....	210
External portal type .....	210
Redirect parameters .....	210
Success message .....	211
Timeout .....	211
Whitelist .....	212
Configuration examples .....	212
Access Policy - Clickthrough .....	213
<b>Chapter 17: Guest Access - cnMaestro .....</b>	<b>215</b>
<b>Chapter 18: Auto VLAN .....</b>	<b>216</b>
<b>Chapter 19: Device Recovery Methods .....</b>	<b>217</b>



Factory reset via 'RESET' button .....	217
Boot partition change via power cycle .....	218
Disable factory Reset Button .....	218
<b>Chapter 20: Command Line Interface (CLI) .....</b>	<b>219</b>
Show commands .....	219
Service commands .....	222
Service show .....	222
Service system .....	223
<b>Glossary .....</b>	<b>225</b>
<b>Appendix .....</b>	<b>227</b>
Supported RADIUS Attributes .....	228
WISPr VSAs (Vendor ID: 14122) .....	228
Cambium VSAs (Vendor ID: 17713) .....	229
Standard RADIUS attributes .....	232
RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security .....	234
Supported CoA messages .....	236
Supported DFS channels .....	238
<b>Cambium Networks .....</b>	<b>240</b>

# About This User Guide

---

This section describes the following topics:

- [Overview of Enterprise Wi-Fi AP products](#)
- [Intended audience](#)
- [Purpose](#)
- [Related documents](#)
- [Hardware platforms](#)
- [Premium Feature List](#)

## Overview of Enterprise Wi-Fi AP products

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

## Intended audience

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

## Purpose

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

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

## Related documents

Table 1 provides details of related documents for Enterprise Wi-Fi AP.

Table 1: Related documents

Document Name	Location
Enterprise Wi-Fi AP product details	<a href="https://www.cambiumnetworks.com/products/wifi/">https://www.cambiumnetworks.com/products/wifi/</a>
Enterprise Wi-Fi 6 AP Hardware and Installation Guide	<a href="https://support.cambiumnetworks.com/files">https://support.cambiumnetworks.com/files</a>
Enterprise Wi-Fi AP User Guide (This document)	<a href="https://support.cambiumnetworks.com/files">https://support.cambiumnetworks.com/files</a>
Enterprise Wi-Fi AP Release Notes	<a href="https://support.cambiumnetworks.com/files">https://support.cambiumnetworks.com/files</a>
Software Resources	<a href="https://support.cambiumnetworks.com/files">https://support.cambiumnetworks.com/files</a>
Community	<a href="http://community.cambiumnetworks.com/">http://community.cambiumnetworks.com/</a>

Document Name	Location
Support	<a href="https://www.cambiumnetworks.com/support/contact-support/">https://www.cambiumnetworks.com/support/contact-support/</a>
Warranty	<a href="https://www.cambiumnetworks.com/support/warranty/">https://www.cambiumnetworks.com/support/warranty/</a>
Feedback	For feedback, e-mail to <a href="mailto:support@cambiumnetworks.com/">support@cambiumnetworks.com/</a>

## Existing hardware platforms

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

Table 2: Existing hardware platforms

Hardware Platform	Description
XE3-4TN	4x4:4, 2x2:2, 2x2:2 802.11b/g/n/ac wave 2/ax Tri-Radio Outdoor Wi-Fi 6e Access point
XV2-21X	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Wi-Fi 6 Access Point
XV2-23T	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor 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
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
XV3-8	8x8:8, 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Radio Indoor Access Point
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
XV2-2	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Access Point
XV2-2T	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Access Point, Omni, PoE out
XV2-2T1	Outdoor Wi-Fi 6 Access point, 2x2 Sector antenna Dual band 802.11ax 2x2, BLE, 2.5GbE
e410	2x2:2, 802.11a/b/g/n/ac wave 2 Indoor Access Point
e510	2x2:2, 802.11a/b/g/n/ac wave 2 Outdoor Access Point
e430	2x2:2, 802.11a/b/g/n/ac wave 2 Indoor Access Point
e600	2x2:2 for 2.4 GHz and 4x4:4 for 5 GHz, 802.11a/b/g/n/ac wave 2 Indoor Access Point
e700	2x2:2 for 2.4 GHz and 4x4:4 for 5 GHz, 802.11a/b/g/n/ac wave 2 Indoor Access Point

## Premium feature list

System 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 will be identified with the label **Premium feature** in the applicable documentation. With the System Release 6.5 and later releases, end users can access these features without a management subscription. However, access to these features is currently on a free trial basis, and only 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
<a href="#">Wireless Intrusion Detection Systems (WIDS)</a>	System Release 6.4.2
<a href="#">RADIUS-based ePSK</a>	System Release 6.4
<a href="#">ePSK scale (more than 300 keys)</a>	System Release 6.3
<a href="#">Stanley AeroScout Location Engine</a>	System Release 6.3
<a href="#">User Groups</a>	System Release 6.2
<a href="#">Advanced Filters (QoS, DSCP, Schedule, and Rate limit)</a>	System Release 6.0
<a href="#">Application Control</a>	System Release 6.0

# Chapter 1: Quick Start – Device Access

---

This chapter describes the following topics:

- [Powering up the device](#)
- [DC power supply](#)
- [Accessing the device](#)
- [LED status](#)

## Powering up the device

This section includes the following topics:

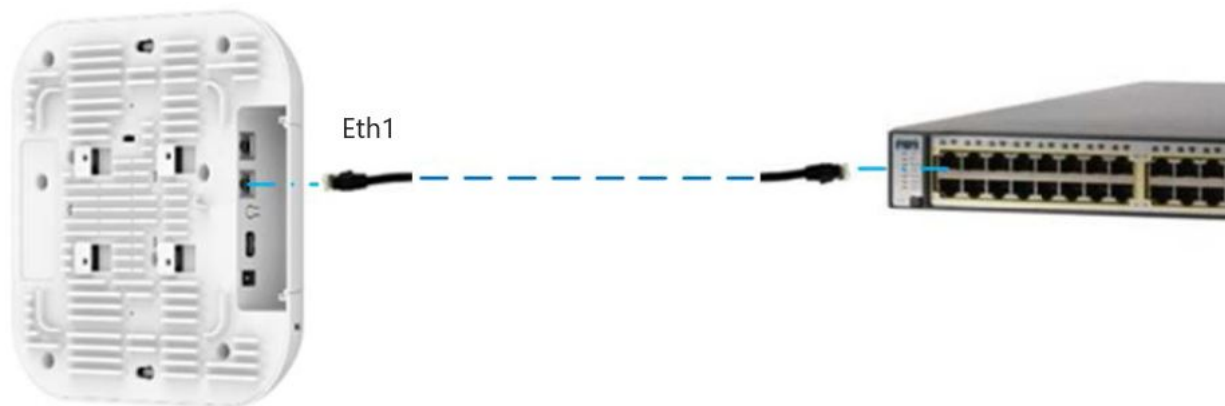
- [PoE switches \(802.3af/802.3at/802.3bt\)](#)
- [PoE adapter](#)
- [DC power supply](#)

Enterprise Wi-Fi AP product family can be powered using 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 related to the 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

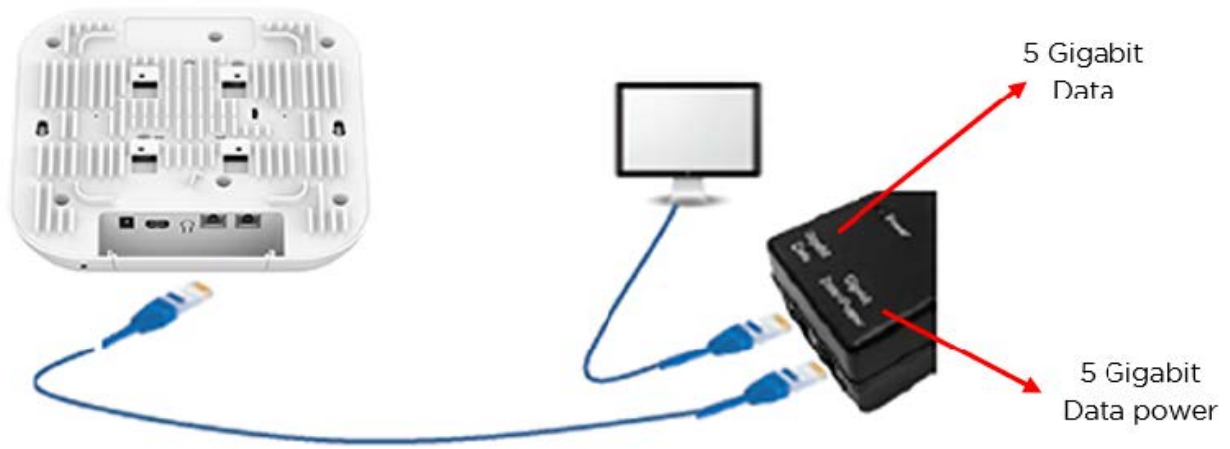
Platform	IEEE 802.3af (12.95W @ PD)	IEEE 802.3at (25.5W @ PD)	IEEE 802.3bt Class - 0/1/2/3/4 (40W @ PD)	IEEE 802.3b Class - 5/6 (51W @ PD)	IEEE 802.3b Class - 7/8 (64W @ PD)
XV3-8	✓	✓	✓		
XV2-2	✓	✓			
XV2-2T	✓	✓	✓	✓	
XV2-2T1	✓	✓	✓	✓	
XE5-8	✓	✓	✓	✓	
XE3-4	✓	✓	✓		
XV2-21X	✓	✓			
XV2-23T	✓	✓			
XV2-22H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

## PoE adapter

Follow the below procedure to power up the device using a PoE adapter:

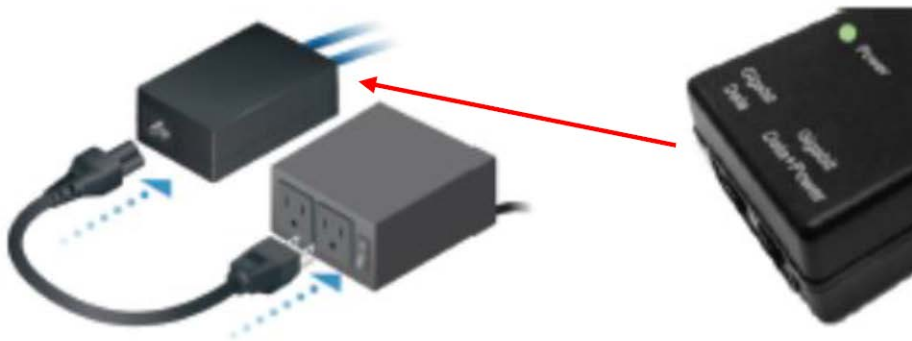
1. Connect the Ethernet cable from Eth1/PoE-IN of the device to the PoE port of 5 Gigabit Data + Power.
2. Connect an Ethernet cable from your LAN or Computer to the 5 Gigabit Data port of the PoE adapter.

Figure 2: Installation of Enterprise Wi-Fi AP to 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: Installation of adapter to 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 both the DC power adapter and PoE are connected, the DC power adapter takes precedence.

## Accessing the device

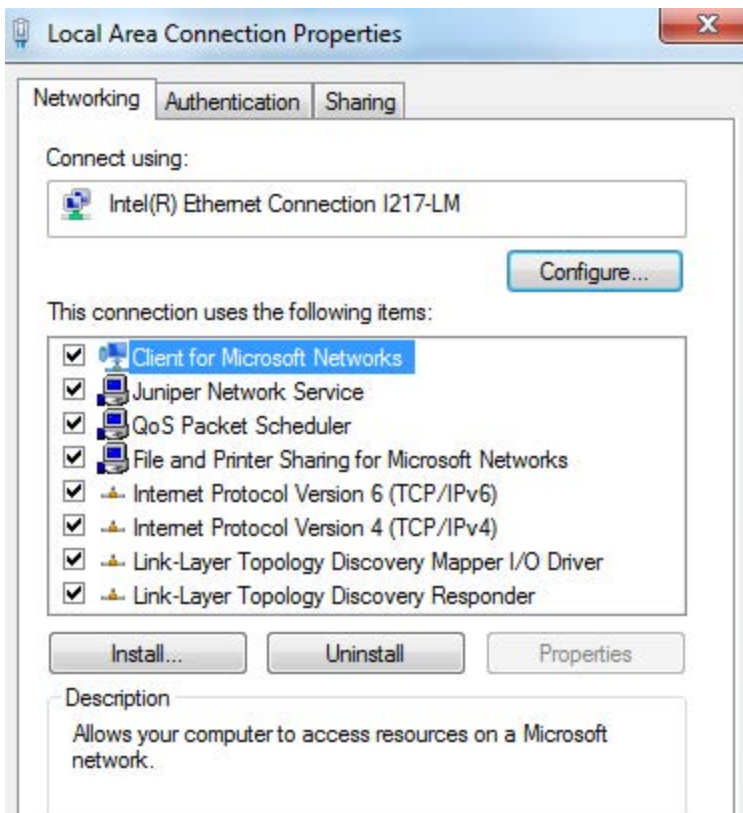
This section includes the following topics:

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

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

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

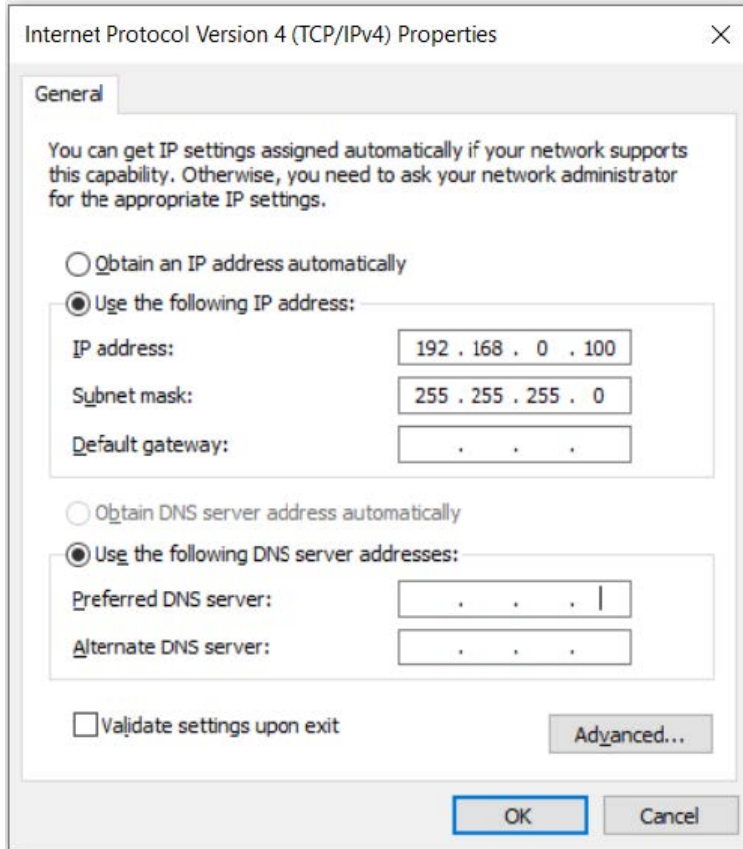


The Enterprise Wi-Fi AP obtains its IP address from a DHCP server. A default IP address of 192.168.0.1/24 will be used if an IP address is not obtained from the DHCP server.

2. Select Internet Protocol Version 4 (TCP/IPv4) from the available list of connections.
3. Click **Properties**.

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



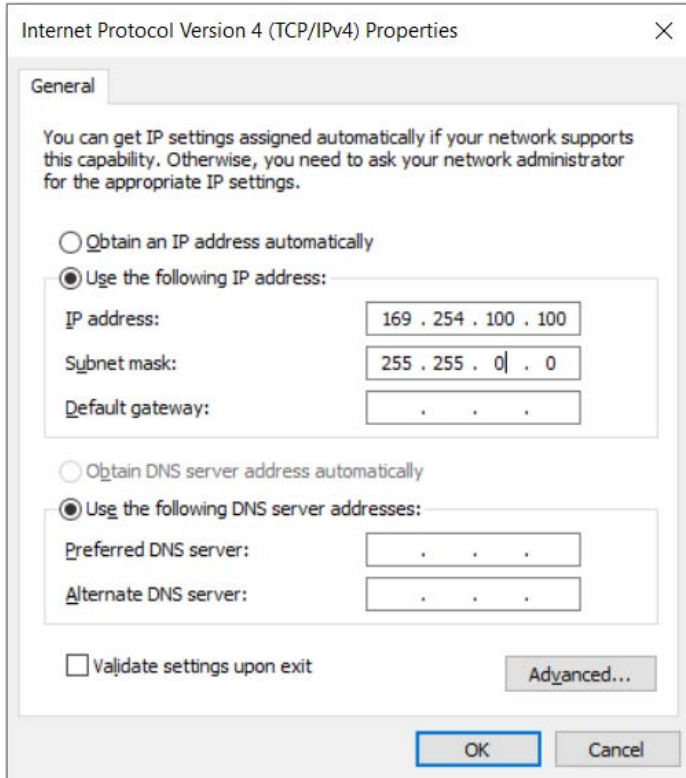


4. In the Use the following IP address section, ensure that an appropriate IP address and a subnet address are provided.
5. Click OK.
6. Ensure that your PC is set up to communicate with the required range of IP addresses.
7. Open a web browser and type the URL - <http://192.168.0.1> - to access the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

## Device access using zeroconf IP

To access the device using zeroconf IP, follow the below 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. Plug in the device to the network.
2. Get 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/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
	<p>The device is booting up.</p> <div style="display: flex; align-items: center;">  <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p><b>Note:</b> If these LEDs remain <b>Amber</b> for more than five minutes, this indicates that the device failed to boot.</p> </div> </div>
	<ul style="list-style-type: none"> <li>• The device is successfully up and accessible.</li> <li>• Wi-Fi services are up, if configured.</li> </ul>
	<p>XMS/cnMaestro connection is successful.</p>

# Chapter 2: Onboarding the Device

---

This chapter describes the following topics:

- [Overview](#)
- [Device Onboarding and Provisioning](#)
  - [cnMaestro](#)
  - [XMS-Cloud](#)
  - [Swift](#)

## 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 devices to correct the cnMaestro server using DHCP options or static URL configuration. For more information go to

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

## Device Onboarding and provisioning

Enterprise Wi-Fi APs support the following Onboarding methods:

### cnMaestro

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

For Onboarding devices to cnMaestro, refer to [cnMaestro Onboarding Devices](#).

### XMS-Cloud

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

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

### Swift

The Swift application gives you cloud-based management of your Enterprise networks right from your phone. It is targeted towards smaller enterprises and does not require extensive networking expertise to deploy and use. You can configure your networks in a few taps and get the most relevant statistics at your fingertips.

The Cambium Networks Swift application is available for Android at (<https://play.google.com/store/apps/details?id=com.cambiumnetworks.swift>) and for iOS at (<https://apps.apple.com/in/app/cambium-networks-swift/id1503771752>).

Following are the QR codes that you can use for downloading the Swift application:



# 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 such as computer, mobile, and tabs. This chapter explains how to access the UI of the Enterprise Wi-Fi AP device.

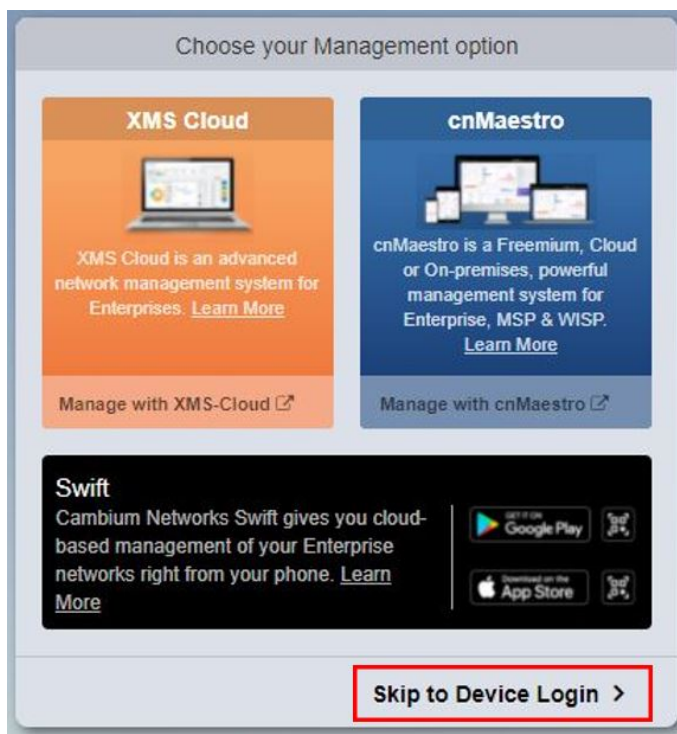
This chapter describes the following topics:

- [Logging into the UI](#)
- [Viewing the Home page \(dashboard\)](#)

## Logging into the UI

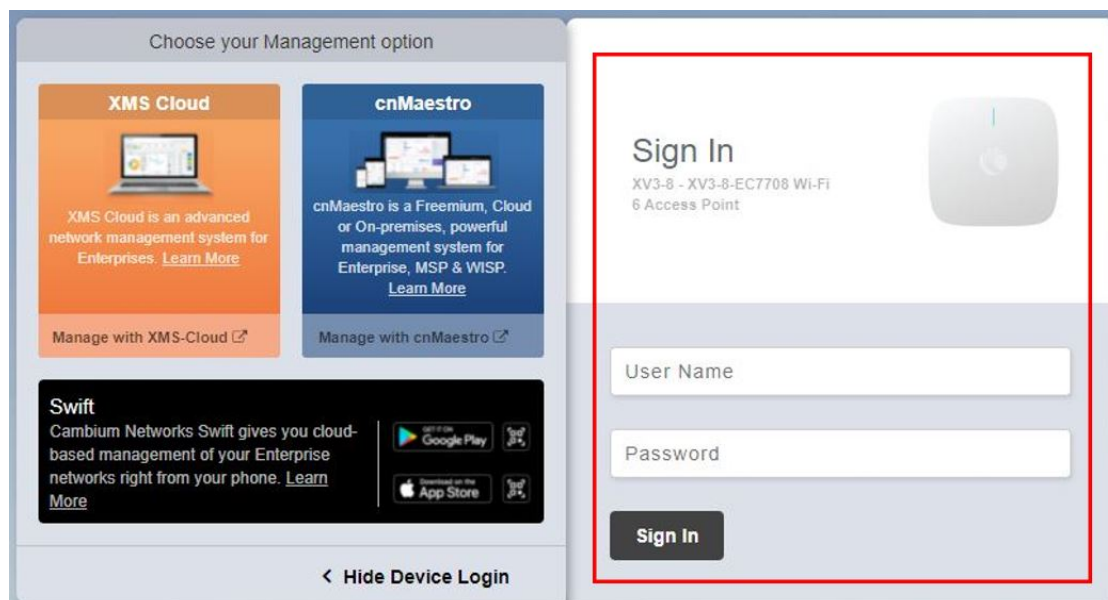
User can select the Management options as **XMS-Cloud** or **cnMaestro** to manage the device, as shown in Figure 4.

Figure 4: *The Management option page*



If the user needs 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 UI login page



To login to the device UI, 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 UI home page (dashboard)

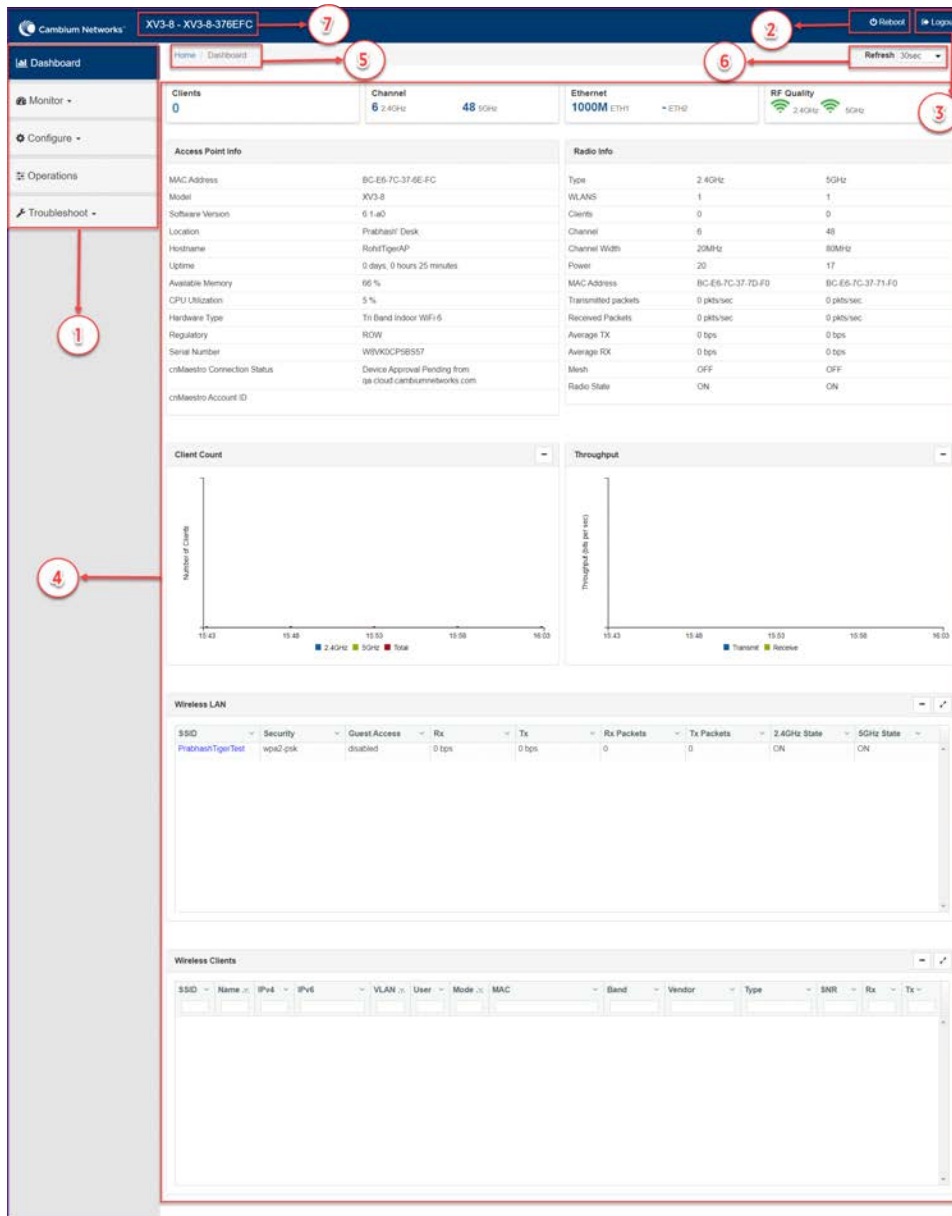




Table 6: Elements in the Enterprise Wi-Fi AP dashboard page

Number	Element	Sub-Element	Description
1	Menu	-	This section contains multiple tabs that help the user to configure, monitor, and troubleshoot the Enterprise Wi-Fi AP device. The menu consists of the following setting options: <ul style="list-style-type: none"> <li>• Monitor</li> <li>• Configure</li> </ul>



Number	Element	Sub-Element	Description
			<ul style="list-style-type: none"> <li>• Operations</li> <li>• Troubleshoot</li> </ul>
2	Reboot	-	Global button to reboot the Enterprise Wi-Fi AP device (  ).
3	Logout	-	Global button to logout user from the Enterprise Wi-Fi AP device (  ).
4	Content	-	Information in the area of the web interface varies based on the tab selected in the Menu section. Usually, this area contains details of configuration or statistics or provision to configure Enterprise Wi-Fi AP device.
		RF Quality	<p>Displays the device radio RF Quality Index that provides the indication of wireless clients' RF link quality (measured in SNR) as seen by the AP.</p> <p>Following are the interpretation of the bars in the image:</p> <ul style="list-style-type: none"> <li>• 4 bar: Indicates the RF link is between 80-100 SNR and the quality is excellent</li> <li>• 3 bar: Indicates the RF link is between 50-79 SNR and the quality is good</li> <li>• 2 bar: Indicates the RF link is between 25-49 SNR and the quality is average</li> <li>• 1 bar: Indicates the RF link is between 0-24 SNR and the quality is poor</li> </ul>
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	-	Provides information related to the Enterprise Wi-Fi AP model number and configured hostname.

## Monitor

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

- **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 Enterprise Wi-Fi AP devices based on deployment requirements. The Configure tab contains multiple sections, as follows:

- **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 maintenance tasks of devices such as the following:

- **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

The section provides users to debug and troubleshoot remotely. The Troubleshoot tab contains multiple sections, as listed below:

- **Wi-Fi Analyzer:** When this is initialized, the device 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
- Management
- Time settings
- Event Logging
- SNMP

## Basic

Table 7 lists configurable system parameters that are available under **Configuration > Basic** tab in the cnMaestro UI:

Table 7: Basic parameters

Parameter	Description	Range	Default
Name	The hostname of the device. The configurable maximum length of the hostname is 64 characters.	-	Enterprise Wi-Fi AP Model Number-Last 3 Bytes of ESN
Location	The location where the device is placed. The maximum length of location is 64 characters.	-	-
Contact	Contact information for the device.	-	-
Country-Code	To be set by the administrator to the country of operation of the device. The allowed operating channels and the transmit power levels on those channels depend on the country of operation. Radios remain disabled unless this is set. The list of countries supported depends on the SKU of the device (FCC and ROW).	-	-
Placement	Enterprise Wi-Fi AP device supports both Indoor and Outdoor deployments. Based on deployment user can configure it as follows: <ul style="list-style-type: none"><li>• <b>Indoor:</b> When selected, only Indoor channels for country code configured will be available and operational.</li><li>• <b>Outdoor:</b> When selected, only outdoor channels for country code configured will be available and operational.</li></ul>	-	Indoor
PoE Output	Enable power over Ethernet to an auxiliary device connected to	-	Off

Parameter	Description	Range	Default
	PoE OUT port.		
Dual 5 GHz radio	Provision to enable Dual 5 GHz radio. This provides the flexibility of splitting 8x8 5 GHz radio into two 4x4 5 GHz radios.	-	Disabled
LED	Select the LED checkbox for the device LEDs to be ON during operation.	-	Enabled
LLDP	Provision to advertise device capabilities and information in the L2 network.	-	Enabled
Channels Distribution	Allows unique distribution of channels across radios when multiple radios are configured with same frequency band. <b>Note:</b> This option is available only as a CLI-based configuration. Use the <code>channels-distribution</code> 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

**Basic Information**

Type  
Enterprise Wi-Fi (E-Series, XE/XV-Series) ▼

Name\*  
XV3-8-EC7708

Auto Sync Automatically push configuration changes to devices sharing this AP Group

Country\*  
India ▼ For appropriate regulatory configuration

Location  
 Location where this device is placed (max 64 characters)

Contact  
 Contact information for the device (max 64 characters)

Description

Placement  
 Indoor  Outdoor Configure the AP placement details

PoE Output  
Off ▼ Enable Power over Ethernet to an auxiliary device connected to PoE OUT port

LED Whether the device LEDs should be ON during operation

LLDP Whether the AP should transmit LLDP packets

**System**

<b>Name</b>	<input type="text" value="XV3-8-EC7708"/>	<i>Hostname of the device (max 64 characters)</i>
<b>Location</b>	<input type="text"/>	<i>Location where this device is placed (max 64 characters)</i>
<b>Contact</b>	<input type="text"/>	<i>Contact information for the device (max 64 characters)</i>
<b>Country-Code</b>	<input type="text" value="India"/>	<i>For appropriate regulatory configuration</i>
<b>Placement</b>	<input checked="" type="radio"/> Indoor <input type="radio"/> Outdoor <i>Configure the AP placement details</i>	
<b>Dual 5GHz radio</b>	<input type="checkbox"/> <i>Splits 8x8 5 GHz radio to two 4x4 5 GHz radios</i>	
<b>LED</b>	<input checked="" type="checkbox"/> <i>Whether the device LEDs should be ON during operation</i>	
<b>LLDP</b>	<input checked="" type="checkbox"/> <i>Whether the AP should transmit LLDP packets</i>	
<b>Default Power Policy</b>	<input type="text" value="Sufficient"/>	<i>Configure default power policy</i>
<b>Power Force Type</b>	<input type="text" value="None"/>	<i>Configure power force type</i>

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

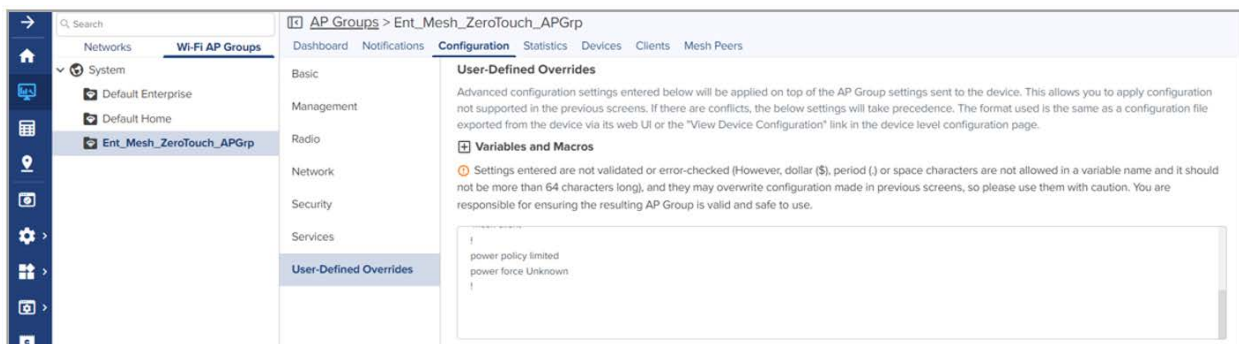
Enterprise Wi-Fi APs first attempt to detect the type and classification of the Power Source (PS) they are being powered by using standard hardware handshake and control logic. Some PS devices are the passive type, like the Cambium PoE power injectors, and therefore the AP cannot detect the type or classification 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:

Table 8: PoE power requirements for the APs

APs	Maximum power draw (Watts)	Power required to boot-up (Watts)	Notes
XV2-21X	12.95	8	No USB or PoE out capability
XV2-22H	22.95	8	12.95W with PoE Out disabled (default) but 22.95W with PoE outsourcing up to 10W
XV2-23T	12.95	8	No USB or PoE out capability
XV2-2	21	8	Has USB
XV3-8	35	12	Has USB and BLE
XE3-4	38.2	15.6	Has USB and BLE
XE5-8	53	12.9	Has USB and BLE
XV2-2TO	53.4	12	PoE out capability of up to 30 W, Has BLE
XV2-2T1	53.4	12	PoE out capability of up to 30 W, Has BLE
XE3-4TN	64	15	PoE out capability of up to 30 W, Has BLE
E410b	11.5	7.3	
E510	12.95	less than 12.95W	
E600	22	less than 12.95W	Has USB
E700	40	less than 12.95W	Has PoE out capability of up to 15 W
E430H	25.5	8	802.3af PoE out on this platform

Figure 8: Power policy configuration



**Attention**

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

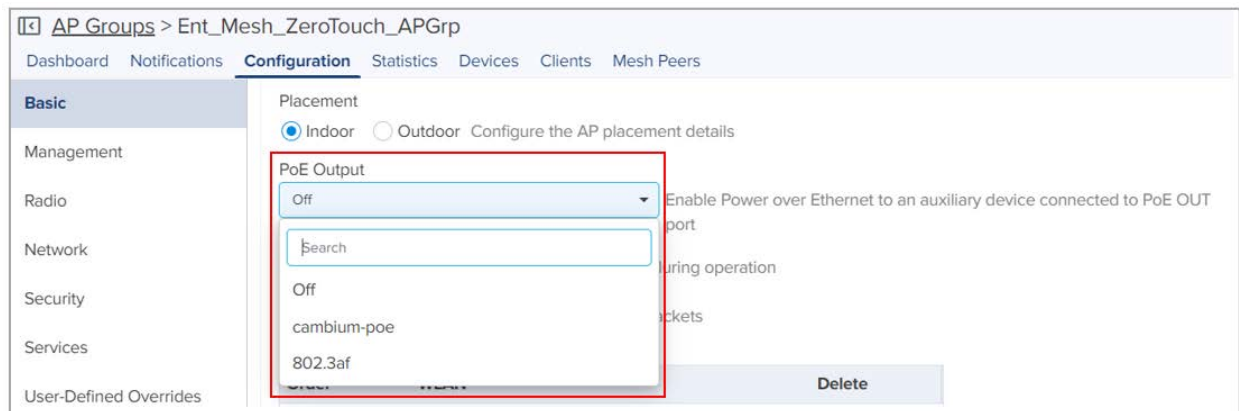
## Power over Ethernet (PoE) Out port

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 9: PoE-out capabilities

SL. No	AP Model	10W	48V @ 15W	48V @ 30W	30V @ 30W	Default State
1	e700					Disabled
2	e430					Disabled
3	XV2-2T		✓	✓	✓	Disabled
4	XV2-2T1		✓	✓	✓	Disabled
5	XV2-22H	✓				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 10 lists configurable fields that are displayed in the **Configuration > System > Management > Administrator Access** tab:

Table 10: Administrator Access parameters

Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	-	admin
Telnet	Enables Telnet access to the device CLI.	-	Disabled
SSH	Enables SSH access to the device CLI.	-	Enabled
SSH Key	Provision to login to device using SSH Keys. 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

Parameter	Description	Range	Default
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.	-	-
<b>cnMaestro</b>			
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 Accesspage

**Administrator Access**

Admin Password  
..... Show Configure password for authentication of GUI and CLI sessions (max 32 characters)

⚠ Change your password, do not use default passwords!

Telnet Enable Telnet access to the device CLI

SSH Enable SSH access to the device CLI

SSH Key  
..... Show Use SSH keys instead of password for authentication

HTTP Enable HTTP access to the device GUI

HTTP Port  
80 Port for HTTP access to the device GUI (1-65535)

HTTPS Enable HTTPS access to the device GUI

HTTPS Port  
443 Port for HTTPS access to the device GUI (1-65535)

RADIUS Mgmt Authentication Enable RADIUS authentication of GUI/CLI sessions

RADIUS Server  
..... RADIUS server IP/Hostname

RADIUS Secret  
..... Show RADIUS server shared secret

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 11](#) lists the fields that are displayed in the **Configuration > Management > Time Settings** section.

Table 11: 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
	 <div style="border: 1px solid #ccc; background-color: #e6f2ff; padding: 5px;"> <p><b>Note</b> Accurate time on the AP is critical for features such as WLAN Scheduled Access, and Syslogs.</p> </div>		
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

**Time Settings**

Time Zone  
 Configure Time Zone

NTP Server 1  
 Name or IP Address of Network Time Protocol Server

NTP Server 2

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

Table 12: 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

**Event Logging**

Syslog Server1 Port

Name or IPv4/IPv6 address of syslog server

Syslog Server2 Port

Syslog Severity

Specify severity of events forwarded to Syslog servers

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

Table 13: 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 RO or RW.	-	RO
Encryption	Choose ON or OFF.	-	ON

Figure 13: SNMP parameters

The screenshot shows the SNMP configuration page. At the top, there is a section titled "SNMP" with a collapse icon. Below it, there is a checked checkbox labeled "Enable" with the text "Enable SNMP support on the device".

Next are two text input fields: "SNMPv2c RO Community" with the value "public" and a description "SNMPv2c read-only community string (max 64 characters)", and "SNMPv2c RW Community" with the value "private" and a description "SNMPv2c read-write community string (max 64 characters)".

Then, "Trap Receiver IP" with the value "xxx.xxx.xxx.xxx" and a description "SNMP trap server IP address".

Followed by "SNMPv3 Username" (empty) and "SNMPv3 Password" (empty) with a "Show" button. Descriptions are "SNMPv3 user name (max 32 characters)" and "SNMPv3 password (8 to 32 characters)".

Below these are three sections of radio buttons: "Authentication" with "MD5" selected and "SHA" unselected; "Access" with "Read-Only" selected and "Read-Write" unselected; and "Encryption" with "On" selected and "Off" unselected.

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 RO or RW 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](#)
- [Configuring Radio parameters](#)
- [BSS coloring](#)
- [Target Wake Time \(TWT\)](#)
- [Receive sensitivity configuration](#)
- [Multicast-snooping and Multicast-to-Unicast conversion](#)

## 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](#)
- [Enhanced Roaming](#)

## Basic

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

Table 14: Configure Radio parameters

Parameter	Description	Range	Default
<b>Radio</b>			
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 <b>Configuration &gt; System</b> UI.	<b>2.4 GHz:</b> 1 - 14 <b>5 GHz:</b> 36 - 173 <b>6 GHz:</b> 1 -233	Auto
Channel Width	The user can select the following channel widths for the operation: <ul style="list-style-type: none"><li>• For 2.4 GHz: Only 20 MHz channel width is supported.</li></ul>	-	20 MHz



Parameter	Description	Range	Default
	<ul style="list-style-type: none"> <li>For 5 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel width are supported. <b>Note:</b> Please refer <a href="#">Chapter 5</a> for 160 MHz support with 5 GHz.</li> <li>For 6 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel width are supported.</li> </ul>		
Transmit Power	<p>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 <a href="https://www.cambiumnetworks.com/products/wifi/">https://www.cambiumnetworks.com/products/wifi/</a>. Transmit power drop-down box varies as per the country selected in Configuration &gt; 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 <b>Configuration &gt; System UI</b>.</p>	<p><b>2.4 GHz:</b> 4 - 30 <b>5 GHz:</b> 4 - 30 <b>6 GHz:</b> 4 - 30</p>	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	<p>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:</p> <ul style="list-style-type: none"> <li><b>For 2.4 GHz:</b> <ul style="list-style-type: none"> <li>All</li> <li>Specific</li> </ul> </li> <li><b>For 5 GHz:</b> <ul style="list-style-type: none"> <li>All</li> <li>Specific</li> <li>Prefer Non-DFS</li> <li>Prefer DFS</li> </ul> </li> </ul>	<p>2.4 GHz: 1 - 14 5 GHz: 36 - 173 6 GHz: 1 -233</p>	All

Parameter	Description	Range	Default
	<ul style="list-style-type: none"> <li>• <b>For 6 GHz:</b> <ul style="list-style-type: none"> <li>◦ All</li> <li>◦ Specific</li> </ul> </li> </ul>		
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.	a) <b>2.4 GHz:</b> b/g/n/ax.  b) <b>5 GHz:</b> a/n/ac/ ax.	All mode
Short Guard Interval	Standard 802.11 parameter to increase the throughput of Enterprise Wi-Fi AP device.	-	Enabled
<b>Off Channel Scan (OCS)</b>			
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
<b>Auto-RF (Dynamic-power)</b>			
Dynamic Power	Provision to enable dynamic power management.	-	-
Mode	Select the required dynamic power modes. Two modes are supported: <ol style="list-style-type: none"> <li>1. By-channel</li> <li>2. By-band</li> </ol>	-	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%
<b>Auto-RF (Dynamic Channel)</b>			
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-	Provision to configure the channel load parameter	-	-

Parameter	Description	Range	Default
weightage	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	<ul style="list-style-type: none"> <li>• access : Only access WLANs are allowed</li> <li>• mesh : Only mesh WLANs are allowed</li> <li>• default : Both mesh and access types of WLANs are allowed</li> </ul>	-	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** Enhanced Roaming

### Radio

**Enable**  Enable operation of this radio

**Band** 2.4GHz Configure the supported bands

**Channel** Automatic Primary operating channel

**Channel Width** 20MHz 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 mSec (100 to 3500 in increments of 100)

**Minimum Unicast rate** default Configure the minimum unicast management rate (Mbps)

**Multicast data rate** default Data-rate to use for transmission of multicast/broadcast packets

**Airtime Fairness**  Enable Airtime Fairness

**Candidate Channels** All

**Mode** default Allow 802.11 b/g/n clients to connect

**Short Guard Interval**  Enable short guard interval

### Off Channel Scan

**Enable**  Enable OCS

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

### Auto RF

**Dynamic Power**  Enable dynamic power management

**Mode**  By-channel  By-band Set dynamic power mode by-channel/by-band

**Minimum Transmit Power** 8 Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes (5-15) dBm

**Minimum Neighbour Threshold** 2 The Minimum number of neighbors to consider for power reduction by autoceil logic. (1-10)

**Cellsize Overlap Threshold** 50% Cell overlap that will be allowed when the AP is determining automatic cell sizes (0-100) %

**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  Continuous 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)

**Auto-RF**

Auto-RF Dynamic Power option adjusts the radio transmit power based on the neighboring Cambium APs transmit power. Auto-RF Dynamic Channel changes the radio channel based on current operating channel RF conditions like channel utilization, interference, packet error rate and etc.

**Mode Selection**

Dynamic Channel

Enable Enable Auto-RF to adjust dynamic channel selection based on RF conditions

Packet Error Rate Enable channel change using unsuccessful packet transmissions by the AP

Channel Utilization Enable channel change using the channel efficiency

Noise Enable channel change with higher noise

**Samples**

3 Configure the minimum number of samples required to run the channel selection (1-20)

**Channel Hold Time**

120

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

**Efficiency Weightage**

60 Configure the efficiency parameter weightage use in ACS algorithm in %(0-100)

**SNR Weightage**

60 Configure the SNR parameter weightage use in ACS algorithm in %(0-100)

**Channel Load Weightage**

40 Configure the channel load parameter weightage use in ACS algorithm in %(0-100)

**Interval**

0 Configure periodic ACS interval in minutes; Set '0' to disable. (0-86400)

**Deprecated (Version 3.11.4 and 4.0)**

**Channel Selection Mode**

Interference Channel selection done based on interference

**Channel Hold Time**

120 Configure channel hold time in minutes (5-1800)

**Channel Utilization Threshold**

25 Configure channel utilization threshold in %(20-40)

## Software Define Radio (SDR) capabilities

Table 15: 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	✓	✓		✓		✓ (SBS)	
XV2-2	✓	✓		✓			
XV2-2T	✓	✓		✓			

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		
XV2-2T1	✓	✓		✓			
XE3-4	✓	✓		✓	✓		
XE3-4TN	✓	✓		✓	✓		
XE5-8	✓	✓	✓	✓	✓	✓	✓ (SBS)
XV2-21X	✓	✓		✓			
XV2-23T	✓	✓		✓			
XV2-22H	✓	✓		✓			

## 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
```

```
dwll-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 16: Configuring Off Channel Scan

Parameter	Description	Range	Default
dwll 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. <ul style="list-style-type: none"> <li>active</li> </ul>	-	active



Parameter	Description	Range	Default
	<p>AP Radio transmits a probe request and listens for a probe response from an AP.</p> <ul style="list-style-type: none"> <li>passive</li> </ul> <p>AP Radio listens on each channel for beacons sent periodically by neighbor APs.</p> <p>Users are advised to use passive as scan type.</p>		

## Enhanced Roaming

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

Table 17: Configure: Radio Enhanced Roaming parameters

Parameter	Description	Range	Default
<b>Enhanced Roaming</b>			
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

The screenshot shows the configuration interface for Enhanced Roaming. It has two tabs: 'Basic' and 'Enhanced Roaming', with 'Enhanced Roaming' being the active tab. Inside the configuration area, there is an 'Enable' checkbox which is checked. To its right is an unchecked checkbox labeled 'Enable active disconnection of clients with weak signal'. Below these, there is a 'Roam SNR threshold' label followed by a text input field containing the value '15'. To the right of the input field is the text 'SNR below which clients will be forced to roam (1-100 dB)'. At the bottom of the configuration area are two buttons: 'Save' and 'Cancel'.

**Enhanced Roaming**

Please enable enhanced roaming only in networks with sufficient signal strength throughout the coverage area, otherwise clients could face connectivity issues

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

Roam SNR Threshold

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

## 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:ff01:0000:0000:0000:0000:0000:0001/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:ff02:0000:0000:0000:0000:0000:0001/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/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 - 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](#)
- [Configuring WLAN parameters](#)
- [Link Aggregation Control Protocol \(LACP\)](#)
- [Radius attributes](#)
- [enhanced PSK \(ePSK\)](#)
- [RADIUS-based ePSK](#)

## 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](#)
- [Radius Server](#)
- [Guest Access](#)
  - [Internal Access Point](#)
  - [External Hotspot](#)
  - [cnMaestro](#)
  - [XMS/EasyPass](#)
- [Usage Limits](#)
- [Scheduled Access](#)
- [Access](#)
- [Passpoint](#)

## Basic

[Table 1](#) lists configurable fields that are displayed in the **Configuration > WLAN > Basic** tab.

Table 18: Basic parameters

Parameters	Description	Range	Default
<b>WLAN &gt; Basic</b>			
Enable	An option to enable a WLAN profile. Once enabled, a Beacon is broadcasted with SSID and respective configured parameters in a WLAN profile.	-	-
Mesh	<p>This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. This parameter supports the following four options:</p> <ol style="list-style-type: none"> <li>1. <b>Base</b> 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.</li> <li>2. <b>Client</b> A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-based AP to connect.</li> <li>3. <b>Recovery</b> 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.</li> <li>4. <b>Off</b> Mesh support disabled on WLAN profile.</li> </ol>	-	OFF (Access Profile Mode)
VLAN	VLAN is configured to segregate 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	<p>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:</p> <ul style="list-style-type: none"> <li>• 2.4 GHz</li> <li>• 5 GHz</li> <li>• 6 GHz</li> </ul>	-	all
SSID	SSID is the unique network name that wireless stations scan and associate.	-	-

Parameters	Description	Range	Default
Security	<p>This parameter determines key values that are encrypted based on the selected algorithm. Following security methods are supported by Enterprise Wi-Fi AP devices:</p> <ol style="list-style-type: none"> <li>1. <b>Open</b> 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.</li> <li>2. <b>OWE</b> This method ensures the communication between each pair of endpoints is protected from other endpoints.</li> <li>3. <b>Osen</b> 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.</li> <li>4. <b>WPA2-Pre-Shared Keys</b> This mode is supported with AES and TKIP encryption. WPA-TKIP can be enabled from the CLI with the “allow-tkip” CLI option.</li> <li>5. <b>WPA2 Enterprise</b> This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication methods.</li> <li>6. <b>WPA2/WPA3 Pre-shared Keys</b> 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.</li> <li>7. <b>WPA3 Pre-shared Keys</b> 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.</li> <li>8. <b>WPA3 Enterprise</b> 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.</li> <li>9. <b>WPA3 Enterprise CNSA</b></li> </ol>	-	Open

Parameters	Description	Range	Default
	<p>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.</p> <p><b>10. User Pre-shared keys</b></p> <p>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.</p>		
Passphrase	The string that is a key value to generate keys based on the security method configured.	-	12345678
VLAN Pooling	<p>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:</p> <p><b>1. Disabled</b></p> <p>This feature is disabled for this WLAN.</p> <p><b>2. Radius Based</b></p> <p>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.</p> <p><b>3. Static</b></p>	-	Disabled

Parameters	Description	Range	Default
	<p>For this mode to support, the user requires to configure VLAN Pool details available under <b>Configure &gt; Network &gt; VLAN pool</b>. 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.</p>		
Max Clients	<p>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 <a href="#">Table 19</a> for more details.</p>	1-512 (Refer <a href="#">Table 19</a> )	256
Client Isolation	<p>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:</p> <ol style="list-style-type: none"> <li>1. <b>Disable</b> <p>This option when selected disables the client isolation feature. i.e. any wireless station can communicate to other wireless stations.</p> </li> <li>2. <b>Local</b> <p>This options when selected enable the client isolation feature. This option prevents wireless station communications connected to the same AP.</p> </li> <li>3. <b>Network Wide</b> <p>This options when selected enable the client isolation feature. It prevents wireless stations communications connected to different AP deployed in the same L2 network.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• Network-wide mode is not supported when Redundancy Gateway protocol is used on deployment.</li> <li>• In the Redundancy Gateway case, Network-wide static can be used to provide a list of Gateway MAC addresses.</li> </ul> </li> <li>4. <b>Network Wide Static</b></li> </ol>		



Parameters	Description	Range	Default
	<p>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.</p> <p><b>Note:</b> 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.</p>		
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.	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.	60-28800	1800

Figure 16: Basic parameter

The screenshot shows the 'Basic' configuration tab for a WLAN. The parameters are as follows:

Parameter	Value	Description
Enable	<input checked="" type="checkbox"/>	
Mesh	Off	Mesh Base/Client/Recovery mode
VLAN	1	Default VLAN assigned to clients on this WLAN. (1-4094)
Radios	all	Define radio types (2.4GHz, 5GHz, 6GHz) on which this WLAN should be supported
SSID	1212	The SSID of this WLAN (upto 32 characters)
Security	WPA2 Pre-shared Keys	Set Authentication and encryption type
Passphrase	*****	WPA2 Pre-shared Security passphrase or key
VLAN Pooling	Disable	Configure VLAN pooling
Max Clients	256	Default maximum Client assigned to this WLAN. (1-512)
Client Isolation	Disable	When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN
cnMaestro Managed Roaming	<input type="checkbox"/>	Enable centralized management of roaming for wireless clients through cnMaestro
Hide SSID	<input type="checkbox"/>	Do not broadcast SSID in beacons
Session Timeout	28800	Session time in seconds (60 to 604800)
Inactivity Timeout	1800	Inactivity time in seconds (60 to 28800)
Drop Multicast Traffic	<input type="checkbox"/>	Drop the send/receive of multicast traffic

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 19: 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
XV2-2T	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
e410/e430 and e510	256	256	NA	256
e600 and e700	512	512	NA	512

\* 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 System 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 20: Advanced parameters

Parameters	Description	Range	Default																														
<b>WLAN &gt; Advanced</b>																																	
UAPSD	<p>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.</p> <table border="1"> <thead> <tr> <th>Priority</th> <th>802.1D Priority (= UP)</th> <th>802.1D Designation</th> <th>Access Category</th> <th>WMM Designation</th> </tr> </thead> <tbody> <tr> <td rowspan="7">                     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> </tbody> </table>	Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation	lowest  highest	1	BK	AC_BK	Background	2	-	0	BE	AC_BE	Best Effort	3	EE	4	CL	AC_VI	Video	5	VI	6	VO	AC_VO	Voice	7	NC	-	Disabled
Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation																													
lowest  highest	1	BK	AC_BK	Background																													
	2	-																															
	0	BE	AC_BE	Best Effort																													
	3	EE																															
	4	CL	AC_VI	Video																													
	5	VI																															
	6	VO	AC_VO	Voice																													
7	NC																																
QBSS	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.	-	Disabled																														
DTIM interval	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.	1-255	1																														
<b>Monitored Host</b>																																	
Host	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.	-	Disabled																														
Interval	The frequency of monitoring the network health based on the status of the keep-alive mechanism w.r.t configured monitored host.	60-3600 sec	300																														
Attempts	The number of packets in the keep-alive mechanism to determine the status.	1-20	1																														
DNS Logging Host	By enabling this feature, the Administrator can monitor the websites accessed by wireless stations connected to WLAN profile.	-	Disabled																														

Parameters	Description	Range	Default
Connection Logging Host	When enabled provides information of all TCP connections accessed by a wireless station that is associated with WLAN.	–	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. <ul style="list-style-type: none"> <li>• Low</li> <li>• Normal</li> <li>• Aggressive</li> </ul>	–	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: <ul style="list-style-type: none"> <li>• Hostname</li> <li>• AP MAC</li> <li>• BSSID</li> <li>• SSID</li> <li>• VLAN ID</li> <li>• SITEID</li> <li>• Custom</li> <li>• All</li> </ul>	–	Disabled
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 msec 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 msec.	–	Disabled

Parameters	Description	Range	Default
	<p>Select any one of the following:</p> <ol style="list-style-type: none"> <li><b>OKC</b> 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.</li> <li><b>802.11r</b> 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.</li> </ol>		
RRM (802.11k)	<p>AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 11k clients.</p> <p>The following parameter needs to be enabled:</p> <ul style="list-style-type: none"> <li>Enable RRM</li> </ul>	–	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
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

The screenshot shows the 'Advanced' configuration page for a wireless LAN. The settings are as follows:

- UAPSD**:  Enable UAPSD
- QBSS**:  Enable QBSS load element
- DTIM interval**:  Number of beacons (1-255)
- Monitored Host** (grouped in a box):
  - Host**:  IP Address or Hostname that should be reachable for this WLAN to be active
  - Interval**:  Duration in seconds (60-3600)
  - Attempts**:  Number of attempts to check the reachability of monitored host (1-20)
- DNS Logging Host**:  **Port**:  Syslog server where all client DNS requests will be logged
- Connection Logging Host**:  **Port**:  Syslog server where all client connection requests will be logged
- Band Steering**:  Steer dual-band capable clients towards 5GHz radio
- Proxy ARP**:  Respond to ARP requests automatically on behalf of clients
- Proxy ND**:  Respond to IPv6 ND requests automatically on behalf of clients
- Unicast DHCP**:  Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients
- Insert DHCP Option 82**:  Enable DHCP Option 82
- Option 82 Circuit ID**:
- Option 82 Remote ID**:
- Tunnel Mode**:  Enable tunnelling of WLAN traffic over configured tunnel
- Fast-Roaming Protocol**:  OKC  802.11r Configure roaming protocol
- RRM (802.11k)**:  Enable Radio Resource Measurements (802.11k)
- 802.11v**:  Enable 802.11v BSS Transition Management

At the bottom of the page, there are two buttons: **Save** and **Cancel**.

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 > Radius Server** page:

Table 21: 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	<p>This field is enabled based on customer requirements. The accounting packet is transmitted based on the mode selected.</p> <ol style="list-style-type: none"> <li>1. Start-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station is connected and then disconnects.</li> <li>2. 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.</li> <li>3. None The accounting mode will be disabled.</li> </ol>	-	Disabled
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Server Pool Mode	<p>Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode.</p> <ol style="list-style-type: none"> <li>1. Failover AP selects the RADIUS server which is up and running based on the order of configuration.</li> </ol>	-	Failover
NAS Identifier	This is a configurable parameter and is appended in the RADIUS request packet.	-	Hostname/ System Name

Parameters	Description	Range	Default
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
Proxy through cnMaestro aka Proxy Through Controller	This option is enabled, whenever cnMaestro is required to act as proxy server to RADIUS authentication requests coming from cnPilot devices that are connected to cnMaestro.	-	Disabled
Called Station ID	The following information can be communicated to the RADIUS server: <ul style="list-style-type: none"> <li>• AP-MAC</li> <li>• AP-MAC: SITE-NAME</li> <li>• AP-MAC: SSID</li> <li>• AP-MAC: SSID-SITE-NAME</li> <li>• AP-NAME</li> <li>• AP-NAME: SITE-NAME</li> <li>• AP-NAME: SSID</li> <li>• SITE-NAME</li> <li>• SSID</li> <li>• CUSTOM</li> </ul>	-	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

The screenshot shows the 'Radius Server' configuration page. It includes the following fields and options:

- Authentication Servers:** Three rows for configuring Host, Secret, Port, and Realm.
- Accounting Servers:** Three rows for configuring Host, Secret, and Port.
- Timeout:** Input field with value '3' and description 'Timeout in seconds of each request attempt (1-30)'. Includes an 'Attempts' field with value '1' and description 'Number of attempts before giving up (1-3)'.
- Accounting Mode:** A dropdown menu set to 'None' with the description 'Configure accounting mode'.
- Accounting Packet:** A checkbox for 'Enable Accounting-On messages'.
- Sync Accounting Records:** A checkbox for 'Configure accounting records to be synced across neighboring AP's'.
- Server Pool Mode:** Radio buttons for 'Load Balance' (selected), 'Failover', and 'None'.
- NAS Identifier:** Input field with value 'AP-HOSTNAME' and description 'NAS-Identifier attribute for use in Request packets. Defaults to system name'.
- Interim Update Interval:** Input field with value '1800' and description 'Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)'.
- Dynamic Authorization:** A checkbox for 'Enable RADIUS dynamic authorization (COA, DM messages)'.
- Dynamic VLAN:** A checked checkbox for 'Enable RADIUS assigned VLANs'.
- Proxy through cnMaestro:** A checkbox for 'Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP'.
- Called Station ID:** A dropdown menu set to 'AP-MAC.SSID' with the description 'Configure AP-MAC.SSID as Called-Station-Id in the RADIUS packet'.

## 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:

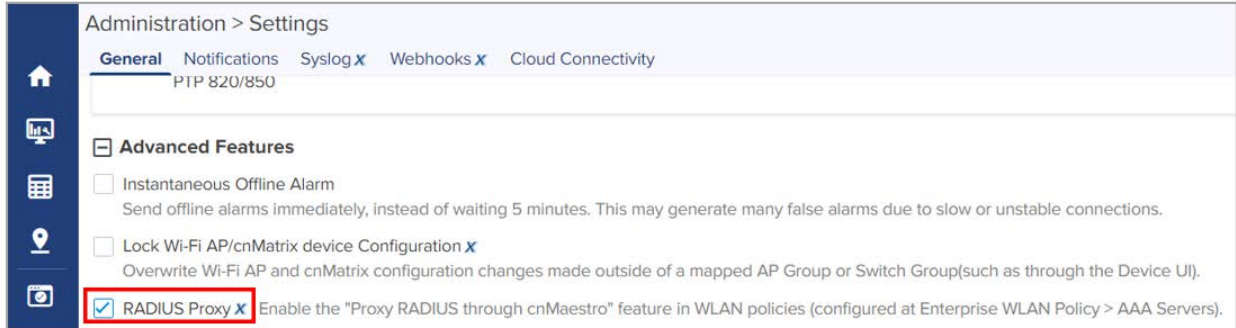
```
XV3-8-EC7708(config-wlan-1)# radius-server through-controller
```

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 22: Internal Access Point parameters

Parameters	Description	Range	Default
<b>WLAN &gt; Guest Access &gt; Internal Access Point</b>			
Enable	Enables the Guest Access feature.	-	Disabled
Access Policy	<p>There are four types of access types provided for the user:</p> <ol style="list-style-type: none"> <li>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</li> <li>2. RADIUS</li> </ol>	-	Clickthrough >

Parameters	Description	Range	Default
	<p>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.</p> <p>3. Local Guest Account</p> <p>Users must configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.</p>		
Redirect Mode	<p>This option helps the user to configure the HTTP or HTTPS mode of redirection URL.</p> <p>1. HTTP</p> <p>AP sends an HTTP POSTURL to the associated client, which will be <a href="http://&lt;Pre-defined-URL&gt;">http://&lt;Pre-defined-URL&gt;</a>.</p> <p>2. HTTPS</p> <p>AP sends HTTPS POSTURL to the success associated client, which will be <a href="https://&lt;Pre-defined-URL&gt;">https://&lt;Pre-defined-URL&gt;</a>.</p>	-	HTTP
Redirect Hostname	<p>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.</p>	-	-
Title	<p>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.</p>	Up to 255 characters	Welcome To Cambium Powered Hotspot
Contents	<p>Users can configure the contents of the Splash page using this field. Displays the text configured under the Title section of the redirection page.</p>	Up to 255 characters	Enter username and password to get Web Access
Terms	<p>Splash page displays the text configured when the user accepts the Terms and Agreement.</p>	Up to 255 characters	-
Logo	<p>Displays the logo image updated in URL <a href="http(s)://&lt;ipaddress&gt;/logo.png">http(s)://&lt;ipaddress&gt;/logo.png</a>. Either PNG or JPEG format of the logo is supported.</p>	-	-

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: <ol style="list-style-type: none"> <li>1. Internal Logout Page After successful login, the wireless client is redirected to the logout page hosted on AP.</li> <li>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.</li> <li>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.</li> </ol>	-	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. <ul style="list-style-type: none"> <li>• Prefix Query Strings in Redirect URL This option is selected by default. The following information is appended in the redirection URL: <ul style="list-style-type: none"> <li>◦ SSID</li> <li>◦ AP MAC</li> <li>◦ NAS ID</li> <li>◦ AP IP</li> <li>◦ Client MAC</li> <li>◦ Redirection URL</li> <li>◦ Users can provide either HTTP or HTTPS URL</li> </ul> </li> </ul>	-	-
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
	<ul style="list-style-type: none"> <li>Prefix Query Strings in Redirect URL</li> </ul> <p>This option is selected by default. The following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> <li>SSID</li> <li>AP MAC</li> <li>NAS ID</li> </ul>		
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	<ul style="list-style-type: none"> <li>If enabled, only HTTP URLs will be redirected to the Guest Access login page.</li> <li>If disabled, both HTTP and HTTPS URLs will be redirected to the Guest Access login page.</li> </ul>	-	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.	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
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, therefore 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

Basic | Radius Server | **Guest Access** | Usage Limits | Scheduled Access | Access | Passpoint

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  cnMaestro

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

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

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

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

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

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

**Logo**   
*Logo to be displayed on the splash page*

**Background Image**   
*Background image to be displayed on the splash page*

**Success Action**  Internal Logout Page  Redirect user to External URL  Redirect user to Original URL

**Success message**

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

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

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

**Session Timeout**  *Session time in seconds (60 to 288000)*

**Inactivity Timeout**  *Inactivity time in seconds (60 to 288000)*

**MAC Authentication Fallback**  *Use guest-access only as fallback for clients failing 802.1X authentication*

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

---

**Add Whitelist** | Captive Portal bypass User Agent

**IP Address or Domain Name**

IP Address   Domain Name	Action
No white list available	

## External Hotspot

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

Table 23: External Hotspot parameters

Parameters	Description	Range	Default
<b>WLAN &gt; Guest Access &gt; External Hotspot</b>			
Access Policy	<p>There are four types of access types provided for the end user:</p> <ol style="list-style-type: none"> <li><b>Clickthrough</b> 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.</li> <li><b>RADIUS</b> 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.</li> <li><b>Local Guest Account</b> 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.</li> </ol>	–	Clickthrough
Redirect Mode	<p>Provision to configure the HTTP or HTTPS mode of redirection URL.</p> <ol style="list-style-type: none"> <li><b>HTTP</b> AP sends an HTTP POSTURL to the associated client, which will be <a href="http://&lt;Pre-defined-URL&gt;">http://&lt;Pre-defined-URL&gt;</a>.</li> <li><b>HTTPS</b> AP sends an HTTPS POSTURL to the associated client, which will be <a href="https://&lt;Pre-defined-URL&gt;">https://&lt;Pre-defined-URL&gt;</a>.</li> </ol>	–	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. <ul style="list-style-type: none"> <li>• <b>Standard</b> This mode is selected, for all third-party vendors whose Guest Access services are certified and integrated with Enterprise Wi-Fi AP products.</li> </ul>	-	Standard
Success Action	Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL: <ol style="list-style-type: none"> <li>1. Internal Logout Page After successful login, the wireless client is redirected to the logout page hosted on AP.</li> <li>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.</li> <li>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.</li> </ol>	-	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. <ul style="list-style-type: none"> <li>• Prefix Query Strings in Redirect URL</li> </ul>	-	-

Parameters	Description	Range	Default
	<p>This option is selected by default. The following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> <li>◦ SSID</li> <li>◦ AP MAC</li> <li>◦ NAS ID</li> <li>◦ AP IP</li> <li>◦ Client MAC</li> </ul> <ul style="list-style-type: none"> <li>• Redirection URL</li> </ul> <p>Users can provide either HTTP or HTTPS URLs.</p>		
Redirection user to Original URL	<p>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:</p> <ul style="list-style-type: none"> <li>• Prefix Query Strings in Redirect URL</li> </ul> <p>This option is selected by default. The following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> <li>◦ SSID</li> <li>◦ AP MAC</li> <li>◦ NAS ID</li> <li>◦ AP IP</li> <li>◦ Client MAC</li> </ul>	–	–
Success message	<p>Provision to configure the text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.</p>	–	–
Redirection URL Query String	<p>The following information is appended in the redirection URL, if <b>Prefix Query Strings in Redirect URL</b> is enabled.</p> <ul style="list-style-type: none"> <li>• Client IP</li> <li>• RSSI</li> <li>• AP Location</li> </ul>	–	Disabled
Redirect	<ul style="list-style-type: none"> <li>• If enabled, only HTTP URLs will be redirected to the Guest Access login page.</li> </ul>	–	Enabled

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> <li>If disabled, both HTTP and HTTPS URLs will be redirected to the Guest Access login page.</li> </ul>		
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.	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
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

Basic Radius Server **Guest Access** Usage Limits Scheduled Access Access Passpoint Delete

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  cnMaestro  XMS/Easypass

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

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

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

**WISPr Clients External Server Login**

**External Page URL**   
*URL of external splash page*

**External Portal Post Through cnMaestro**

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

**Success Action**  Internal Logout Page  Redirect user to External URL  Redirect user to Original URL

**Success message**

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

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

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

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

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

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

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

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

---

**White List** Captive Portal Bypass User Agent

**IP Address or Domain Name**

IP Address   Domain Name	Action
No white list available	

1 / 1 10 items per page

## cnMaestro

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

Table 24: The cnMaestro parameters

Parameters	Description	Range	Default
<b>WLAN &gt; Guest Access &gt; cnMaestro</b>			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	–	–
Redirect	<ul style="list-style-type: none"><li>If enabled, only HTTP URLs will be redirected to the Guest Access login page.</li><li>If disabled, both HTTP and HTTPS URLs will be redirected to Guest Access login page.</li></ul>	–	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.	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

Basic Radius Server **Guest Access** Usage Limits Scheduled Access Access Passpoint Delete

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  cnMaestro  XMS/Easypass

**Guest Portal Name**   
*Guest Portal Name which is hosted on cnMaestro*

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

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

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

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

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

**White List**

**IP Address or Domain Name**

IP Address   Domain Name	Action
No white list available	

Navigation: 1 / 1 items per page

## XMS/EasyPass

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

Table 25: 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 **Secret** 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

Basic Radius Server **Guest Access** Usage Limits Scheduled Access Access Passpoint Delete

Enable

Portal Mode  Internal Access Point  External Hotspot  cnMaestro  XMS/Easypass

External Page URL   
URL of external splash page

Secret   
Configure the secret to be used during redirection

**White List** Captive Portal Bypass User Agent

IP Address or Domain Name

IP Address   Domain Name	Action
No white list available	

1 / 1 10 items per page



**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 26: 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 27: The Scheduled Access parameters

Parameters	Description	Range	Default
Scheduled Access	<p>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.</p> <div style="border: 1px solid black; background-color: #e1f5fe; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>From System 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.</p> </div>	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

The screenshot shows the configuration interface for Scheduled Access. At the top, there are several tabs: Basic, Radius Server, Guest Access, Usage Limits, Scheduled Access (which is highlighted), Access, and Passpoint. Below the tabs, the interface is organized into a grid for each day of the week, from Sunday to Saturday. For each day, there are two input fields: 'Start Time' and 'End Time'. To the right of each 'End Time' field, the text 'HH:MM format' is displayed. At the bottom right of the grid, there are two buttons: 'Save' and 'Cancel'.

## 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 28: The Access parameters

Parameters	Description	Range	Default
<b>DNS-ACL</b>			
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.	-	-
<b>MAC Authentication</b>			
MAC Authentication Policy	Enterprise Wi-Fi AP supports multiple methods of MAC authentication. Following are the details of each mode:  <b>1. Permit</b>  Wireless station MAC addresses listed will be allowed to associate to AP.  <b>2. Deny</b>  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
	<p><b>3. Radius</b></p> <p>For every wireless authentication, AP sends a radius request and if radius acceptance is received, then the wireless station is allowed to associate.</p> <p><b>4. cnMaestro</b></p> <p>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.</p>		

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

The screenshot displays the 'Access' configuration page with the following sections:

- Navigation:** Basic, Radius Server, Guest Access, Usage Limits, Scheduled Access, **Access**, Passpoint, Delete.
- DNS-ACL Section:**
  - Fields: Precedence (1), Action (Deny), Domain (empty).
  - Table: Precedence, Policy, Domain Name, Action. Content: No Rules available.
  - Footer: 1 / 1, 10 items per page.
- MAC Authentication Section:**
  - Fields: MAC Authentication Policy (Deny), MAC (empty), Description (empty).
  - Table: MAC Address, Action, Description. Content: No MAC Address available.
  - Footer: 1 / 1, 10 items per page.

### 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

Precedence	Policy	Domain
1	deny	*facebook.com
2	deny	*youtube.com
256	permit	*.*

## Passpoint

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

Table 29: Passpoint parameters

Parameters	Description	Range	Default
<b>Configuration &gt; Hotspot2.0 / Passpoint</b>			
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: <ul style="list-style-type: none"> <li>Private</li> <li>Chargeable Public</li> <li>Emergency Services</li> <li>Free Public • Personal Device</li> <li>Private with Guest</li> <li>Test • Wildcard</li> </ul>	–	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: <ul style="list-style-type: none"> <li>• 3GPP Cellular Network Information</li> <li>• Connection Capability</li> <li>• Domain Name List</li> <li>• Icons</li> <li>• IP Address Type information</li> <li>• NAI Realm List</li> <li>• Network Authentication Type</li> <li>• Operating Class Indication</li> <li>• Operator Friendly Names</li> <li>• OSU Provider List</li> <li>• Venue Name Information</li> <li>• WAN Metrics</li> </ul>	–	–

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

The screenshot shows the 'Passpoint' configuration page. At the top, there are tabs for 'Basic', 'Radius Server', 'Guest Access', 'Usage Limits', 'Scheduled Access', 'Access', and 'Passpoint'. The 'Passpoint' tab is active. Below the tabs is a 'Configuration' section with a sub-section 'Hotspot2.0 / Passpoint'. This section contains several settings:
 

- Enable:** A checkbox with the text 'Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning'.
- DGAF:** A checkbox with the text 'Downstream Group Addressed Forwarding, When enabled the WLAN doesn't transmit any multicast and broadcast packets'.
- ANQP Domain ID:** A text input field containing '0'. A tooltip reads: 'ANQP domain identifier (0-65535) included when the HS 2.0 Indication element is in Beacon and Probe Response frames'.
- Comeback Delay:** A text input field containing '0'. A tooltip reads: 'Comeback delay in milliseconds. Supported range is 100-2000 ms, use 0 to disable'.
- Access Network Type:** A dropdown menu set to 'Private'. A tooltip reads: 'The configured Access Network Type is advertised to STAs'.
- ASRA:** A checkbox with the text 'Additional Step Required for Access, indicate that the network requires a further step for access'.
- Internet:** A checkbox with the text 'The network provides connectivity to the Internet, Otherwise unspecified'.
- HESSID:** A text input field. A tooltip reads: 'Configure the desired specific HESSID network identifier or the wildcard network identifier'.
- Venue Info:** Two dropdown menus, the first set to 'Please select'. A tooltip reads: 'Configure Venue group and Venue type'.
- Roaming Consortium:** A text input field, an 'Add' button, another dropdown menu, and a 'Delete' button. A tooltip reads: 'The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP'.

 Below this section is an 'ANQP Elements (Access Network Query Protocol)' section with an 'ANQP' dropdown menu set to 'Please Select'. At the bottom of the configuration section are 'Save' and 'Cancel' buttons. Below the configuration section is a 'Summary' section with a table:
 

Hotspot2.0 / Passpoint			
Status	Disable	DGAF	Disable
Access Network Type	Private	ASRA	No
HESSID		Domain ID	0
		Internet	Not Available

## Radius attributes

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

Table 30: 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-	55	Replay protection (RFC 5176)

Type	Attribute Name	Attribute Number	Purpose
	Timestamp		
Standard	Filter-ID	11	<ul style="list-style-type: none"> <li>Assign station to a user group</li> <li>Re-assign station to a different user group (RFC 5176)</li> </ul>
Standard	Framed-IP-Address	8	Session identification (RFC 5176)
Standard	Idle-Timeout	28	Specifies the amount of time a station may remain idle 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	<ul style="list-style-type: none"> <li>Station username update</li> <li>Session identification (RFC 5176)</li> </ul>
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)

## enhanced PSK (ePSK)

By using the ePSK feature, users can configure and support individual PSK keys 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:**  
ePSK scale is a [Premium feature](#) where users can configure more than 300 ePSK (up to 2000 ePSK) per WLAN and it is controlled by cnMaestro X.

Table 31: Maximum ePSK Keys per platform

Platform	Maximum ePSK Keys
XV3-8	2000
XE5-8	2000
XV2-2	2000
XV2-21X	2000
XV2-23T	2000
XV2-22H	2000
XV2-2T	2000
XV2-2T1	2000
XE3-4	2000
XE3-4TN	2000
e410, e430, e510, e600, and e700	1024

## 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.

### Configuration CLI:

```
XV3-8-EC7708(config)# wireless wlan 1
XV3-8-EC7708(config-wlan-1)# epsk
RADIUS : Configure RADIUS based ePSK
username : Configure Username
XV3-8-EC7708(config-wlan-1)# epsk RADIUS
XV3-8-EC7708(config-wlan-1)# save
```

## 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:

AP Groups > Ent\_Mesh\_ZeroTouch\_APGrp

Dashboard Notifications **Configuration** Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

**User-Defined Overrides**

**User-Defined Overrides**

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

**Variables and Macros**

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 1
gtk-per-vlan
!
```

### 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](#)
- [Configuring Network parameters](#)

## Overview

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

## Configuring Network parameters

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

- [VLAN](#)
- [Routes](#)
- [Ethernet Ports](#)
- [Security](#)
- [DHCP](#)
- [Tunnel](#)
- [PPPoE](#)
- [VLAN Pool](#)

## IPv4 network parameters

### VLAN

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

Table 32: VLAN (IPv4) parameters

Parameters	Description	Range	Default
<b>VLAN &gt; IPv4</b>			
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:  1. <b>DHCP</b>  This is the default mode in which the Enterprise Wi-Fi AP device tries to obtain an IPv4 address from the DHCP server.  2. <b>Static IP</b>  Users must explicitly configure the IPv4 address and Netmask for a VLAN selected.	–	DHCP

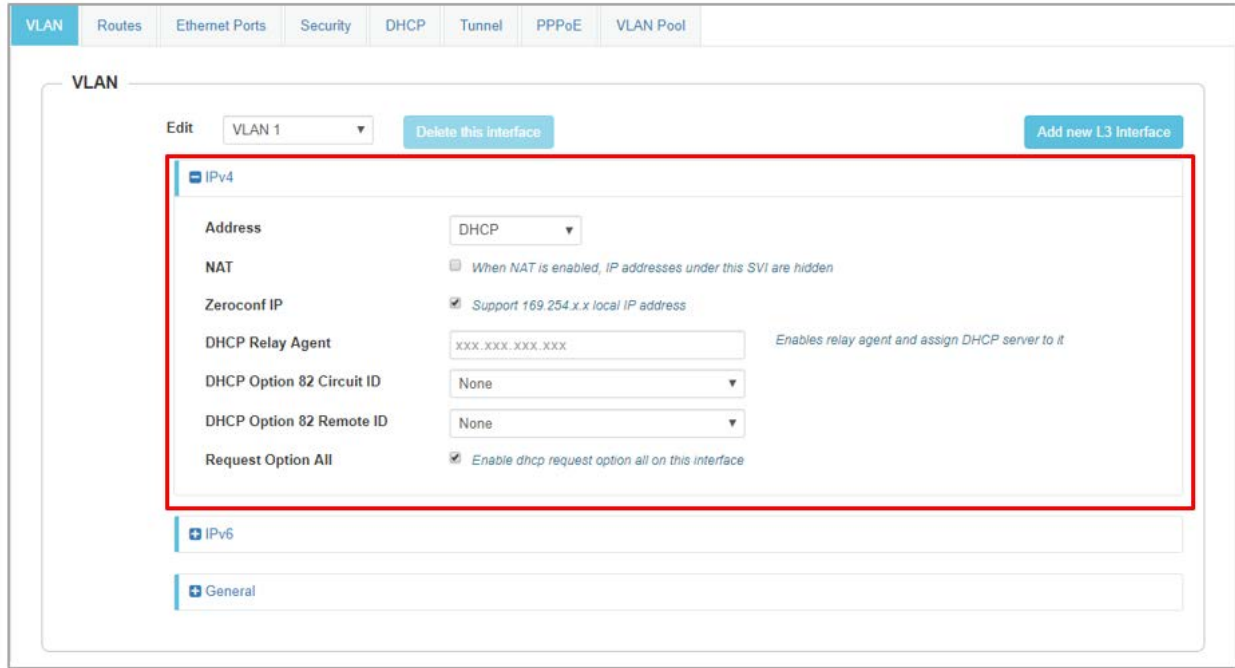
Parameters	Description	Range	Default
NAT	This option enables wireless traffic gets NAT'ed with APs respective uplink interface IP. This option is recommended when DHCP pools are configured in AP.	–	Disabled
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only in the VLAN1 configuration section. If VLAN 1 is not allowed in Ethernet interfaces, this IP will not be accessible.	–	Enabled
Request Option All	This configuration decides the interface on which Enterprise Wi-Fi AP will learn the following: <ul style="list-style-type: none"> <li>• IPv4 default gateway</li> <li>• DHCP client options like Option 43 and Option 15 (Controller discovery like controller host name / IPv4 address)</li> <li>• DNS Servers</li> <li>• Domain Name</li> </ul>	–	Enabled on VLAN1

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

To configure VLAN IPv4:

1. Select **Edit** 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** checkbox.
4. Enable **Zeroconf IP** checkbox.
5. Select **DHCP Option 82 Circuit ID** from the drop-down list.
6. Select **DHCP Option 82 Remote ID** from the drop-down list.
7. Enable **Request Option All** checkbox.
8. 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 33: 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

Options	Description	Usage	Reference CLI
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
Option 54	DHCP clients use the contents of the <b>server identifier</b> 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 System Release 6.4, this option is used to learn HTTPS Proxy server address from the DHCP server as well.

### DHCP Option 43 format

From System 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 34: 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.	–	–
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 textbox.
2. Enter **Domain** Name in the textbox.
3. Enter primary domain server name in the **DNS Server 1** textbox.
4. Enter secondary domain server name in the **DNS Server 2** textbox.
5. Enable **DNS Proxy** checkbox.
6. Click **Save**.

Figure 30: Routing & DNS (IPv4 ) parameters

The screenshot shows a configuration window titled "Routing & DNS". It has two main sections: "IPv4" and "IPv6". The "IPv4" section is highlighted with a red border and contains the following fields:

- Default Gateway:** A text input field with the description "IP address of default gateway".
- DNS Server 1:** A text input field with the description "Primary Domain Name Server".
- DNS Server 2:** A text input field with the description "Secondary Domain Name Server".
- Domain Name:** A text input field with the description "Domain name".
- DNS Proxy:** A checkbox labeled "DNS Proxy".

The "IPv6" section is partially visible below the IPv4 section. At the bottom of the window, there are two buttons: "Save" and "Cancel".

## Routes

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

Table 35: 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: <ul style="list-style-type: none"> <li>• Destination IP</li> <li>• Mask</li> <li>• Gateway</li> </ul>	–	–
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: <ul style="list-style-type: none"> <li>• Port</li> <li>• IP Address</li> <li>• Type</li> </ul>	–	–

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

To configure Gateway Source Precedence:

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

To configure Add Multiple Route Entries:

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

To configure Port Forwarding:

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

Figure 31: Routes (IPv4) parameters

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

**Gateway Source Precedence**

**IPv4**

STATIC  
DHCP  
PPPoE

Save

**IPv6**

STATIC  
AUTO-CONFIG/DHCP

Save

**Add Multiple Route Entries - IPv4**

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

Destination IP	Mask	Gateway	Action
No routes available			

1 / 1    10 items per page

**Add Multiple Route Entries - IPv6**

Destination IP/prefix:    Gateway:    Save

Destination IP	Gateway	Action
No routes available		

1 / 1    10 items per page

**Port Forwarding**

Port:    IP Address:    Type: TCP    Save

Port	IP Address	Protocol	Action
No rules available			

1 / 1    10 items per page



## IPv6 network parameters

### VLAN

Table 36: VLAN (IPv6) parameters

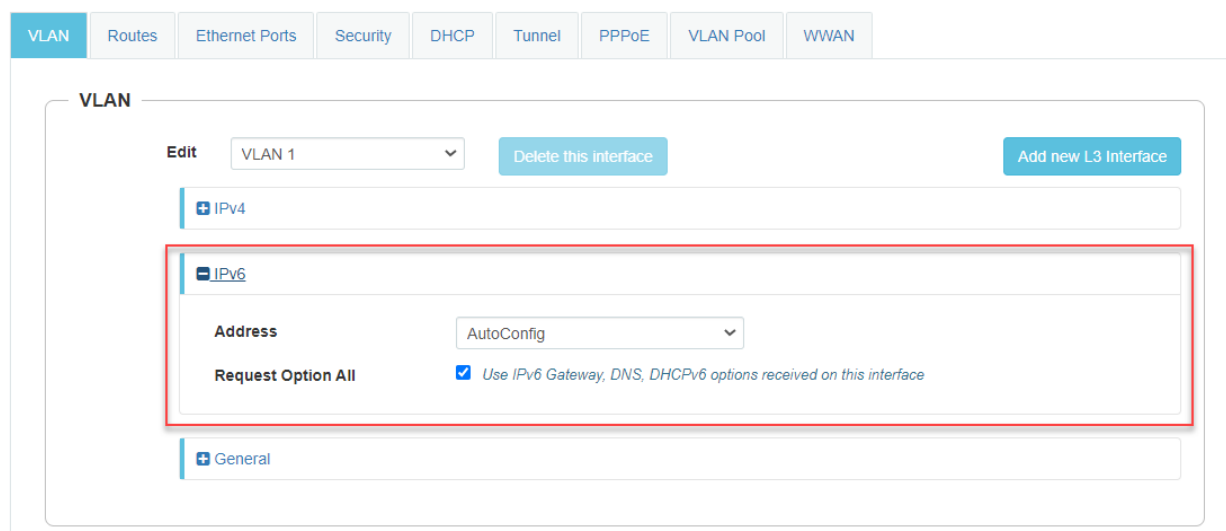
Parameters	Description	Range	Default
Address	Provision to configure the mode of IPv6 address configuration for an interface selected. Five modes are supported: <ul style="list-style-type: none"><li>• Disabled</li><li>• AutoConfig</li><li>• Static</li><li>• Stateless DHCPv6</li><li>• Stateful DHCPv6</li></ul>	–	AutoConfig
Request Option All	This configuration decides the interface on which AP will learn the following: <ul style="list-style-type: none"><li>• IPv6 default gateway</li><li>• DHCP client options like Option 52 and Option 24 (Controller discovery like controller hostname / IPv6 address)</li><li>• DNS Servers</li><li>• Domain Name</li></ul>	–	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** checkbox.
3. Click **Save**.

Figure 32: VLAN (IPv6) parameters



## Routing & DNS

Table 37: 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 textbox.
2. Enter primary domain server name in the **DNS Server 1** textbox.
3. Enter secondary domain server name in the **DNS Server 2** textbox.
4. Enter **Domain Name** in the textbox.
5. Enable **IPv6 Preference** checkbox.
6. Click **Save**.

Figure 33: Routing & DNS (Pv6) parameters

The screenshot shows a configuration window titled "Routing & DNS". At the top, there are two tabs: "IPv4" and "IPv6". The "IPv6" tab is selected and highlighted with a red border. Below the tabs, there are several configuration fields:

- Default Gateway:** A text input field with the description "IP address of default gateway".
- DNS Server 1:** A text input field with the description "Primary Domain Name Server".
- DNS Server 2:** A text input field with the description "Secondary Domain Name Server".
- Domain Name:** A text input field with the description "Domain name".
- IPv6 Preference:** A checkbox with the label "Prefer IPv6 address over IPv4 for addresses resolved via DNS".

At the bottom of the window, there are two buttons: "Save" and "Cancel".

## Routes

Table 38: 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/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: <ul style="list-style-type: none"> <li>• Destination IP/prefix</li> <li>• Gateway</li> </ul>	–	–

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/DHCP** from the **Gateway Source Precedence** checkbox.
2. Click **Save**.

To configure **Add Multiple Route Entries**:

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

Figure 34: Routes (IPv6) parameters

VLAN Routes Ethernet Ports Security DHCP Tunnel PPPoE VLAN Pool WWAN

### Gateway Source Precedence

**IPv4**

STATIC  
DHCP  
PPPoE

Save

**IPv6**

STATIC  
AUTO-CONFIG/DHCP

Save

### Add Multiple Route Entries - IPv4

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

Destination IP	Mask	Gateway	Action
No routes available			

1 / 1    10 items per page

### Add Multiple Route Entries - IPv6

Destination IP/prefix:    Gateway:    Save

Destination IP	Gateway	Action
No routes available		

1 / 1    10 items per page

### Port Forwarding

Port:    IP Address:    Type: TCP    Save

Port	IP Address	Protocol	Action
No rules available			

1 / 1    10 items per page

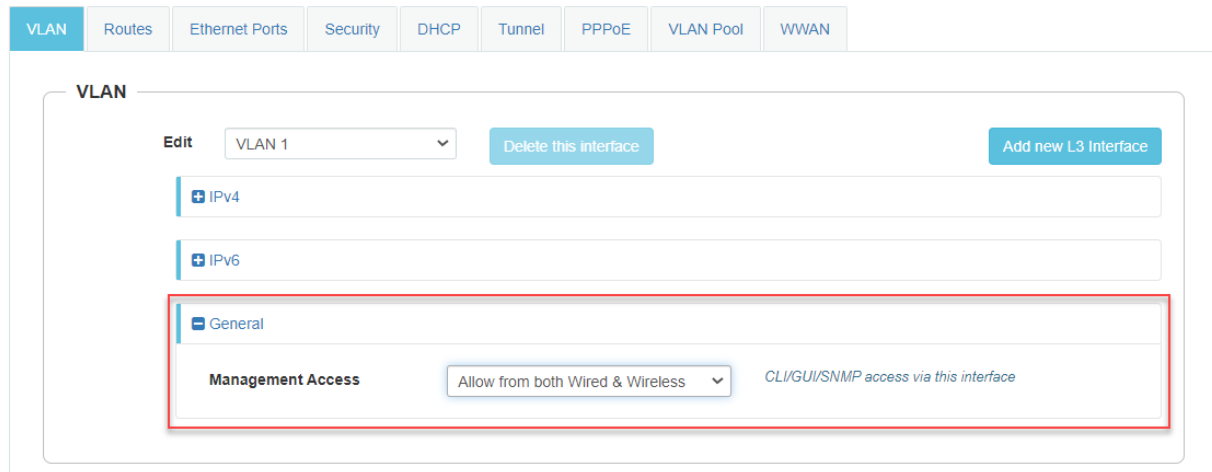
## General network parameters

Table 39: 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: <ul style="list-style-type: none"> <li>Block</li> <li>Allow from Wired</li> <li>Allow from both wired and wireless</li> </ul>	–	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.

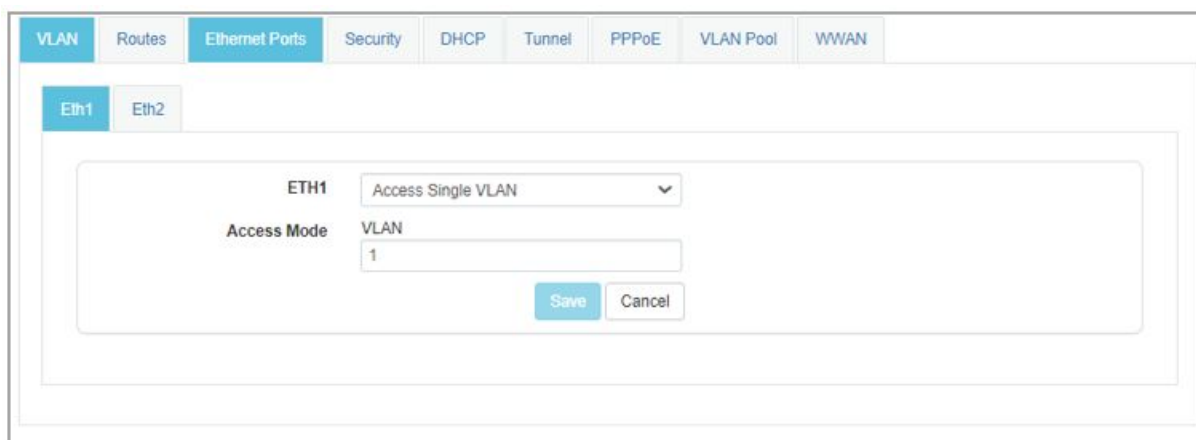
Table 40: Ethernet Ports parameters

Parameters	Description	Range	Default
Ethernet	Enterprise Wi-Fi AP devices Ethernet port is provisioned to operate in the following modes: <ol style="list-style-type: none"> <li>Access Single VLAN Single VLAN traffic is allowed in this mode.</li> <li>Trunk Multiple VLANs Multiple VLANs are supported in this mode.</li> </ol>	–	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 textbox.
3. Click **Save**.

Figure 36: Ethernet Ports parameters



## General network parameters

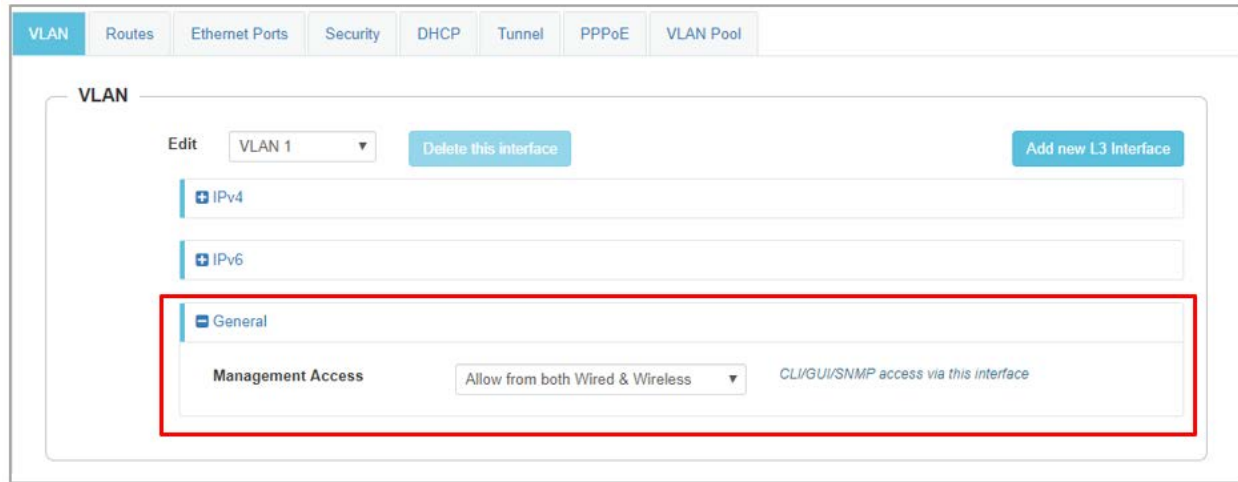
Below table lists the fields that are displayed in **Configure > Network > VLAN > General parameters** tab:

Table 41: 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: <ul style="list-style-type: none"> <li>• Block</li> <li>• Allow from Wired</li> <li>• Allow from both wired and wireless</li> </ul>	–	Allow from both Wired and Wireless

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

Figure 37: The General parameters



## Security

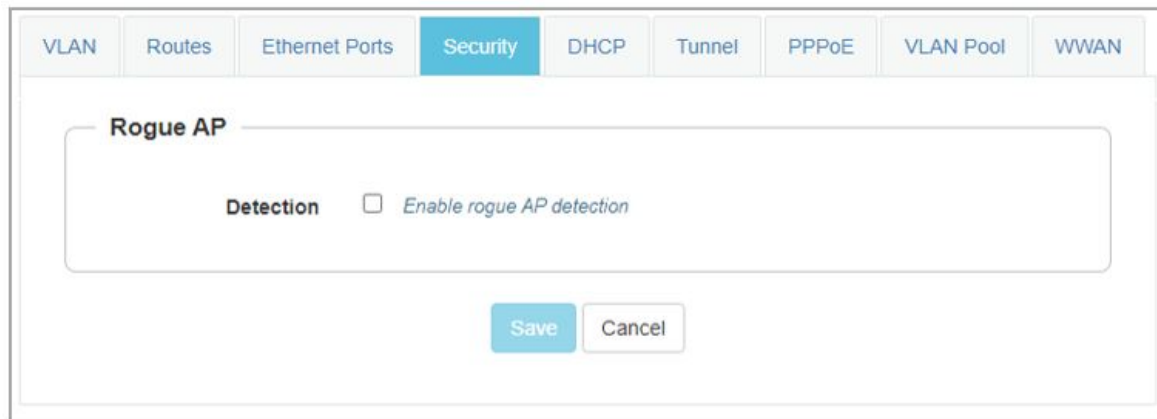
The below table lists the fields that are displayed in the **Configuration > Network > Security** tab.

Table 42: Security parameters

Parameters	Description	Range	Default
<b>Rogue AP</b>			
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** checkbox to enable this functionality.

Figure 38: Security parameters



## DHCP

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

Table 43: 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.	–	–
<b>Add Bind List</b>			
	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: <ul style="list-style-type: none"> <li>• MAC Address</li> <li>• IP Address</li> </ul>	–	–

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** textbox.
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 39: DHCP parameters

The screenshot displays the DHCP configuration page with the following elements:

- Navigation Tabs:** VLAN, Routes, Ethernet Ports, Security, **DHCP**, Tunnel, PPPoE, VLAN Pool.
- Pool Management:** Edit (dropdown), Delete this Pool, Create Pool.
- Configuration Fields:**
  - Address Range:** Start, End (IP address range to be assigned to clients)
  - Default Router:** (Default router IP)
  - Domain Name:** (Domain Name)
  - DNS Address:** Primary, Secondary (Domain name for the client)
  - Network:** IP, Mask (Subnet number and mask of the DHCP address pool)
  - Lease:** 1, Hours, Minutes (Lease time (days:hours:minutes))
- Buttons:** Save, Cancel.
- Add Bind List Section:**
  - MAC Address:** xx:xx:xx:xx:xx:xx
  - IP Address:** xxx.xxx.xxx.xxx
  - Save** button.
  - Table:**

MAC Address	IP Address	Action
No bind list available		
  - Page Controls:** 1 / 1, 10 items per page.

## Tunnel

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

Table 44: 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: <ul style="list-style-type: none"> <li>• L2TP</li> <li>• L2GRE</li> <li>• OFF</li> </ul>	–	OFF
<b>L2TP</b>			
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: <ul style="list-style-type: none"> <li>• DEFAULT</li> <li>• CHAP</li> <li>• MS-CHAP</li> <li>• MS-CHAPv2</li> <li>• PAP</li> </ul>	–	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: <ul style="list-style-type: none"> <li>• DEFAULT</li> <li>• CHAP</li> <li>• MS-CHAP</li> <li>• MS-CHAPv2</li> <li>• PAP</li> </ul>	–	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
<b>L2GRE</b>			
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	A number of retries before Fail-Over to secondary peer.	2-10	5

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** textbox.

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**:

12. Enter IP address or domain name in the **Primary Remote Host/Secondary Remote Host** 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**.

Figure 40: The Tunnel parameters

The screenshot shows the 'Tunnel' configuration page in a network management interface. The 'Tunnel Encapsulation' is set to 'L2TP'. Below this, there are two sections: 'L2TP' and 'L2GRE'.

**L2TP Section:**

- Remote Host:** 0.0.0.0 (IP address or domain)
- Authentication Info:** admin (Max 64 characters)
- Auth Type:** DEFAULT (MS-CHAPv2, MS-CHAP, CHAP, PAP)
- Secondary Remote Host:** 0.0.0.0 (IP address or domain)
- Secondary Authentication Info:** admin (Max 64 characters)
- Secondary Auth Type:** DEFAULT (MS-CHAPv2, MS-CHAP, CHAP, PAP)
- TCP MSS:**  1400 (TCP Maximum Segment Size (422-1410 bytes))
- PMTU Discovery:**  (Path MTU Discovery)
- Disconnect Wireless Clients:**  (Disconnect Wireless Client when state of L2TP tunnel is down)

**L2GRE Section:**

- Primary Remote Host:** 10.110.211.39 (IP address or domain)
- Secondary Remote Host:** 0.0.0.0 (IP address or domain)
- DSCP:** 0 (Differentiated Service Code Point)
- TCP MSS:**  1402 (TCP Maximum Segment Size (472-1460 bytes))
- PMTU Discovery:**  (Path MTU Discovery)
- MTU:** 1460 (Configure MTU for L2GRE tunnel (850-1460 bytes))
- GRE:** GRE in UDP (Enable GRE in UDP encapsulation (RFC 8086))
- Disconnect Wireless Clients:**  (Disconnect Wireless Client when state of L2TP tunnel is down)
- Tunnel Reachability:** 240 (Periodic interval for verifying the RX packet from GRE peer (30-240))
- Tunnel Retry Attempts:** 5 (Number of Retries before Fail-Over to Secondary peer (2-10 seconds))

At the bottom of the form, there are 'Save' and 'Cancel' buttons.

## 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 45: PPPoE parameters

Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disabled

Parameters	Description	Range	Default
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 41: PPPoE parameters

**PPPoE**

**Basic Settings**

Enable

VLAN ID  
 Vlan ID assigned to PPPoE

Service Name  
 Configure PPPoE service-name parameters (max 32 characters)

**Authentication Info**

Username

Password

MTU  
 Configure MTU for PPPoE connection (500-1492 bytes)

TCP MSS Clamping Enable TCP Maximum Segment Size Clamping to avoid packet fragmentation

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

## VLAN Pool

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

Table 46: 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 42: The VLAN Pool parameters

The screenshot displays the configuration page for a VLAN Pool. At the top, there is a navigation menu with tabs for VLAN, Routes, Ethernet Ports, Security, DHCP, Tunnel, PPPoE, VLAN Pool (selected), and WWAN. The main configuration area contains the following elements:

- VLAN Pool Name:** An empty text input field.
- VLAN ID List:** A text input field containing the value "1-4094".
- Table:** A table with three columns: "VLAN Pool Name", "VLAN ID List", and "Act...". It contains one entry: "pool1" with "1,20" in the second column and a trash icon in the third.
- Footer:** A status bar showing "1\_ 1 of 1 items", navigation arrows, a page number "1", a search icon, and a dropdown menu set to "10 items per page".
- Buttons:** "Save" and "Cancel" buttons at the bottom center.



## 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 e600, XV2-2, XV3-8, XE3-4, and XE5-8 platforms only.

Table 47: 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: <ul style="list-style-type: none"><li>• Enabled: Ethernet will be the primary connection and WWAN will be backup.</li><li>• Disabled: 3G/4G (WWAN) will be the only working connection.</li></ul> <b>Note:</b> 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** checkbox to enable this functionality.
2. Check/Uncheck **Failover Only** to enable/disable.
3. Enter the **APN** address in the textbox.
4. Enter the **Authentication** credentials.
5. Enter any IPv4 address to **Monitor Hoist** textbox.
6. Click **Save**.

Figure 43: WWAN parameters

The screenshot shows a web-based configuration interface for an AP Group named 'Ent\_Mesh\_ZeroTouch\_APGrp'. The 'Configuration' tab is active, and the 'Network' section is selected in the left-hand navigation menu. The main content area displays several configuration options: 'DHCP Pool', 'Tunnels', 'PPPoE', and 'VLAN Pool', each with a plus sign icon. The 'WWAN' section is expanded, showing a checkbox for 'Enable Wireless WAN using a USB cellular dongle for internet access' which is currently unchecked. Below this, the 'Failover Only' section has a checked checkbox for 'Use WWAN as backhaul only when failover is triggered'. The 'APN' section includes a text input field and a label 'Configure network provider APN address'. The 'Authentication Info' section contains fields for 'Username' and 'Password' (with a 'Show' button), and a 'Monitor Host' field with the label 'Host to monitor in order to trigger WWAN failover'. A 'Save' button is located at the bottom of the configuration area.

## Supported hardware

Cambium Networks currently support following models:

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

# Chapter 8: Managing Filters

---

This chapter describes the following topics:

- [Overview](#)
- [Filter list](#)
- [Filters](#)
- [Application control](#) Premium feature

## 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/{mask|prefix-length}}|any) (SOURCE-PORT|any) (DESTINATION-IP/{mask|prefix-length}}|any) (DESTINATION-PORT|any) (in|out|any) (DSCP{0-63}) <(optional)//Filter_name>
```



#### Note

All fields are mandatory. If no parameter to configure, give 'any'. Direction is 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/{mask|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) <(optional)//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 !1.1.1/8 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-len
gth]}|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: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
```

- 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
```

- 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      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      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 Category 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 Application	Productivity Index	Productivity 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	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 frame:** 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 9: 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 10: Configuring Services

---

This chapter describes the following topics:

- [Overview](#)
- [Configuring services](#)

## Overview

This chapter gives an overview of Enterprise Wi-Fi AP configurable parameters related to 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](#)
- [Location API](#)
- [Speed Test](#)
- [BT Location API](#)
- [Bonjour Gateway](#)
- [Link Aggregation Control Protocol \(LACP\)](#)
- [Real-Time Location System \(RTLS\)](#)

## User Groups [Premium feature](#)

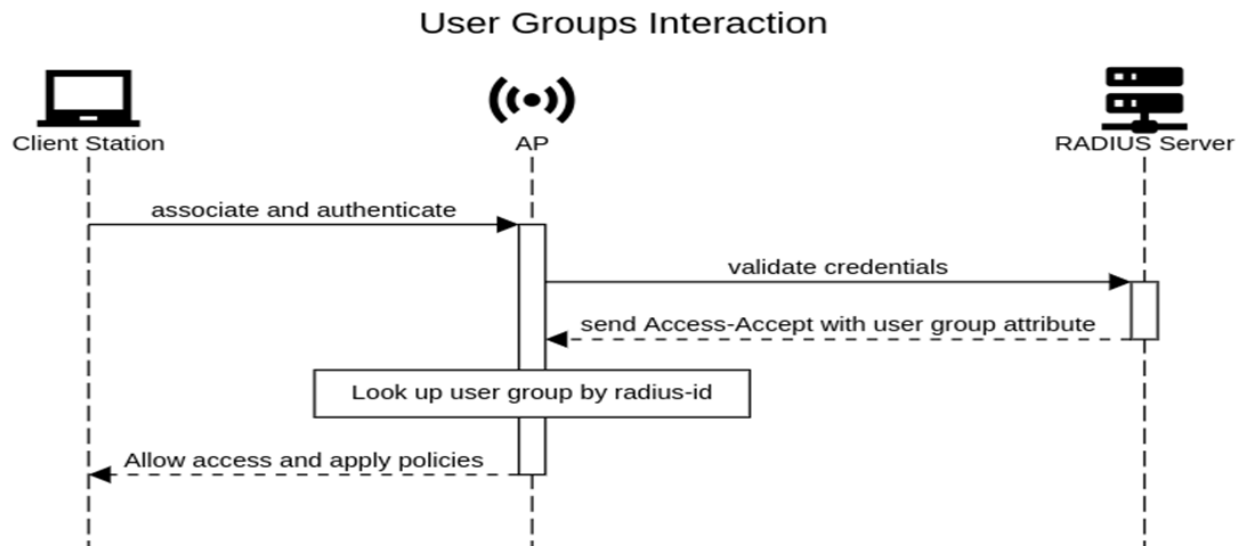
Some policies, like VLAN, require many RADIUS attributes to be sent by the RADIUS server and processed by the AP. Some wireless network administrators do not have administrative access to the RADIUS server, so making changes to wireless policies would require waiting for the RADIUS administrator to make 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 44: 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 selection 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:

```

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

```

## User group properties and actions

A user group supports the following properties and actions:

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

## User group policies

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

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

## 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 48: 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 45: Location API parameters

**Location API**

Enable

Server  Configure HTTP/HTTPS server with the port number (0-65535)

Interval  Configure Location API interval (2-3600) seconds

MAC Anonymization  Ignore Anonymized MACs ⓘ



**Note**

For further details about this feature and sample reference output, go to <https://support.cambiumnetworks.com/files/cnpilot-tech-ref/> and download **Wireless client Presence and Locating 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 AP or between Enterprise Wi-Fi AP and with 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.

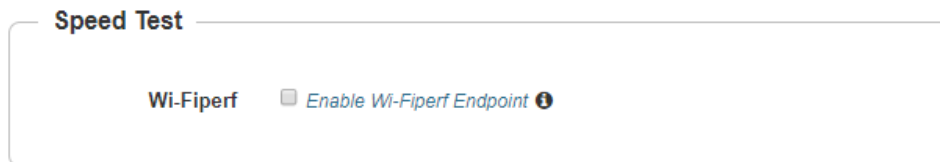
Table 49 lists the fields that are displayed in the **Configuration > Services > Speed Test** tab.

Table 49: Speed Test parameters

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

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

Figure 46: Speed Test parameters



## 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 50: 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 51: 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': 'E600-A55AEC',  
  'ble_discoverd_clients':{Array of 0-250 devices}  
}
```

Bluetooth API Data Format

```
{  
  bt_rssi': u' -80 dBm ',  
  bt_mac': 14-8F-21-FD-37-18', u  
  'bt_uuids': Garmin International, Inc. (0xfelf)\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 52: 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 47: 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 System 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 11: Operations

This chapter describes the following topics:

- [Overview](#)
- [Firmware upgrade](#)
- [System](#)
- [Configuration](#)

## 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.



### Warning

Platform: e410, e510, e430, e600 and e700

- Firmware upgrade should be in HTTP mode.
- Path to upgrade above platforms to 6.4 Software version.
  - Software version 4.2.2 > Software version 6.4

Table 53 lists the fields that are displayed in the **Operations > Firmware** update tab.

Table 53: 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 48: Firmware update parameters

### Firmware update

Choose File No file chosen

Upgrade Firmware

Upgrade Status :

## System

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

Table 54 lists the fields that are displayed in the **Operations > System** tab:

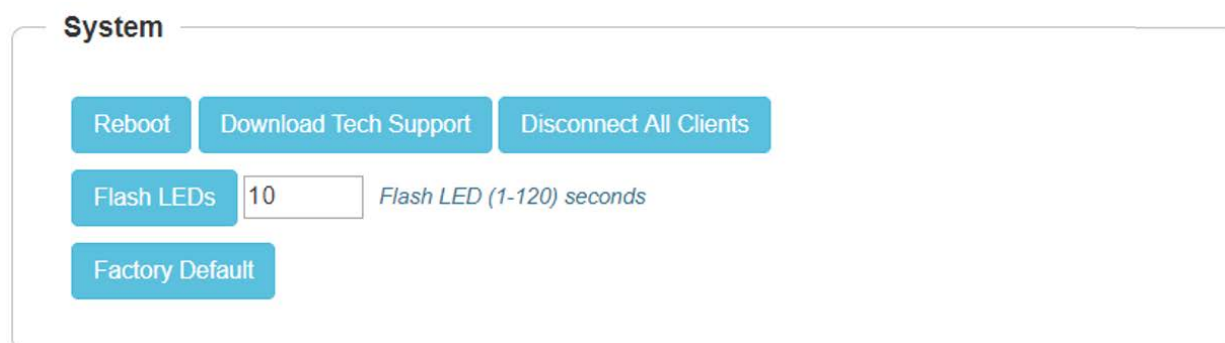
Table 54: System parameters

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 49: 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, XV2-2T, 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.

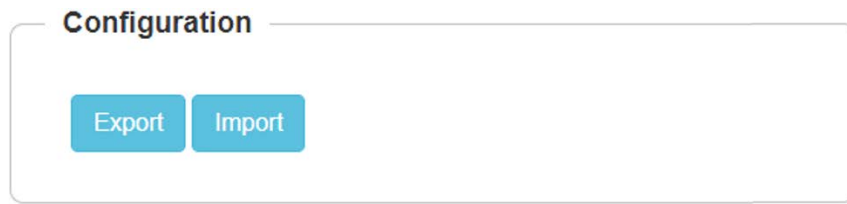
Figure 50: Configuration parameters

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 51: Configuration parameters



# Chapter 12: 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](#)
  - [Debug Logs](#)
  - [Events](#)
- [Rdio Frequency \(RF\)a](#)
  - [Wi-Fi Analyzer](#)
- [Packet capture](#)
- [Performance](#)
  - [Connectivity](#)
  - [Speedtest on Access Point](#)
- [XIRCON tool support](#)
  - [XIRCON tool support for Linux 1.0.0.40](#)

## Logging

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

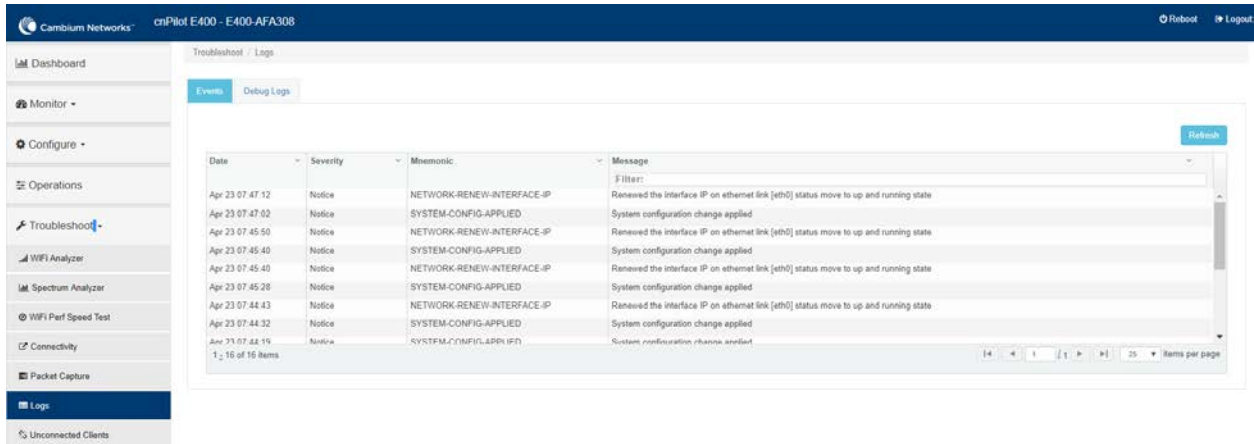
## Events

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 52: Events parameters

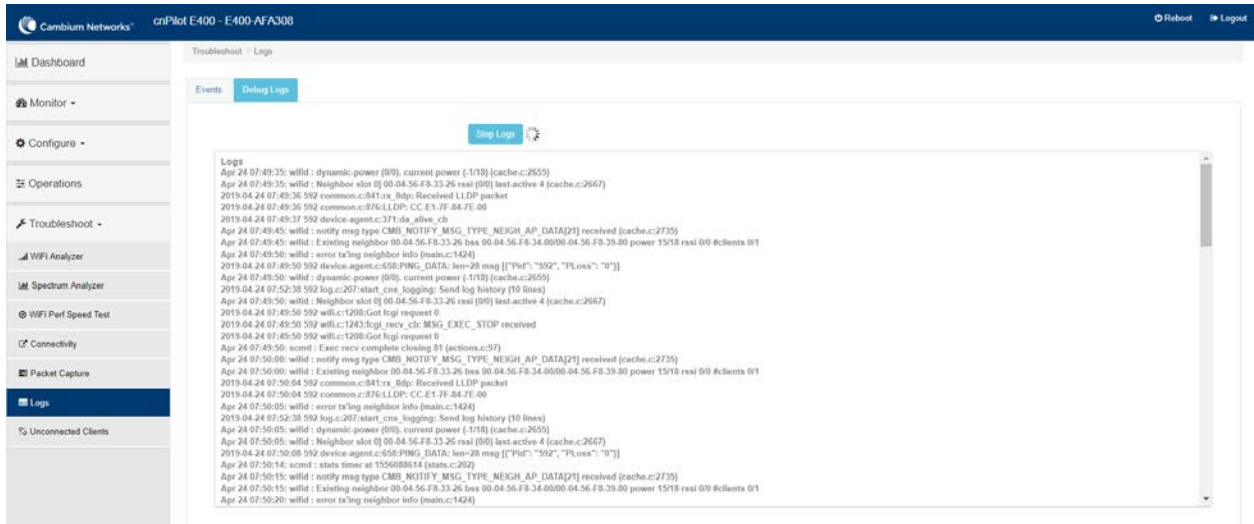


## Debug Logs

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 53: 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 54: *Interference Mode*



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



Figure 55: Troubleshoot > Wi-Fi Analyzer > Number of APs Mode



## Packet capture

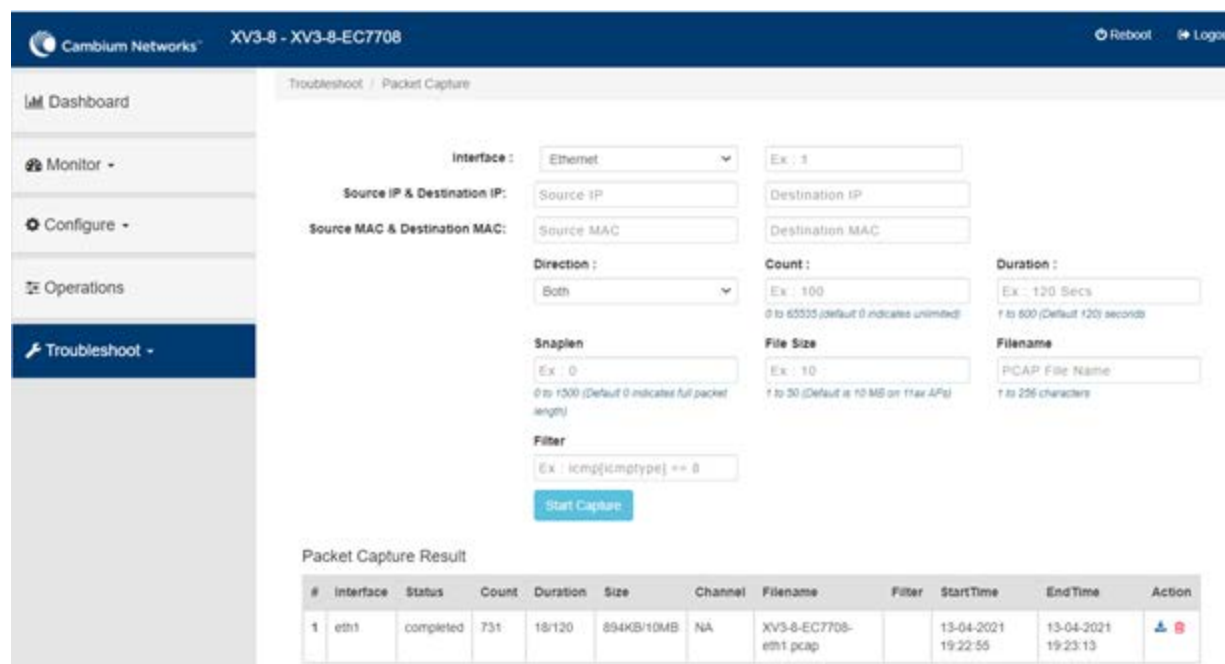
Allows the administrator to capture packets from the APs UI, cnMaestro UI, or XMS-Cloud. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, and port number. The user can trigger packet capture on one or more interfaces, simultaneously view the 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 56: 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 55: Troubleshoot: Connectivity

Parameters	Description	Range	Default
<b>Ping</b>			
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.	-	-
<b>DNS Lookup</b>			
Host Name	Provide Hostname whose IP must be resolved.	-	-
DNS Test Result	Displays the IPs that are associated with configured Hostname.	-	-
<b>Traceroute</b>			
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 57: Connectivity (Ping) parameters

The screenshot shows a web-based interface for network troubleshooting. At the top, it says "Troubleshoot / Connectivity". The main section is titled "Test Type:" and has a dropdown menu set to "Ping", which is highlighted with a red box. Below this, there are three input fields: "IP Address or Hostname:" with "www.google.com", "Number of Packets:" with "3" (and "Min = 1, Max = 10" to the right), and "Buffer Size:" with "56" (and "Min = 1, Max = 65507" to the right). A blue "Start Ping" button is located below these fields. At the bottom, there is a "Ping Result" section containing the following text: "PING www.google.com (216.58.197.68): 56 data bytes", "64 bytes from 216.58.197.68: seq=0 ttl=56 time=7.428 ms", "64 bytes from 216.58.197.68: seq=1 ttl=56 time=7.131 ms", "64 bytes from 216.58.197.68: seq=2 ttl=56 time=7.359 ms", "--- www.google.com ping statistics ---", "3 packets transmitted, 3 packets received, 0% packet loss", and "round-trip min/avg/max = 7.131/7.306/7.428 ms".

Figure 58: Connectivity (DNS Lookup) parameters

Troubleshoot / Connectivity

Test Type : DNS Lookup ▼

Host Name:

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

Figure 59: Connectivity (Traceroute) parameters

Troubleshoot / Connectivity

Test Type : Traceroute ▼


IP Address or Hostname :

Fragmentation :  Off  On

Trace Method :  ICMP Echo  UDP

Display TTL :  Off  On

Verbose :  Off  On



**Traceroute Result**

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

## 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 System 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 13: Management Access

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

- [Local authentication](#)
- [SSH-Key authentication](#)
- [RADIUS authentication](#)

## Local authentication

This is the default authentication mode enabled on 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 60: Configure/update default password of the admin user

The screenshot shows the Cambium Networks web interface for a cnPilot E400 - E400-AFA308 device. The interface is divided into two main sections: System and Management. The System section includes fields for Name (E400-AFA308), Location, Contact, Country-Code (India), Placement (Indoor selected), LED (checked), and LLDP (unchecked). The Management section includes fields for Admin Password (masked), Autopilot (Default), Teinet (unchecked), SSH (checked), SSH Key (empty), HTTP (checked), and HTTP Port (80).

## 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 61: Management parameters

The screenshot displays the configuration page for a Cambium Networks cnPilot E400 - E400-AFA308 device. The interface is divided into two main sections: System and Management.

**System Configuration:**

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

**Management Configuration:**

- Admin Password:** (Configure password for authentication of GUI and CLI sessions)
- Autopilot:** Default (Autopilot Management of APs)
- Teletnet:**  Enable Telet access to the device CLI
- SSH:**  Enable SSH access to the device CLI
- SSH Key:** (Use SSH keys instead of password for authentication)
- HTTP:**  Enable HTTP access to the device GUI
- HTTP Port:** 80 (Port No for HTTP access to the device GUI(1-65535))
- HTTPS:**  Enable HTTPS access to the device GUI
- HTTPS Port:** 443 (Port No for HTTPS access to the device GUI(1-65535))

## SSH Key generation

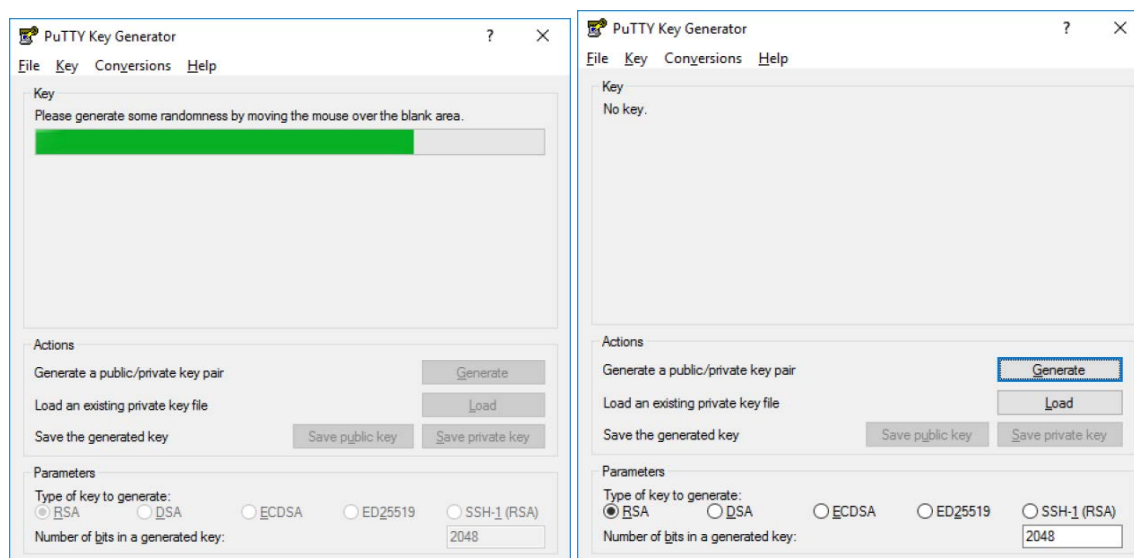
### Windows

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 13](#).

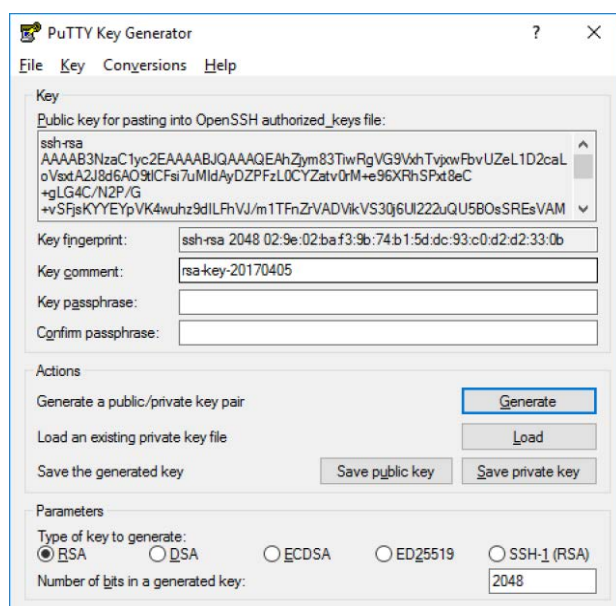


Figure 62: Generating public/private Key



2. Save the Public key and Private key once the key pair is generated as shown in Chapter 13.

Figure 63: 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 13.

Figure 64: Public Key location path

```
pk@ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/pk/.ssh/id_rsa):
Created directory '/home/pk/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/pk/.ssh/id_rsa.
Your public key has been saved in /home/pk/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:0qt4vJduO4uvsdpTpkNzQ9uorlH7ydwE9fiEXOh0Kao pk@ubuntu
The key's randomart image is:
+----[RSA 2048]-----+
|
| ..
| .+.o|
| . . . =.*|
| . S.. = o|
| .oo*... o|
| . +E.. . .|
| oo*X. + +|
| ooBXOO. = .|
|
+----[SHA256]-----+
pk@ubuntu:~$
```

2. The Public key is now located in PATH mentioned in [Chapter 13](#).

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

3. The private key (identification) is now saved in PATH as mentioned in [Figure 65](#).

PATH = “Your identification has saved in <>”

Figure 65: Private Key saved path

```
pk@ubuntu:~$ cat /home/pk/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDfZq+gc13qG8DlckyFU2JqyW5pI9q8POMrVtrM9Vu5
P851kbIiCtsTmPm6Ewrfq/nhWwsn6k4p20pTZ/1aX/Ww9Bwf4jjw8nOqNY95z1JUD9mV48gqrOY8qbXv
5gybXLZ+A0LarSgDaeoasM34xiJEqL+/GwkJw9/ckyueliSwAeX8ki++zJeIOQZrJWcJ6mlYHZfd4Yyb
1LRg78L+q4YbHZAdkooUkTNXJ0kaBwR2i30JjHxD1D+SRE3DrP9xAAD1lcB5MvgQNWeBJ4ale4rkwkphP
QetH/lisY/DI9nkr8Hwul2JEDeMq5yII7Fdh6ALJb+b2mtZnbGBxdsM4HrTt pk@ubuntu
pk@ubuntu:~$
pk@ubuntu:~$
```

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 66: RADIUS Server and RADIUS Secret parameters

The screenshot displays the configuration page for a Cambium Networks criPilot E400 - E400-AFA308 device. The interface is divided into two main sections: System and Management.

**System Configuration:**

- Name: E400-AFA308
- Location: (empty)
- Contact: (empty)
- Country-Code: India
- Placement: Indoor (selected), Outdoor
- LED:  Whether the device LEDs should be ON during operation
- LLDP:  Whether the AP should transmit LLDP packets

**Management Configuration:**

- Admin Password: (masked)
- Autopilot: Default
- Telnet:  Enable Telnet access to the device CLI
- SSH:  Enable SSH access to the device CLI
- SSH Key: (empty)
- HTTP:  Enable HTTP access to the device GUI
- HTTP Port: 80
- HTTPS:  Enable HTTPS access to the device GUI
- HTTPS Port: 443
- RADIUS Mgmt Auth:  Enable RADIUS authentication of GUI/CLI sessions
- RADIUS Server: (empty)
- RADIUS Secret: (empty)

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

Figure 67: UI Login page

The screenshot shows the login interface. At the top, there is a blue header with the text "Login". Below this, there is a red-bordered box containing the login form. The form includes a user selection dropdown menu with "bob" selected, a password input field with masked characters, and a blue "Sign In" button.

# Chapter 14: Mesh

---

From System Release 6.4 onwards, Enterprise Wi-Fi 6 Access Point supports Mesh connections between radios. Even though multiple mesh hop is supported in System Release 6.4, the suggested max 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 E600 is supported. Given the larger set of available channels and typically cleaner RF environment, Cambium Networks recommend 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 characters.

## 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 different deployment scenarios which are listed below:

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

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

Figure 68: Single hop mesh connection in 5 GHz with two Mesh Clients

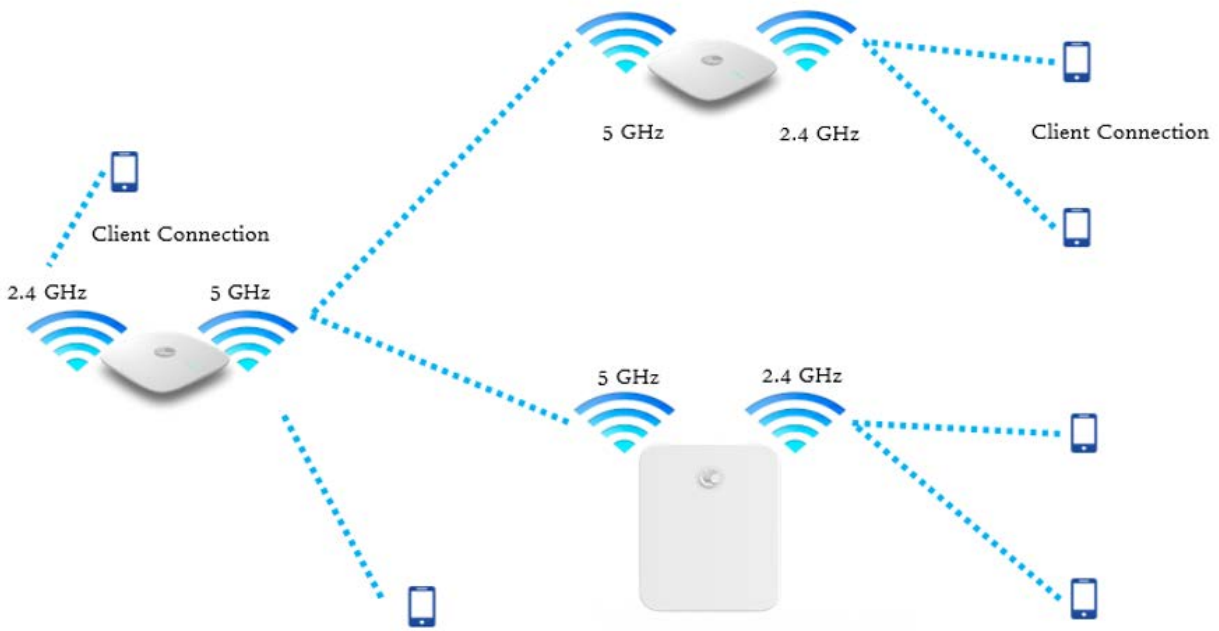


Figure 69: Single hop mesh connection in 5 GHz with two Mesh Clients and 2.4 GHz and 5 GHz as access

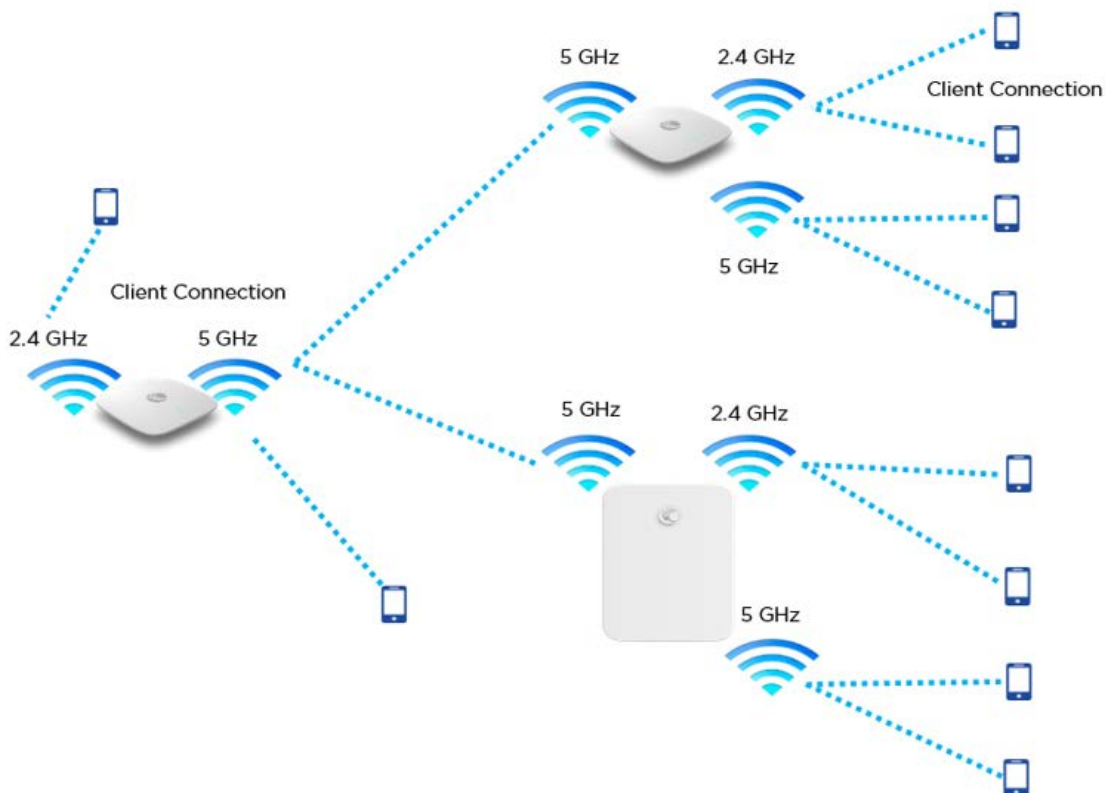
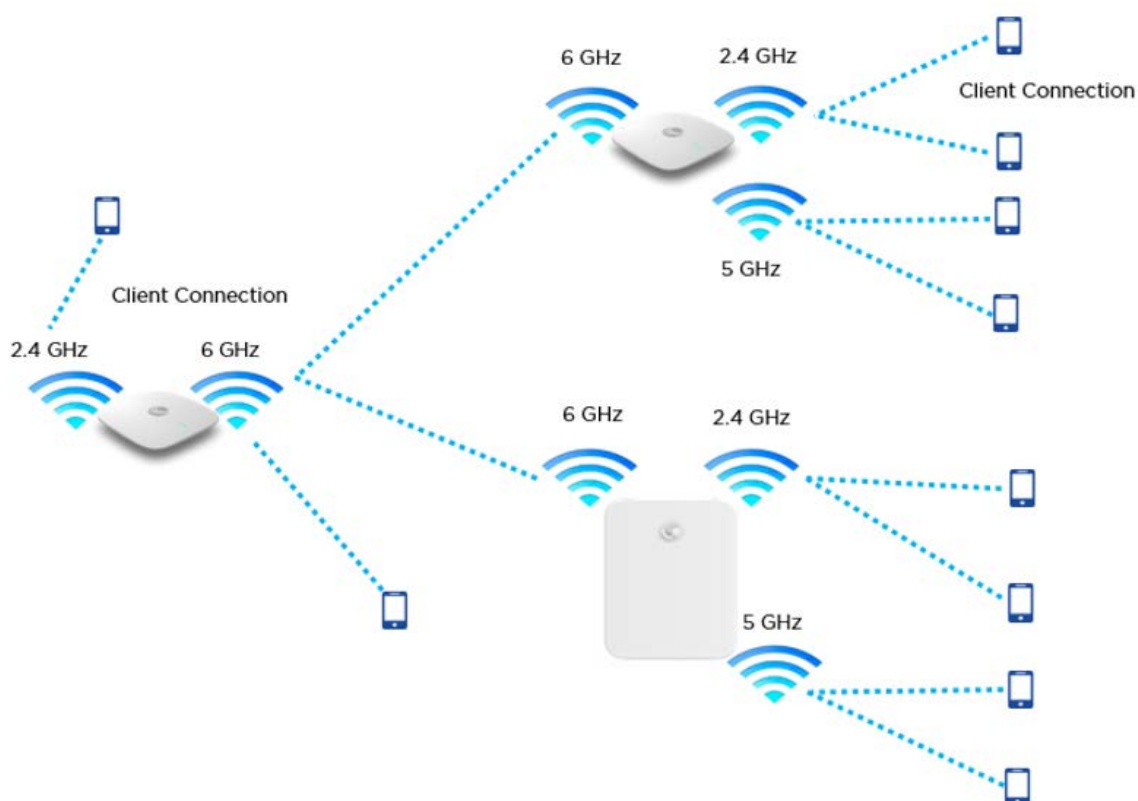


Figure 70: Single hop mesh Connection in 6 GHz with two Mesh Clients



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

1. 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.

2. 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.

3. 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 56: Mesh configurable parameters

Parameter	Description	Range	Default
Mesh	<p>This parameter is required when a mesh connection is established with Enterprise Wi-Fi devices. Four options are available under this parameter:</p> <ol style="list-style-type: none"> <li>1. Base <p>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.</p> </li> <li>2. Client <p>A WLAN profile configured with a Mesh Client scans all available channels on startup, looking for a mesh-based AP to connect.</p> </li> <li>3. Recovery <p>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.</p> </li> </ol>	-	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	<p>Each SSID can be configured to be transmitted as per the deployment requirement. For a mesh WLAN profile, options available to configure the band:</p> <ul style="list-style-type: none"> <li>• 2.4 GHz</li> <li>• 5 GHz</li> <li>• 6 GHz</li> </ul>	-	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	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol>	-	Disabled
Mesh Client Monitor	<ol style="list-style-type: none"> <li>1. Duration Duration in minutes of ping failure after which mesh connectivity is re-established.</li> <li>2. Host Configure a server to monitor with ping to decide if mesh connectivity needs to be re-established.</li> </ol>	-	-
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:

WLANs > Ent\_Mesh\_Base

Configuration Devices

**WLAN**

AAA Servers

Guest Access

Access Control

**Basic Information**

Type\*  
Enterprise Wi-Fi

Name\*  
Ent\_Mesh\_Base

Description

**Basic Settings**

**SSID**

Enable

SSID\*  
CMBIUM\_MESH\_BASE The SSID of this WLAN (up to 32 characters)

Mesh  
Base Mesh Base/Client/Recovery mode

VLAN\*  
1 Default VLAN assigned to clients on this WLAN (1-4094)

Security  
WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase\*  
..... Show WPA2 Pre-shared security passphrase or key

Band  
 2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation  
Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

Hide SSID Do not broadcast SSID in beacons

Mesh Vlan Tagging Enable the vlan tagging over mesh link

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

CLI configuration:

```
XV3-8-EC7708(config-wlan-1)# Mesh Base
XV3-8-EC7708(config-wlan-1)# ssid CMBIUM_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:

WLANs > Ent\_Mesh\_Client

Configuration Devices

WLAN

**Basic Information**

Type\*  
Enterprise W-Fi

Name\*  
Ent\_Mesh\_Client

Description

**Basic Settings**

SSID

Enable

SSID\*  
CAMBIUM\_MESH\_BASE The SSID of this WLAN (up to 32 characters)

Mesh  
Client Mesh Base/Client/Recovery mode

VLAN\*  
1 Default VLAN assigned to clients on this WLAN (1-4094)

Security  
Open Set authentication and encryption type

Transition SSID  
Configure the matching open/owe transition SSID

Band

2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Mesh Vlan Tagging Enable the vlan tagging over mesh link

AP Groups > Ent\_Mesh\_ZeroTouch\_APGrp

Dashboard Notifications Configuration Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

**User-Defined Overrides**

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

**Variables and Macros**

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 1
mesh-recovery-interval 5
mesh-client-monitor host 8.8.8.8
mesh-client-monitor duration 2
!
```

## 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:

The screenshot shows the configuration page for 'Ent\_Mesh\_Recovery' in the cnMaestro interface. The page is divided into two main sections: 'Basic Information' and 'Basic Settings'. In 'Basic Information', the 'Type' is set to 'Enterprise Wi-Fi', the 'Name' is 'Ent\_Mesh\_Recovery', and the 'Description' field is empty. In 'Basic Settings', the 'SSID' section has 'Enable' checked. The 'Mesh' mode is set to 'Recovery', with a note 'Mesh Base/Client/Recovery mode'. The 'VLAN' is set to '1', with a note 'Default VLAN assigned to clients on this WLAN (1-4094)'. The 'Transition SSID' field is empty, with a note 'Configure the matching open/owe transition SSID'. The 'Band' section has '5 GHz' selected, with a note 'Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported'.

### CLI configuration:

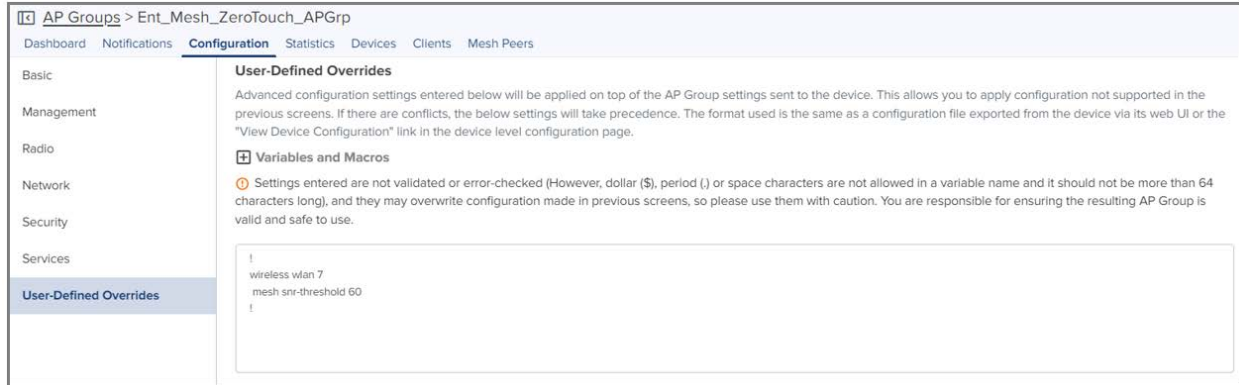
```
XV3-8-EC7708(config-wlan-1)# mesh recovery
XV3-8-EC7708(config-wlan-1)# vlan 1
XV3-8-EC7708(config-wlan-1)# band 5GHz
```

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:

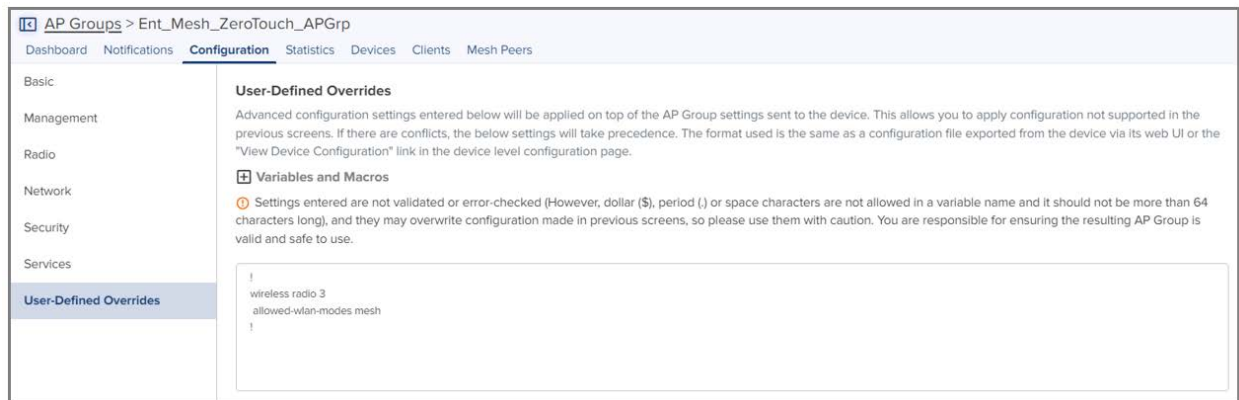
```
XV3-8-EC7708(config-wlan-1)# mesh snr-threshold 60
```

## 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:**

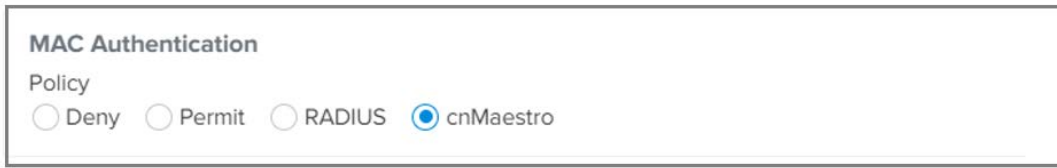
```
XV3-8-EC7708(config-wlan-1)# mac-authentication policy radius
```

- 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

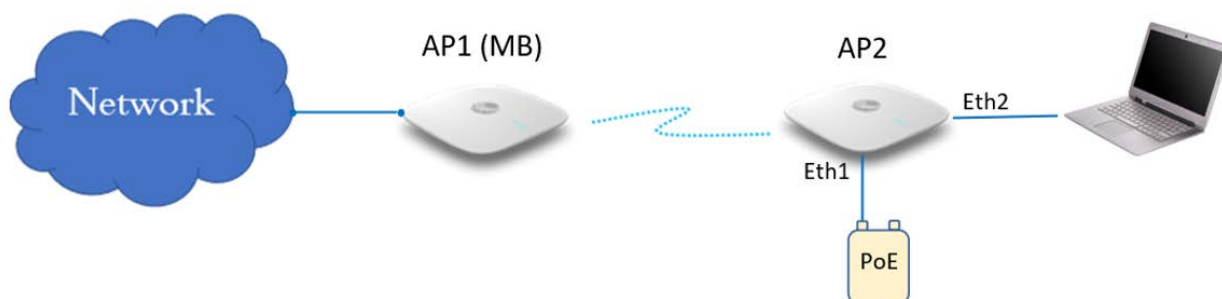
When a single AP Group is used for both MB and MC, AP2 can decide its mesh mode based on eth1 and eth2 connections. To auto-trigger, the type of mesh mode below configuration needs to be pushed on all APs in the mesh link.

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
<ul style="list-style-type: none"> <li>Connected</li> <li>No data enabled</li> </ul>	Connected with no network reachability	No	Disabled	Enabled
<ul style="list-style-type: none"> <li>Connected</li> <li>No data enabled</li> </ul>	Connected with network reachability	Yes	Enabled	Disabled
<ul style="list-style-type: none"> <li>Connected</li> <li>Data-enabled</li> </ul>	Connected with no network reachability	No	Disabled	Enabled
<ul style="list-style-type: none"> <li>Connected</li> </ul>	Connected with no network reachability	Yes	Enabled	Disabled

Eth 1	Eth 2	8.8.8.8 Reachability	MB	MC
<ul style="list-style-type: none"> <li>Data-enabled</li> </ul>				
<ul style="list-style-type: none"> <li>Connected</li> <li>Data-enabled</li> </ul>	Connected with network reachability	Yes	Enabled	Disabled

Figure 71: Deployment Scenario 1

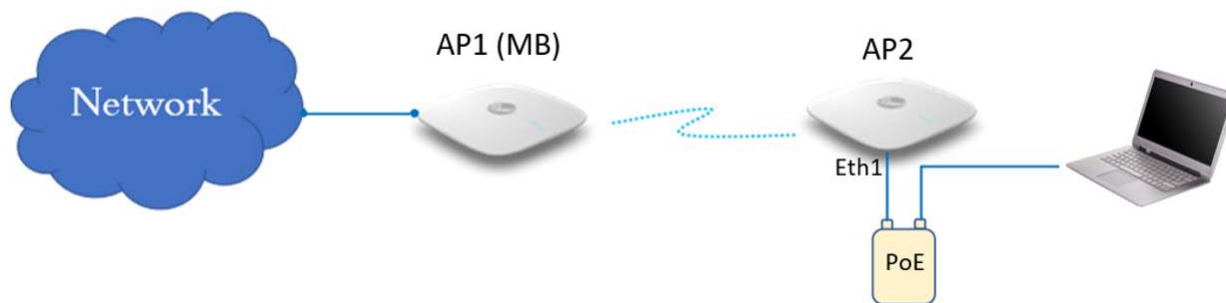


## Scenario 2

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
<ul style="list-style-type: none"> <li>Connected</li> <li>No data enabled</li> </ul>	No	Disabled	Enabled
<ul style="list-style-type: none"> <li>Connected</li> <li>Data-enabled</li> </ul>	No	Disabled	Enabled
<ul style="list-style-type: none"> <li>Connected</li> <li>Data-enabled</li> </ul>	Yes	Enabled	Disabled

Figure 72: Deployment Scenario 2

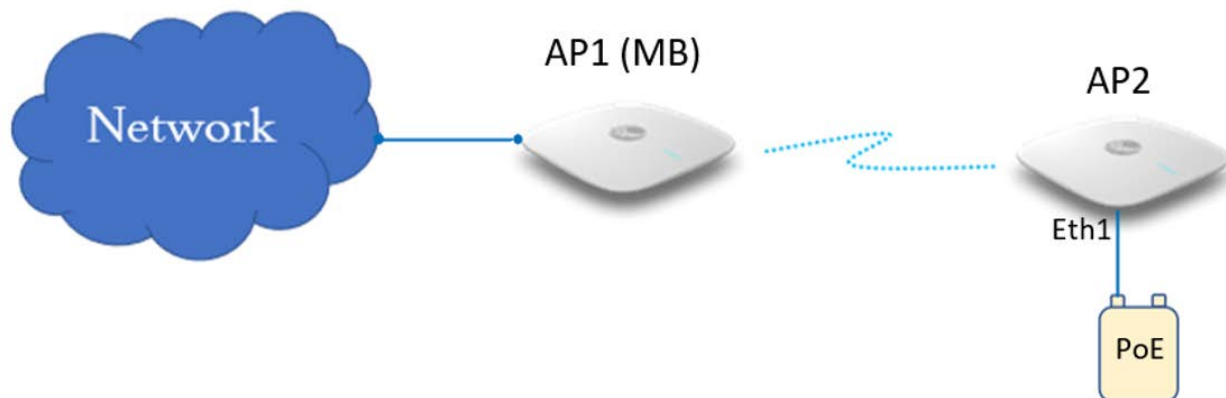


### Scenario 3

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 73: Deployment Scenario 3



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



## cnMaestro configuration:

### Mesh Client

WLANs > Ent\_Mesh\_Client

Configuration Devices

WLAN

**Basic Settings**

SSID

Enable

SSID\*  
 The SSID of this WLAN (up to 32 characters)

Mesh  
 Mesh Base/Client/Recovery mode

VLAN\*  
 Default VLAN assigned to clients on this WLAN (1-4094)

Security  
 Set authentication and encryption type

Passphrase\*  
  WPA2 Pre-shared security passphrase or key

Band  
 2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Mesh Vlan Tagging Enable the vlan tagging over mesh link

**Advanced Settings**

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

Mesh Monitor Duration  
 Duration in minutes (5-60)

Mesh Recovery Interval  
 Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30)

## Mesh Base

WLANs > Ent\_Mesh\_Base

Configuration Devices

**WLAN**

AAA Servers

Guest Access

Access Control

Enable

SSID\*  
CAMBIUM\_MESH\_BASE The SSID of this WLAN (up to 32 characters)

Mesh  
Base Mesh Base/Client/Recovery mode

VLAN\*  
10 Default VLAN assigned to clients on this WLAN (1-4094)

Security  
WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase\*  
..... Show WPA2 Pre-shared security passphrase or key

Band  
 2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

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

Hide SSID Do not broadcast SSID in beacons

Mesh Vlan Tagging Enable the vlan tagging over mesh link

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

Mesh Multi Hop  
Enable/Disable the multi-hop mesh link support. This configuration will be used if and only if mesh auto detect backhaul feature is enabled.

AP Groups > Ent\_Mesh\_ZeroTouch\_APGrp

Dashboard Notifications Configuration Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

**User-Defined Overrides**

**User-Defined Overrides**

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

**Variables and Macros**

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 7
mesh client
band 5 ghz
fast-roaming 802.11r
mesh-auto-detect-backhaul monitor-host
!
```

### 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 Multi-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 74: Multi-Hop deployment Scenario



## cnMaestro configuration:

WLANs > Ent\_Mesh\_Base

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

SSID

Enable

SSID\*  
CAMBIUM\_MESH\_BASE The SSID of this WLAN (up to 32 characters)

Mesh

Base Mesh Base/Client/Recovery mode

VLAN\*  
10 Default VLAN assigned to clients on this WLAN (1-4094)

Security

WPA2 Pre-Shared Keys Set authentication and encryption type

Passphrase\*  
..... Show WPA2 Pre-shared security passphrase or key

Band

2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Client Isolation

Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

Hide SSID Do not broadcast SSID in beacons

Mesh Vlan Tagging Enable the vlan tagging over mesh link

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

Mesh Multi Hop  
Enable/Disable the multi-hop mesh link support. This configuration will be used if and only if mesh auto detect backhaul feature is enabled.

## 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 System 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:

AP Groups > Ent\_Mesh\_ZeroTouch\_APGrp

Dashboard Notifications **Configuration** Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

**User-Defined Overrides**

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

**Variables and Macros**

ⓘ Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```
!
wireless wlan 7
mesh base
fast-roaming 802.11r
!
```

### 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 57: 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:

AP Groups > Ent\_Mesh\_ZeroTouch\_APGrp

Dashboard Notifications **Configuration** Statistics Devices Clients Mesh Peers

Basic

Management

Radio

Network

Security

Services

**User-Defined Overrides**

Advanced configuration settings entered below will be applied on top of the AP Group settings sent to the device. This allows you to apply configuration not supported in the previous screens. If there are conflicts, the below settings will take precedence. The format used is the same as a configuration file exported from the device via its web UI or the "View Device Configuration" link in the device level configuration page.

**Variables and Macros**

Settings entered are not validated or error-checked (However, dollar (\$), period (.) or space characters are not allowed in a variable name and it should not be more than 64 characters long), and they may overwrite configuration made in previous screens, so please use them with caution. You are responsible for ensuring the resulting AP Group is valid and safe to use.

```

!
wireless radio 2
mesh-client-bgscan
mesh-client-bgscan channel-list all-channels
mesh-client-bgscan roaming-rssi-threshold -65
mesh-client-boscan long-interval 300
!
wireless wlan 1
mesh client
band 5 ghz
fast-roaming 802.11r
!

```

### 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:

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

#### cnMaestro configuration:

WLANs > Ent\_Mesh\_Base

Configuration Devices

**WLAN**

AAA Servers

Guest Access

Access Control

**SSID**

Enable

SSID\*  The SSID of this WLAN (up to 32 characters)

**Mesh**

Base  Mesh Base/Client/Recovery mode

**VLAN\***

Default VLAN assigned to clients on this WLAN (1-4094)

**Security**

WPA2 Pre-Shared Keys  Set authentication and encryption type

Passphrase\*   WPA2 Pre-shared security passphrase or key

**Band**

2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

**Client Isolation**

Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

Hide SSID Do not broadcast SSID in beacons

Mesh Vlan Tagging Enable the vlan tagging over mesh link

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

### 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:

WLANs > Ent\_Mesh\_Recovery

Configuration Devices

**WLAN**

Access Control

**Basic Information**

Type\*  
Enterprise Wi-Fi

Name\*  
Ent\_Mesh\_Recovery

Description

**Basic Settings**

SSID

Enable

Mesh

Recovery Mesh Base/Client/Recovery mode

VLAN\*  
1 Default VLAN assigned to clients on this WLAN (1-4094)

Transition SSID  
Configure the matching open/owe transition SSID

Band

2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

**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:**



WLANs > Ent\_Mesh\_Client

Configuration Devices

WLAN

**Basic Settings**

SSID  
 Enable  
 SSID\*  
 The SSID of this WLAN (up to 32 characters)

Mesh  
 Mesh Base/Client/Recovery mode

VLAN\*  
 Default VLAN assigned to clients on this WLAN (1-4094)

Security  
 Set authentication and encryption type

Passphrase\*  
  WPA2 Pre-shared security passphrase or key

Band  
 2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Mesh Vlan Tagging Enable the vlan tagging over mesh link

**Advanced Settings**

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

Mesh Monitor Duration  
 Duration in minutes (5-60)

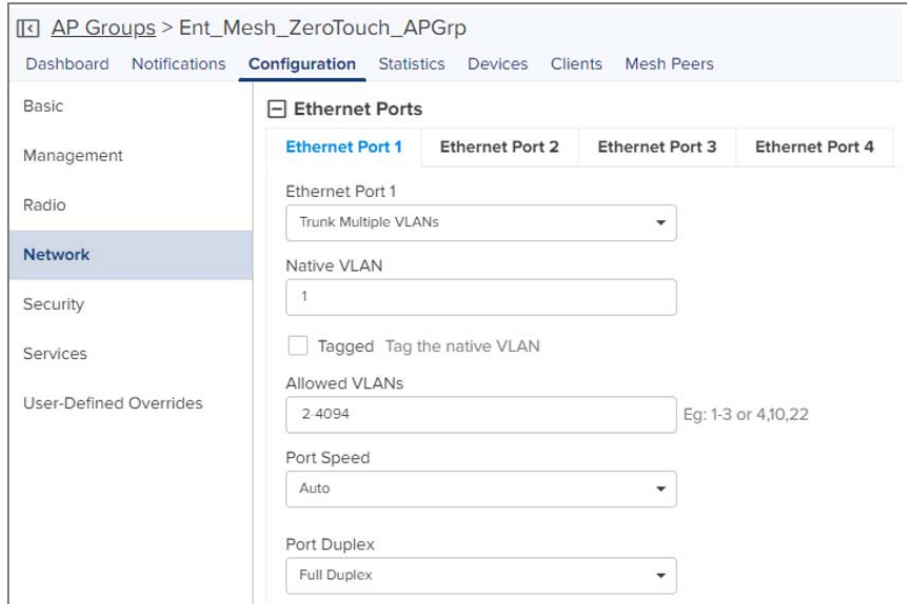
Mesh Recovery Interval  
 Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30)

**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
```

- 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:**

WLANs > Ent\_Mesh\_Base

Configuration Devices

**WLAN**

AAA Servers

Guest Access

Access Control

**Basic Settings**

**SSID**

Enable

SSID\*  The SSID of this WLAN (up to 32 characters)

**Mesh**

Base  Mesh Base/Client/Recovery mode

**VLAN\***

Default VLAN assigned to clients on this WLAN (1-4094)

**Security**

WPA2 Pre-Shared Keys  Set authentication and encryption type

**Passphrase\***

WPA2 Pre-shared security passphrase or key

**Band**

2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

**Client Isolation**

Disable

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

Hide SSID Do not broadcast SSID in beacons

Mesh Vlan Tagging Enable the vlan tagging over mesh link

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

### 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:

WLANs > Ent\_Mesh\_Recovery

Configuration Devices

**WLAN**

Access Control

**Basic Information**

Type\*  
Enterprise Wi-Fi

Name\*  
Ent\_Mesh\_Recovery

Description

**Basic Settings**

SSID

Enable

Mesh  
Recovery Mesh Base/Client/Recovery mode

VLAN\*  
10 Default VLAN assigned to clients on this WLAN (1-4094)

Transition SSID  
Configure the matching open/owe transition SSID

Band  
 2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

**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:**

WLANs > Ent\_Mesh\_Client

Configuration Devices

**WLAN**

**Basic Settings**

SSID  
 Enable  
 SSID\*  
 The SSID of this WLAN (up to 32 characters)

Mesh  
 Mesh Base/Client/Recovery mode

VLAN\*  
 Default VLAN assigned to clients on this WLAN (1-4094)

Security  
 Set authentication and encryption type

Passphrase\*  
  WPA2 Pre-shared security passphrase or key

Band  
 2.4 GHz  5 GHz  6 GHz Define radio types (2.4 GHz, 5 GHz, 6 GHz) on which this WLAN should be supported

Mesh Vlan Tagging Enable the vlan tagging over mesh link

**Advanced Settings**

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

Mesh Monitor Duration  
 Duration in minutes (5-60)

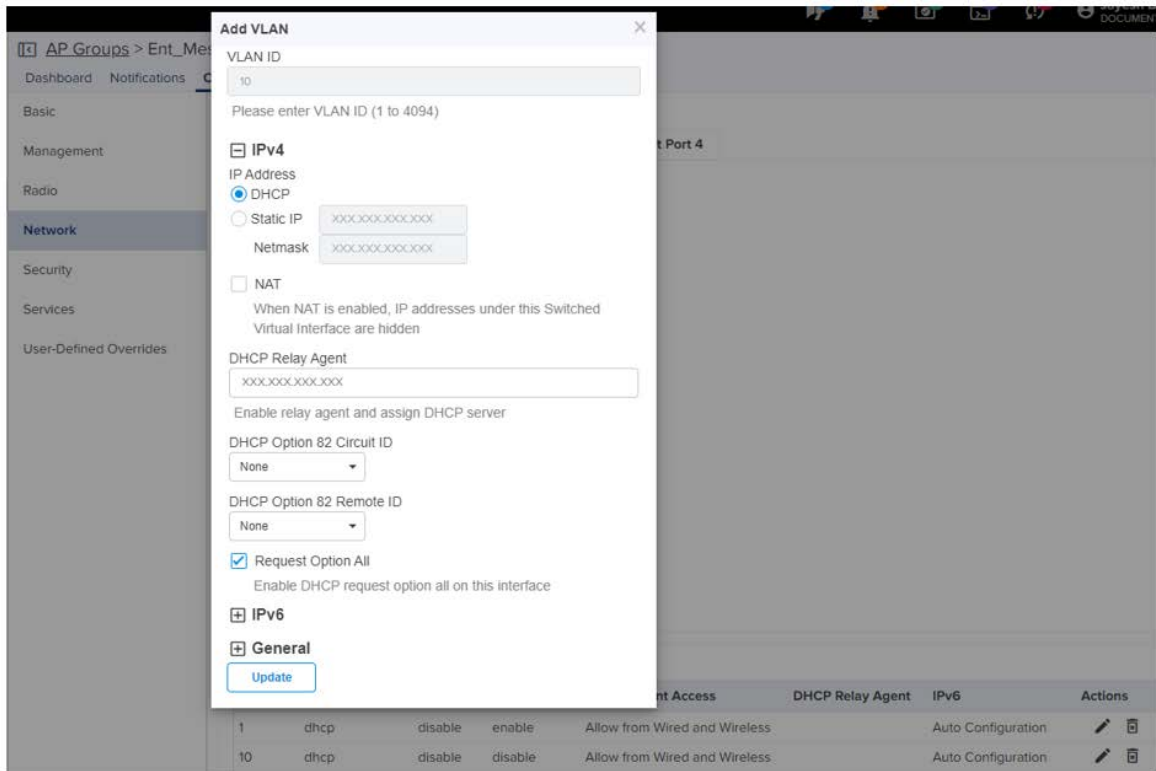
Mesh Recovery Interval  
 Interval in minutes after which a full recovery is attempted if the mesh base is not reachable (5-30)

**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

# Chapter 15: 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.

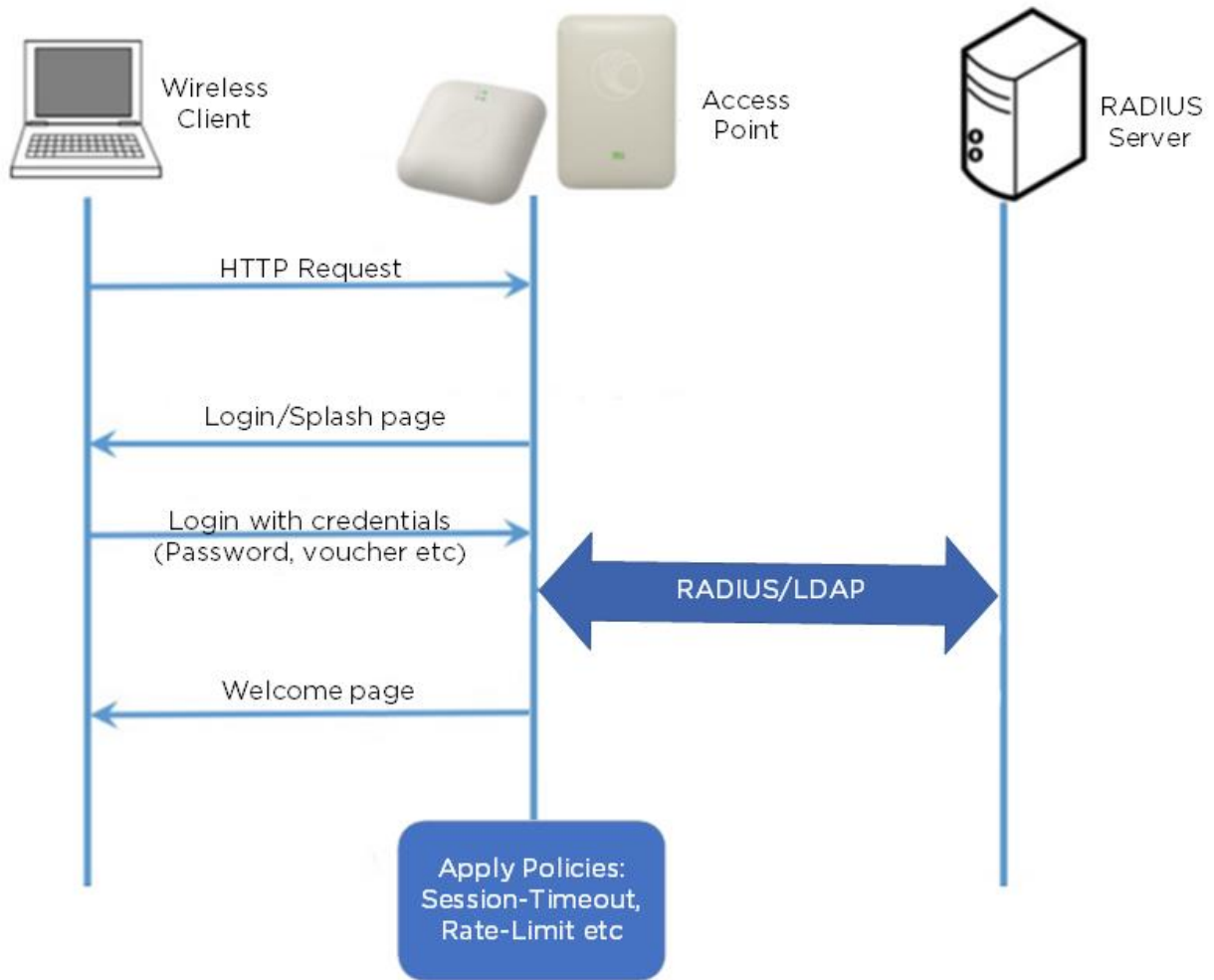
Modes of Captive Portal Services supported by Enterprise Wi-Fi AP devices:

- **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. More details on this Guest Access Portal method are described in [Chapter 15](#).
- **cnMaestro:** Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login, and Paid login are supported. More details on this Guest Access Portal method are described in [Chapter 16](#).
- **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 75: Topology



## Configurable parameters

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

Figure 76: Guest Access Internal Access Point parameter

The screenshot shows a configuration page for Guest Access with several tabs: Basic, Radius Server, Guest Access (selected), Usage Limits, Scheduled Access, Access, Passpoint, and Delete. The 'Guest Access' tab is active, displaying various settings:

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

At the bottom, there are 'Save' and 'Cancel' buttons.

## 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 77: Success action



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

## 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 78: Redirect



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

## Redirect Mode

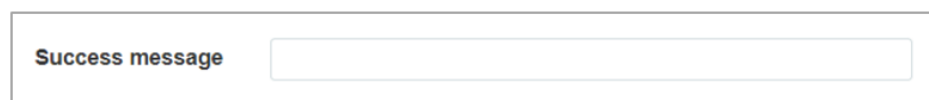
There are two redirect modes available:

- **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 79: Success Message



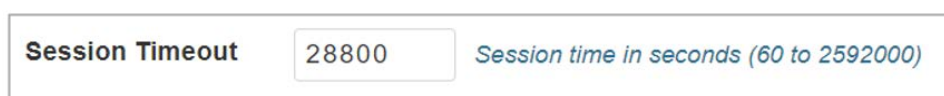
Success message

## Timeout

### Session

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

Figure 80: Session timeout



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

## Inactivity

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

Figure 81: *Inactivity timeout*

<b>Inactivity Timeout</b>	<input type="text" value="1800"/>	<i>Inactivity time in seconds (60 to 2592000)</i>
---------------------------	-----------------------------------	---

## 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

Basic | Radius Server | **Guest Access** | Usage Limits | Scheduled Access | Access | Passpoint | Delete

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  onMaestro  XMS/Easypass

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

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

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

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

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

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

**Logo**   
Logo to be displayed on the splash page

**Background Image**   
Background image to be displayed on the splash page

**Success Action**  Internal Logout Page  Redirect user to External URL  Redirect user to Original URL

**Success message**

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

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

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

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

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

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

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

---

**White List** | Captive Portal Bypass User Agent

**IP Address or Domain Name**

IP Address   Domain Name	Action
No white list available	

1 / 1 10 items per page

Figure 82: Authentication – redirected splash page

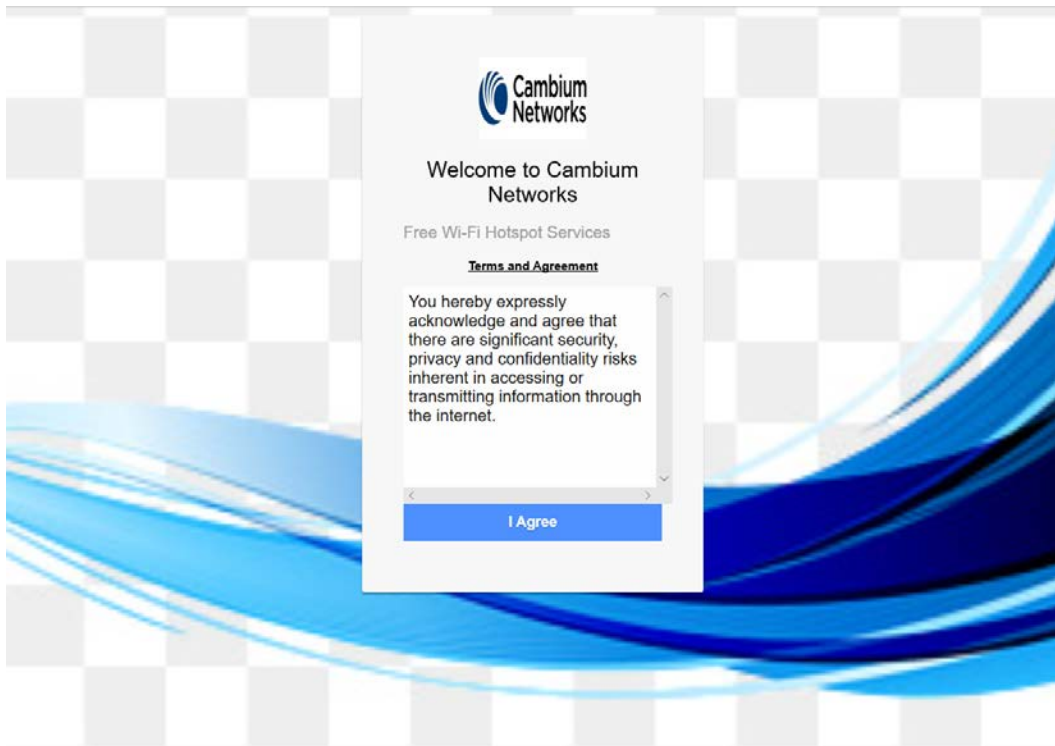
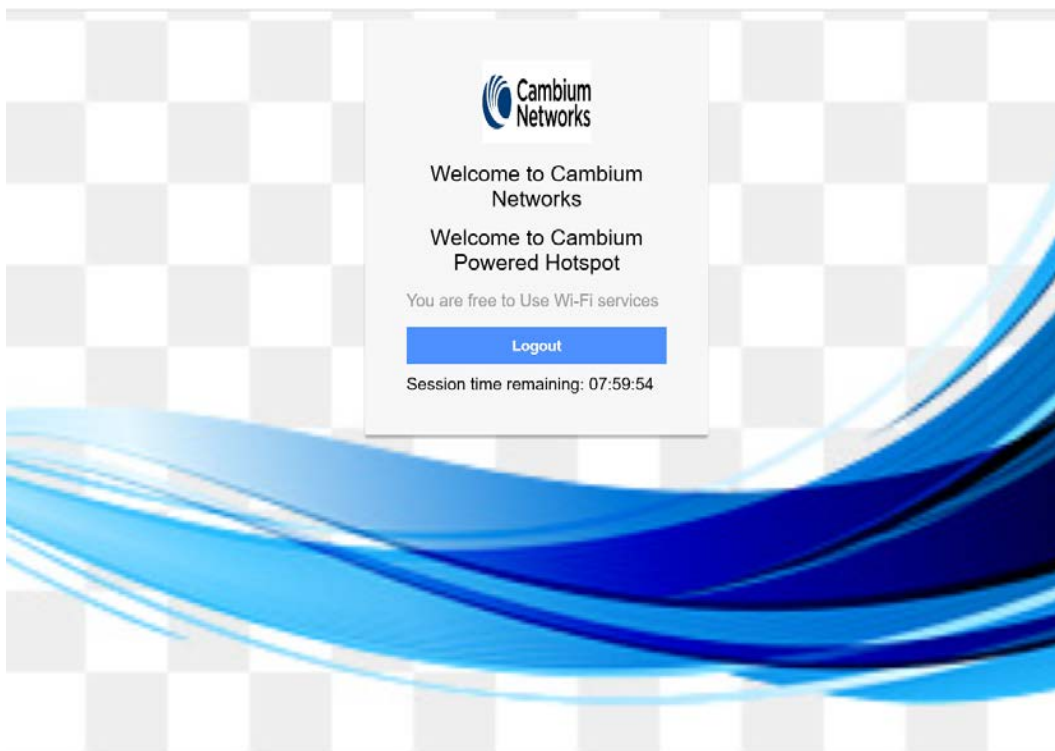


Figure 83: Successful login – redirected splash page



# Chapter 16: 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/](https://www.cambiumnetworks.com/wifi_partners/).

## Configurable parameters

Figure 84 displays multiple configurable parameters supported for External Guest Access hosted on AP.



Figure 84: External Access Point parameter

The screenshot displays the configuration interface for the Guest Access feature. The 'Guest Access' tab is active, and the 'External Hotspot' option under Portal Mode is selected. The configuration includes sections for enabling the feature, setting portal and access policies, defining redirect modes and hostnames, and configuring WISPr clients. It also allows for customizing success messages, redirection query strings, and session timeouts. A 'White List' section at the bottom shows a table with columns for IP Address/Domain Name and Action, currently containing no entries.

**Basic** | **Radius Server** | **Guest Access** | Usage Limits | Scheduled Access | Access | Passpoint | Delete

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  cnMaestro  XMS/Easypass

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

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

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

**WISPr Clients External Server Login**

**External Page URL**   
*URL of external splash page*

**External Portal Post Through cnMaestro**

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

**Success Action**  Internal Logout Page  Redirect user to External URL  Redirect user to Original URL

**Success message**

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

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

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

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

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

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

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

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

**White List** | Captive Portal Bypass User Agent

**IP Address or Domain Name**

IP Address   Domain Name	Action
No white list available	

/ 1  Items per page

## 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.

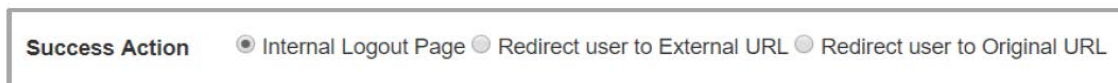
- Redirect users to external URL

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 85: 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 86: Redirect



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

## 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 87: Success Message



**Success message**

## Timeout

### Session

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

Figure 88: Session timeout



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

### Inactivity

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

Figure 89: Inactivity timeout



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

## 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

Basic | Radius Server | **Guest Access** | Usage Limits | Scheduled Access | Access | Passpoint | Delete

**Enable**

**Portal Mode**  Internal Access Point  External Hotspot  cnMaestro  XMS/Easypass

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

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

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

**WISPr Clients External Server Login**

**External Page URL**   
*URL of external splash page*

**External Portal Post Through cnMaestro**

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

**Success Action**  Internal Logout Page  Redirect user to External URL  Redirect user to Original URL

**Success message**

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

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

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

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

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

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

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

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

---

**White List** | Captive Portal Bypass User Agent

**IP Address or Domain Name**

IP Address   Domain Name	Action
No white list available	

1 / 1 10 items per page

Figure 90: Authentication – redirected splash page

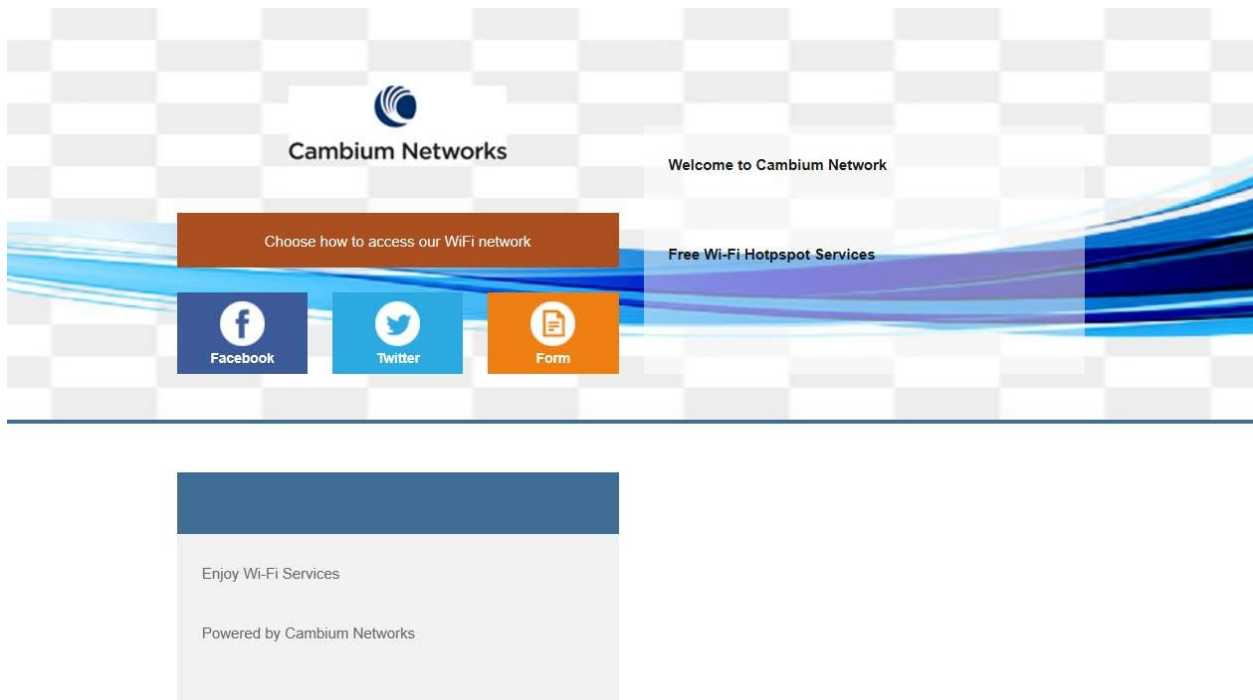
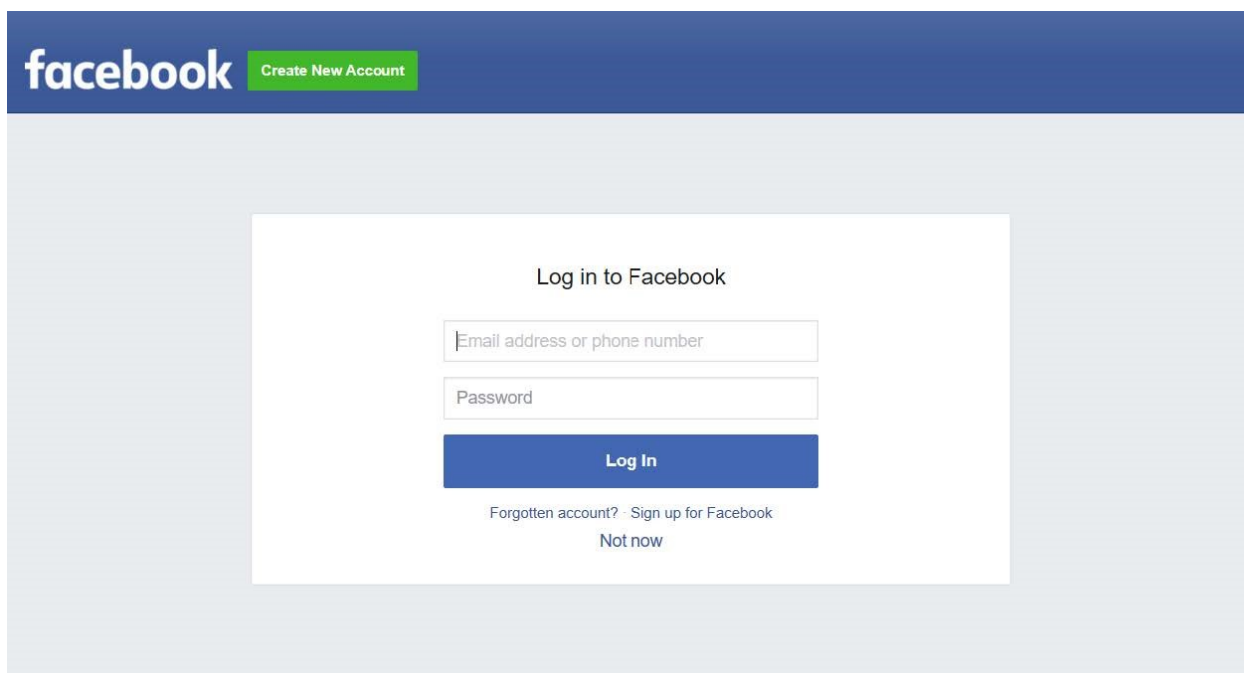


Figure 91: Successful Login – redirected splash page



# Chapter 17: 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 18: 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 58: 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 19: Device Recovery Methods

## Factory reset via 'RESET' button

Table 59: 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
XV2-2T	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
e410	Press and hold the Reset button for 25 seconds	LED will be OFF and turned onto Amber
e510	Press and hold the Reset button for 20 seconds	Both LEDs will be OFF and turned onto Amber
e430	Press and hold the Reset button for 25 seconds	LED will be OFF and turned onto Amber
e600	Press and hold the Reset button for 20 seconds	LED will be OFF and turned onto Amber
e700	Press and hold the Reset button for 25 seconds	Both LEDs will be OFF and turned onto Amber

## Boot partition change via power cycle

Table 60: 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)
XV2-2T	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)
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)
e410	Follow power ON and off 9 times with an interval of 15 Sec (ON) and 5 Sec (OFF)
e510	Follow power ON and off 9 times with an interval of 15 Sec (ON) and 5 Sec (OFF)
e430	Follow power ON and off 9 times with an interval of 15 Sec (ON) and 5 Sec (OFF)
e600	Follow power ON and off 9 times with an interval of 7 Sec (ON) and 5 Sec (OFF)
e700	Follow power ON and off 9 times with an interval of 15 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 20: 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 61: Show commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
<b>Deep Packet Inspection (DPI)</b>		
1	<code>show application-statistics by-application</code>	Provides statistics of each application that are accessed by the station connected to the AP.
2	<code>show application-statistics by-category</code>	Provides statistics of application category that are accessed by the station connected to the AP.
<b>Network Information</b>		
3	<code>show arp</code>	Displays list of ARP entries learned by AP
4	<code>show conntrack</code>	Displays current connection track entries along with application ID Mapping.
5	<code>show route</code>	Displays IP route information
6	<code>show dhcp-pool &lt;Index number&gt;</code>	Displays the DHCP pool configuration
7	<code>show interface brief</code>	Displays interface details such as IP, Netmask, and traffic statistics.
8	<code>show ip dhcp-client-info</code>	Displays the DHCP options learned by device across all interfaces.
9	<code>show ip domain-name</code>	Displays learned domain name information
10	<code>show ip gw-source-precedence</code>	Displays the Precedence of gateway sources
11	<code>show ip interface</code>	Displays IP interface parameters
12	<code>show ip name-server</code>	Displays DNS server information
13	<code>show ip neighbour</code>	Displays IPv4 neighbour entries
14	<code>show ip route</code>	Displays IP route information
15	<code>show ipv6 dhcp-client-info</code>	Displays learned DHCPv6 client information
16	<code>show ipv6 domain-name</code>	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
<b>Radio Information</b>		
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 <b>mesh-xtnded-dev-list</b> 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
<b>Bonjour Information</b>		
41	show bonjour-services	Displays Bonjour services available
42	show bonjour-statistics	Displays Bonjour rule statistics
<b>System Information</b>		
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
<b>Guest Access</b>		
59	show ext-guest clients	Displays information of ext-guest clients
<b>Filters</b>		
60	show filter-statistics	Displays filter statistics
<b>LLDP</b>		
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
<b>Real-Time Location System</b>		
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
<b>Tunnel</b>		
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 62: 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

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

## Service system

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

Table 63: Service system commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
1	<code>service boot backup- firmware</code>	Helps to boot to other partition
2	<code>service clear-cores</code>	Clear system core files (if any)

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



## 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

---

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

Table 64: 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	
7	WISPr-Bandwidth-Max-Up	integer	No	No	Yes	No	No	No	Yes	
8	WISPr-Bandwidth-Max-Down	integer	No	No	Yes	No	No	No	Yes	
9	WISPr-Session-Terminate-Time	string	No	No	Yes	No	No	No	Yes	

Table 65 lists the WISPr VSAs supported on Enterprise Wi-Fi APs with CoA support.

Table 65: 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 66 lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs.

Table 66: 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	string	Yes	-NA-	No				-NA-	Yes
161.2	Cambium-ePSK-M2	string	Yes	-NA-	No				-NA-	Yes
161.3	Cambium-ePSK-BSSID	string	Yes	-NA-	No				-NA-	Yes
161.4	Cambium-ePSK-AP-MAC	string	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 67 lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs with CoA.

Table 67: 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	string	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	string	Yes	-NA-	No				-NA-	-NA-
161.3	Cambium-ePSK-BSSID	string	Yes	-NA-	No				-NA-	-NA-
161.4	Cambium-ePSK-AP-MAC	string	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 68 lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs.

Table 68: 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 69 lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs with CoA support.

Table 69: 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 70 lists the RADIUS attributes supported in authentication and accounting packets with WPA2-Enterprise security.

Table 70: 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 71 lists the supported CoA messages.

Table 71: CoA messages

CoA Message	Supported By MAB (Wired Clients)
Disconnect client	Yes
Update VLAN	Yes
Session Timeout	No
Accounting Interval	Yes
Quota Limit	No

## Supported DFS channels

Table 72 lists the DFS channel support for various platforms in conformance with FCC standards.

Table 72: 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 73 lists the DFS channel support for various platforms in conformance with IC standards.

Table 73: 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 74 lists the DFS channel support for various platforms in conformance with CE standards.

Table 74: 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

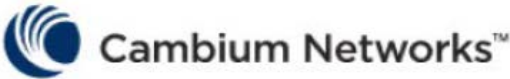
AP Model	5250-5350 MHz (U-NII-2A)	5470-5725 MHz (U-NII-2C)	5725-5850 MHz (U-NII-3)
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes
XE3-4	Yes	Yes	Yes
XE5-8	Yes	Yes	Yes
XV2-2	Yes	Yes	No
XV3-8	No	Yes	No
XV2-2T0	Yes	Yes	Yes
XV2-2T1	Yes	Yes	Yes

# 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	<a href="https://support.cambiumnetworks.com">https://support.cambiumnetworks.com</a>
Support enquiries	
Technical training	<a href="https://learning.cambiumnetworks.com/learn">https://learning.cambiumnetworks.com/learn</a>
Main website	<a href="http://www.cambiumnetworks.com">http://www.cambiumnetworks.com</a>
Sales enquiries	<a href="mailto:solutions@cambiumnetworks.com">solutions@cambiumnetworks.com</a>
Warranty	<a href="https://www.cambiumnetworks.com/support/standard-warranty/">https://www.cambiumnetworks.com/support/standard-warranty/</a>
Telephone number list	<a href="http://www.cambiumnetworks.com/contact-us/">http://www.cambiumnetworks.com/contact-us/</a>
User Guides	<a href="http://www.cambiumnetworks.com/guides">http://www.cambiumnetworks.com/guides</a>
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



[www.cambiumnetworks.com](http://www.cambiumnetworks.com)

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

Copyright © 2023 Cambium Networks, Ltd. All rights reserved.