



USER GUIDE

Enterprise Wi-Fi Access Point

Release 7.1



Reservation of Rights

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

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

Contents

Contents	3
About This User Guide	12
Overview of Enterprise Wi-Fi AP products	12
Intended audience	12
Purpose	12
Feedback	12
Important regulatory information	13
Complying with rules for the country of operation	13
Related documents	14
Existing hardware platforms	15
Premium feature list	15
Quick Start – Device Access	17
Powering up the device	17
PoE switches (802.3af/802.3at/802.3bt)	17
PoE adapter	18
DC power supply	19
Accessing the device	19
Device access using default or fallback IP	19
Device access using zeroconf IP	21
Device access using DHCP IP address	22
LED status	22
Onboarding the Device	24
Overview	24
Device onboarding and provisioning	24
cnMaestro	24
XMS-Cloud	25

Configuring the System	26
Basic	26
Power over Ethernet (PoE) in	28
Power over Ethernet (PoE) Out port	30
Link Layer Discovery Protocol (LLDP)	30
Management	32
Administrator Access	32
HTTPS Proxy server configuration	34
Time settings	34
Event logging	35
SNMP	36
Configuring the Radio	38
Overview	38
Configuring Radio parameters	38
Basic	38
Software-Defined Radio (SDR) capabilities	46
Enhanced Roaming	46
BSS Coloring	47
Target Wake Time (TWT)	47
Receive sensitivity configuration	47
Multicast-snooping and Multicast-to-Unicast conversion	47
Boot loop detection	48
Auto-RF	49
Overview	49
Dynamic Channel	49
Dynamic Power	50
Auto-RF behavior on device turn on	50
Auto-RF Rx Sensitivity	51

Configuring Dynamic Channel	51
Configuring Dynamic Power	53
Radio Configuration	54
Configuring the Wireless LAN	56
Overview	56
Configuring the WLAN parameters	56
Basic	57
WLAN VLAN allowed list	71
ICMPv6 Router advertisement (RA) unicast conversion	71
802.11k/v	71
RADIUS server	72
Guest Access	76
Usage Limits	88
Scheduled Access	89
Access	91
Passpoint	94
RADIUS attributes	96
Enterprise PSK (ePSK)	98
Configuring ePSKs	98
ePSK registration for WPA3 clients	101
Creating a Personal Wi-Fi ePSK	109
RADIUS-based ePSK Premium feature	110
Configuring RADIUS-based ePSK	110
Groupwise Transient Key (GTK) per VLAN	112
Dynamic ARP Inspection	112
Configuring the Network	113
Overview	113
Configuring Network parameters	113

IPv4 network parameters	113
Routes	119
IPv6 network parameters	120
General network parameters	123
Ethernet Ports	124
DHCP	127
Tunnel	128
Point-to-Point Protocol over Ethernet (PPPoE)	131
VLAN Pool	132
Configuring Access Control	134
Enabling Access Control Policy	134
User Group Policy	135
Device Policy	136
Managing Filters	138
Overview	138
Filter list	138
Filters	138
Configuring filter CLI	139
Device class filter	143
Wi-Fi Calling support	144
Air cleaner	144
Application control Premium feature	146
Deep Packet Inspection (DPI)	147
Custom Applications X	160
WIDS/WIPSPremium feature	163
Wireless Intrusion Detection Systems (WIDS)	163
Wireless flood detection	163
Neighbor AP detection	164

Rogue APs	164
Honeyapot APs	164
Ad Hoc network detection	164
Wired Devices	165
Configuring WIDS	165
Wireless Intrusion Prevention System (WIPS)	166
Configuring Services	167
Overview	167
Configuring services	167
Lightweight Directory Access Protocol (LDAP)	167
NAT Logging	168
User Groups Premium feature	170
Real-Time Location System (RTLS)	171
Speed Test	175
DHCP Option-82	176
Bonjour Gateway	177
Link Aggregation Control Protocol (LACP)	179
Operations	181
Overview	181
Firmware upgrade	181
System	182
LED Test flashing pattern	183
Troubleshoot	184
Status	184
Downloading tech support file	185
Logging	185
Debug Logs	185
Radio Frequency (RF)	186

Wi-Fi Analyzer	186
Packet capture	188
Performance	190
Network Connectivity	190
Remote CLI	192
Flash LEDs	193
XIRCON tool support	193
XIRCON tool support for Linux 1.0.0.40	194
Management Access	195
Local authentication	195
Device configuration	195
SSH Key authentication	195
Device configuration	195
SSH Key generation	196
RADIUS authentication	198
Device configuration	199
Mesh	200
Deployment scenarios	200
Mesh configurable parameters	202
Order of Mesh profile configuration	204
Mesh Auto Detect Backhaul	211
Scenario 1	211
Scenario 2	212
Scenario 3	212
Mesh Muti-Hop	215
Mesh Roaming	216
Mesh Base configuration	216
Mesh Client configuration	217

Mesh link-Sample configuration	218
VLAN 1 as the management interface	218
Non-VLAN 1 as the management interface	222
Typical use-cases	226
Additional mesh topology supported	227
Guest Access Portal - Internal	228
Introduction	228
Configurable parameters	229
Access policy	230
Splash page	230
Redirect parameters	231
Success message	232
Timeout	232
Whitelist	232
Configuration examples	232
Guest Access Portal - External	234
Introduction	234
Configurable parameters	234
Access policy	235
WISPr	235
External portal post through cnMaestro	235
External portal type	235
Redirect parameters	235
Success message	236
Timeout	236
Whitelist	236
Configuration examples	236
Guest Access – cnMaestro	238

Auto VLAN	239
Device Recovery Methods	240
Factory reset via 'RESET' button	240
Boot partition change via power cycle	240
Disable factory Reset Button	240
Command-Line Interface (CLI)	241
Show commands	241
Service commands	244
Service show	244
Service system	245
cnMaestro X Assurance	247
MarketApps	248
Target audience	248
Benefits	248
Glossary	249
Appendix	251
Supported RADIUS Attributes	252
WISPr VSAs (Vendor ID: 14122)	252
Cambium VSAs (Vendor ID: 17713)	253
Standard RADIUS attributes	255
RADIUS attributes in authentication and accounting packets with WPA2-Enterprise security	258
Supported CoA messages	261
Supported DFS channels	262
Priority order for parameters	263
Reasons for AP restarting	263
Best practices for wireless clients seamless roaming across APs	264
External network recommendations	264
AP WLAN profile configuration recommendations	265

AP group configuration recommendations	267
Cambium Networks	269

About This User Guide

This section describes the following topics:

- [Overview of Enterprise Wi-Fi AP products](#)
- [Intended audience](#)
- [Purpose](#)
- [Feedback](#)
- [Important regulatory information](#)
- [Related documents](#)
- [Existing 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 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.

Feedback

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

or completeness of our documents. To provide feedback, visit our support website:

<https://support.cambiumnetworks.com>.

Important regulatory information

Complying with rules for the country of operation

USA specific information



Caution

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation of the device.



Note

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

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

Canada specific information



Caution

This device complies with Innovation, Science and Economic Development Canada (ISED) license-exempt RSSs. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation of the device.

Renseignements spécifiques au Canada



Caution

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- l'appareil ne doit pas produire de brouillage, et
- l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Europe specific information

Cambium Networks Enterprise Wi-Fi AP products are compliant with applicable European Directives required for CE marking:

- 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC; Radio Equipment Directive (RED).
- 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS Directive).
- Cambium Networks complies with the European Regulation 2023/988 of 10 May 2023 on General Product Safety. EU Authorized Representative: Cambium Networks Europe B.V., Muiderstraat 1, 1011PZ Amsterdam, Netherlands. Contact Information: GPSR@cambiumnetworks.com.

Related documents

[Table 1](#) provides details of related documents for Enterprise Wi-Fi AP.

Table 1 Related documents

Document Name	Location
Enterprise Wi-Fi AP product details	https://www.cambiumnetworks.com/products/wifi/
Enterprise Wi-Fi AP Hardware and Installation Guide	https://support.cambiumnetworks.com/files
Enterprise Wi-Fi AP User Guide (This document)	https://support.cambiumnetworks.com/files
Enterprise Wi-Fi AP Release Notes	https://support.cambiumnetworks.com/files
Enterprise Wi-Fi AP Command-Line Interface Reference Guide	https://support.cambiumnetworks.com/files
Software Resources	https://support.cambiumnetworks.com/files
Community	http://community.cambiumnetworks.com/

Document Name	Location
Support	https://www.cambiumnetworks.com/support/contact-support/
Warranty	https://www.cambiumnetworks.com/support/warranty/
Feedback	support@cambiumnetworks.com

Existing hardware platforms

[Table 2](#) lists the existing hardware platforms in Enterprise Wi-Fi Access Points:

Table 2 Existing hardware platforms

Hardware Platform	Description	Supported Software Version
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	Release 6.5 and above
XV2-21X	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Indoor Wi-Fi 6 Access Point	Release 6.5 and above
XV2-23T	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Wi-Fi 6 Access Point	Release 6.5 and above

Premium feature list

Enterprise Wi-Fi AP firmware support certain advanced features that are available only through a paid subscription to cnMaestro X. These features are identified with the label **Premium feature** in the documentation. End users can also access these features without a management subscription on a free trial basis and for a limited time. As Cambium Networks releases new versions, restrictions will be enforced on the use of these premium features only in conjunction with a current cnMaestro X subscription. If the user does not have a current subscription at that time, the APs will stop enabling configurations, including these premium features.

Release 6.0 and later releases of Enterprise Wi-Fi AP firmware support certain advanced features that are available only through a paid subscription to cnMaestro X or XMS-Cloud management. These features are identified with the label **Premium feature** in the documentation. With Release 6.5 and later releases, end users can access these features without a management subscription on a free trial basis and for a limited time. As Cambium Networks releases new versions, restrictions will be enforced on the use of these premium features only in conjunction with a current cnMaestro X or XMS-Cloud subscription. If the user does not have a current subscription at that time, the APs will stop enabling configurations, including these premium features.

Table 3 Premium feature list

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

Quick Start – Device Access

This chapter describes the following topics:

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

Powering up the device

This section includes the following topics:

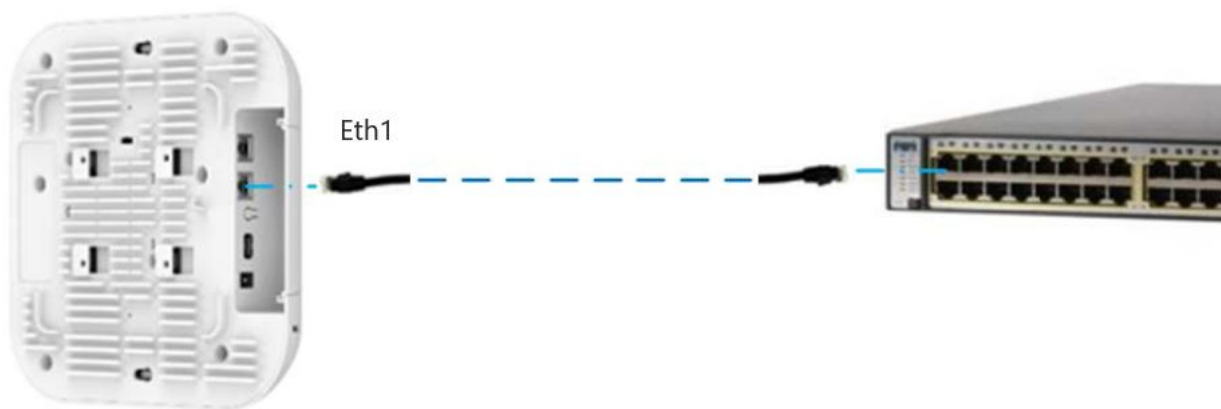
- [PoE switches \(802.3af/802.3at/802.3bt\)](#)
- [PoE adapter](#)
- [DC power supply](#)

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 to the related product datasheet to determine the options available.

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

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

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



[Table 4](#) provides detailed information on the AP modules that are enabled based on power negotiated via LLDP.

Table 4 Power management policy

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

PoE adapter

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

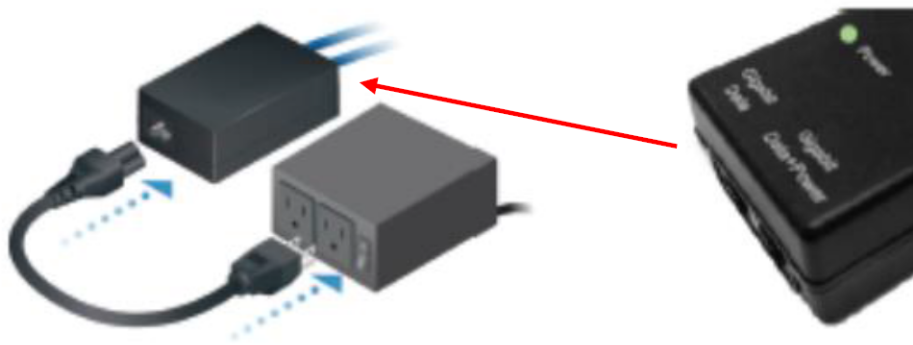
1. Connect the Ethernet cable from the Eth1/PoE-IN port of the device to the 5 Gigabit Data + Power port of the PoE adapter.
2. Connect an Ethernet cable from your LAN or computer to the 5 Gigabit Data port of the PoE adapter.

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



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

Figure 3 Connecting PoE adapter to a power outlet



DC power supply

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

Accessing the device

This section includes the following topics:

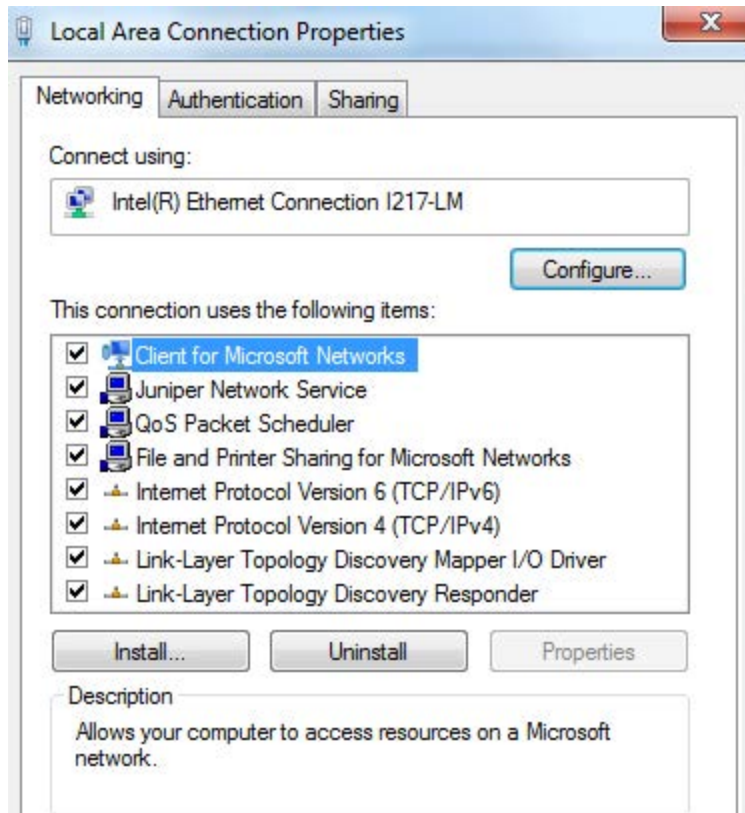
- [Device access using default or fallback IP](#)
- [Device access using zeroconf IP](#)
- [Device access using DHCP IP address](#)

Once the device is powered up, ensure it is operational by checking the LED status. The power LED on the AP should turn green, which indicates that the device is ready for access.

Device access using default or fallback IP

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

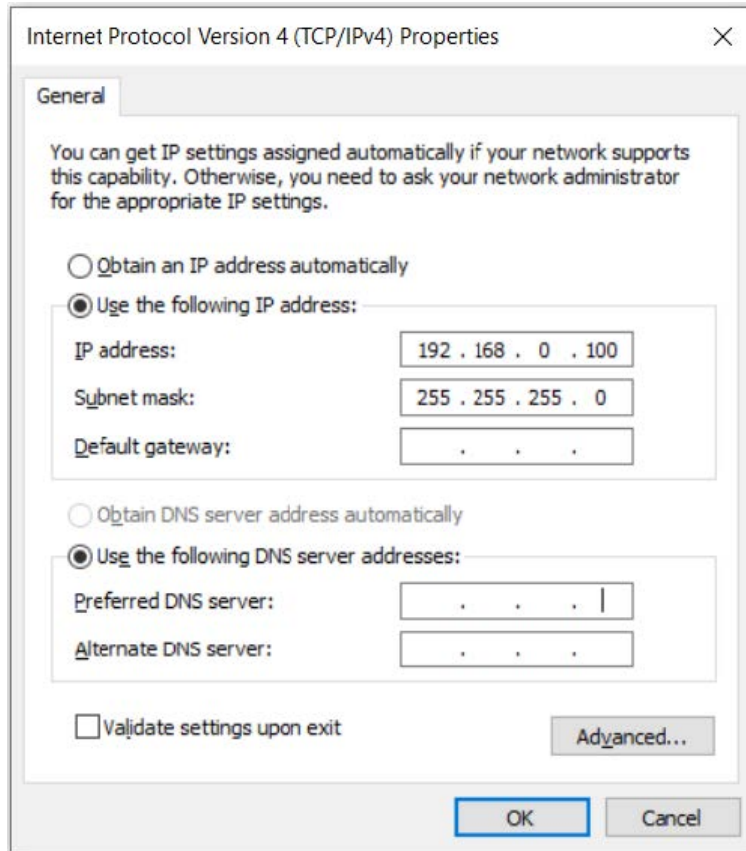
1. Open **Local Area Connection Properties** by performing one of the following steps:
 - In computers running Windows 7 operating system, go to **Control Panel > Network and Internet > Network Connections > Local Area Connection > Properties** (in the **Local Area Connection Status** window).
 - In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



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

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

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

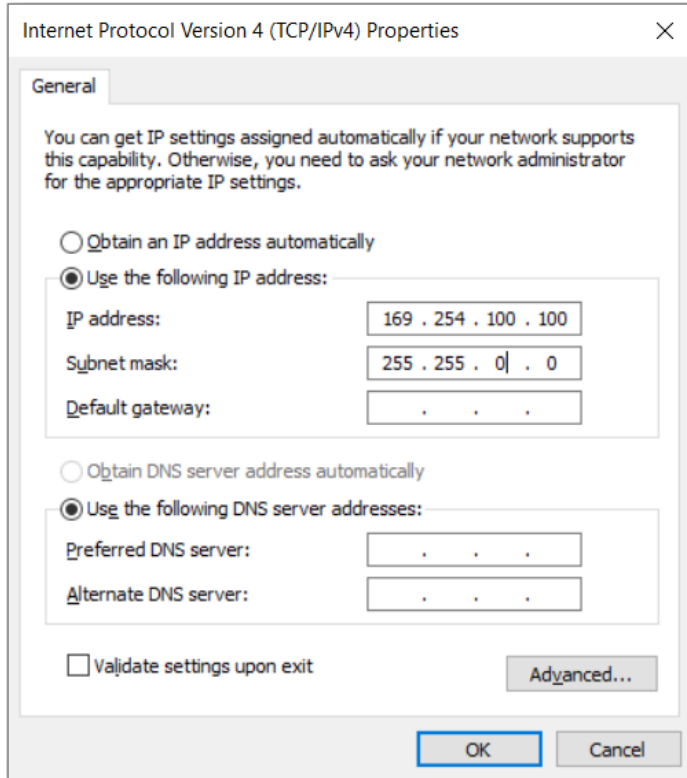


3. In the **Use the following IP address** section, ensure that an appropriate IP address and a subnet address are provided.
4. Click OK.
5. Ensure that your computer is set up to communicate with the required range of IP addresses.
6. Open a web browser and type the URL - <http://192.168.0.1> - to access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

Device access using zeroconf IP

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

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



3. Access the device UI using <http://169.254.170.187> with default credentials as below:

- Username: admin
- Password: admin

Device access using DHCP IP address

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

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

LED status

The Enterprise Wi-Fi AP features a single-color LED. The power LED glows amber when AP is turning on and turns green once the AP has successfully turned on. The network or status LED glows green if the connection to XMS or cnMaestro controller or manager is down. It turns blue once the AP is connected successfully to XMS or cnMaestro.

Table 5 Enterprise Wi-Fi AP LED status

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

Onboarding the Device

This chapter describes the following topics:

- [Overview](#)
- [Device Onboarding and Provisioning](#)

Overview

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

If you are using cnMaestro On-Premises, you must direct the devices to connect to the cnMaestro server using DHCP options or static URL configuration. For more information, refer to the *cnMaestro On-Premises User Guide*.

Device onboarding and provisioning

Enterprise Wi-Fi APs support the following onboarding methods:

- [cnMaestro](#)
- [XMS-Cloud](#)

cnMaestro

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

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

Supported devices and minimum version

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



Note

- The AP version is the minimum version required to manage the APs using cnMaestro Cloud, On-Premises, or XMS-Cloud.
- Similarly, the cnMaestro Cloud, On-Premises, and XMS-Cloud versions are the minimum versions required to manage the APs.



Warning

- Enterprise Wi-Fi 6 APs (XV series) running Release 7.1 cannot be downgraded to a version earlier than 6.6.1.

- Release 7.1 will not be available for Wi-Fi 6/6E APs in XMS-Cloud.

Table 6 Supported minimum AP and cnMaestro versions

AP Model	Supported Minimum AP Version			Supported Minimum cnMaestro / XMS-Cloud Version		
	cnMaestro Cloud	cnMaestro On-Premises	XMS-Cloud	cnMaestro Cloud	cnMaestro On-Premises	XMS-Cloud
XV2-22H	6.6.0.3	6.6.0.3	6.6.0.3	Current	3.1.1	Current
XV2-21X	6.6.0.3	6.6.0.3	NA	Current	3.1.1	NA
XV2-23T	6.6.0.3	6.6.0.3	NA	Current	3.1.1	NA

XMS-Cloud

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

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

Configuring the System

This chapter describes the following topics:

- [Basic](#)
- [Management](#)
- [Time settings](#)
- [Event Logging](#)
- [SNMP](#)

Basic

To configure the basic parameters for the AP, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.

By default, the **Basic** tab is displayed.



Note

- The following special characters are supported when creating the AP Group and WLAN passwords:

a-zA-Z_~*%#@!<>().[]^`\$1234567890.

- By default, the password is not configured.

You can also change the password after creating it.

[Table 7](#) lists the configurable parameters that are available in the **Basic** tab in the cnMaestro UI.

Table 7 Basic parameters

Parameter	Description	Range	Default
Name	Hostname of the device. Supported maximum length of the hostname: 64 characters	-	Enterprise Wi-Fi AP Model Number-Last 3 Bytes of ESN
Location	Location where the device is placed. Supported maximum length of location: 64 characters	-	-
Contact	Contact information for the device.	-	-
Country	Country of operation of the device.	-	-

Parameter	Description	Range	Default
	To be set by the administrator only. The allowed operating channels and the respective transmit power levels depend on the country of operation. The list of countries supported depends on the SKU of the device (FCC and ROW). Note: Radios remain disabled unless this parameter is configured.		
Placement	Enterprise Wi-Fi AP device supports both Indoor and Outdoor deployments. Based on deployment user can configure it as follows: • Indoor: Only indoor channels for configured country code will be available and operational. • Outdoor: Only outdoor channels for configured country code will be available and operational.	-	Indoor
PoE Output	Enable power over Ethernet to an auxiliary device connected to PoE OUT port.	-	Off
Dual 5 GHz radio	Enable Dual 5 GHz radio. This parameter provides the flexibility of splitting 8x8 5 GHz radio into two 4x4 5 GHz radios.	-	Disabled
LED	When enabled, turns on the device LEDs during operation.	-	Enabled
LLDP	Advertises device capabilities and information in the L2 network.	-	Enabled
Recommended Channel Distribution	Allows unique distribution of channels across radios when multiple radios are configured with same frequency band. Note: This option is available only as a CLI-based configuration. Use the <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 4 The AP Groups > Basic page

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Basic Information

Type
Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)

Name*

Scope
Shared Shared Scope means the AP Group is accessible to all Managed Accounts

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

Country* 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

☒ Recommended Channel Distribution
Disabling the recommended channel distribution allows any approved channel on any radio in APs with multiple 5/6GHz radios such as the XE3-4, XE3-4TN, and XE5-8. By default allowed channels are restricted to optimize the performance of multiple radios on the same band. Use this with advice from an RF planning expert. (applies to XE3-4, XE3-4TN and XE5-8 APs which have more than two 5/6 GHz radios)

WLAN

Add WLAN

Create WLAN

Order	WLAN
No WLAN Selected	

Save

Close

Power over Ethernet (PoE) in

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

request a specific amount of PoE power from the PS. This feature in the Enterprise Wi-Fi APs is called LLDP power request and it is enabled by default.

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



Caution

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

Table 8 PoE power requirements for APs

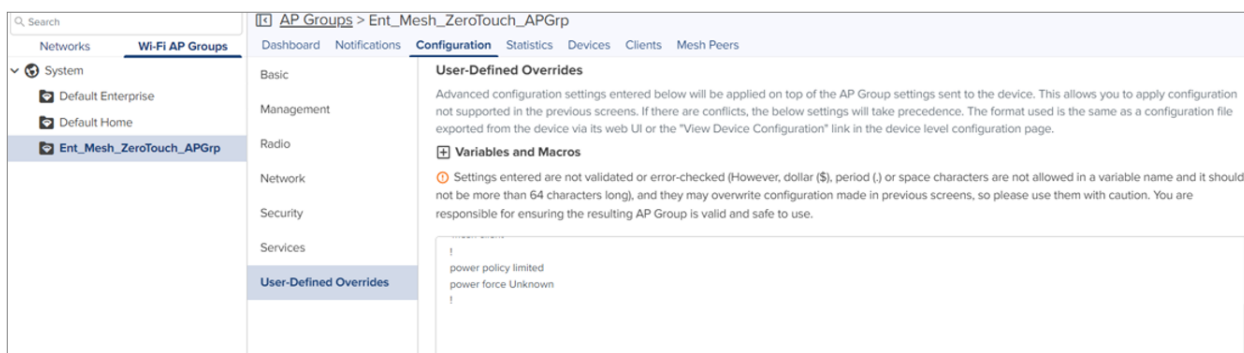
Device	PoE Out	Hardware Power Requirement	Maximum Power Draw (Watts)	Minimum Power Required to boot (Watts)
XV2-22H	Yes (Max 10W)	802.3af	22.95	8
XV2-21X	No	802.3af	12.95	8
XV2-23T	No	802.3af	12.95	8



Note

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

Figure 5 Power policy configuration



[Table 9](#) lists the Cambium PoE injectors and cnMatrix models supported on the APs.

Table 9 Supported Cambium PoE Injectors and cnMatrix models

AP Model	Cambium PoE Injector	cnMatrix Recommended Model
XV2-22H	N000000L142A / N000000L034B	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P

AP Model	Cambium PoE Injector	cnMatrix Recommended Model
XV2-21X	N000000L142A / N000000L034B / N000900L017A	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P
XV2-23T	N000000L142A / N000000L034B / N000900L017A	EX3028R-P / EX3052R-P / EX2016M-P / EX2052-P / EX2052R-P / EX2028-P / EX2010-P / EX1028-P / EX1010-P



Attention

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

Power over Ethernet (PoE) Out port

PoE out provision is provided to power on devices that are compatible with IEEE 802.3 af/at PoE IN as per power consumption or Cambium 30V POE as shown in the below table.

Table 10 PoE-out capabilities

AP Model	10W	48V @ 15W	48V @ 30W	30V @ 30W	Default State
----------	-----	-----------	-----------	-----------	---------------

Figure 6 PoE Output cnMaestro configuration

The screenshot shows the 'Configuration' tab for 'Ent_Mesh_ZeroTouch_APGrp'. Under the 'Basic' section, the 'PoE Output' dropdown is set to 'Off'. A search bar below it shows '802.3af' and 'cambium-poe' as suggestions. The 'Delete' button is visible at the bottom right of the configuration area.

Link Layer Discovery Protocol (LLDP)

LLDP is a Layer 2 network protocol used to share information, such as the device manufacturer, model, network capabilities, and IP address 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 the AP. This implies that the 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.

Power negotiation

LLDP discovers a device port (connected to a PoE PSE switch, for example) that supplies power to the AP. The AP checks that the port can supply the maximum power that is required by the AP model. The 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, the AP enables radios and other Model Specific peripherals (for example, USB port, Bluetooth).
- If the AP receives a power allocation that is less than the maximum but more than the minimum required to keep the radios operational, the AP issues a Syslog message and shuts down the other peripherals (for example, USB port, Bluetooth).
- If the AP receives less than the minimum power required for the radios to operate, the radios are shut down for five minutes. During this time, LLDP power negotiation continues to monitor the available power to ensure it meets the minimum requirement for the 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:

```
ap(config)# lldp
ap(config)#
```

To disable:

```
ap(config)# no lldp
ap(config)#
```

To list LLDP configuration:

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

Request power

To enable/disable power negotiation via LLDP:

```
ap(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)
ap(config)# lldp request-power
```

<ENTER>

```
ap(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.

```
ap(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)
```

```
ap(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.

```
ap(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)
```

```
ap(config)# lldp tx-interval
```

Specify LLDP transmit delay in sec (max 65535)

Management

Administrator Access

To configure Administrator access parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **Administrator Access** section.

[Table 11](#) lists configurable fields that are displayed in the **Administrator Access** section.

Table 11 Administrator Access parameters

Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	-	admin

Parameter	Description	Range	Default
Telnet	Enables Telnet access to the device CLI.	-	Disabled
SSH	Enables SSH access to the device CLI.	-	Enabled
SSH Key	Provision to login to device using SSH Keys. The user needs to add Public Key in this section. If configured, the user has to login to AP using Private Keys. This is applicable for both CLI and GUI.	-	Disabled
HTTP	Enables HTTP access to the device UI.	-	Enabled
HTTP Port	Provision to configure HTTP port number to access device UI.	1-65535	80
HTTPS	Enables HTTPS access to the device UI.	-	Enabled
HTTPS Port	Provision to configure HTTPS port number to access device UI.	1-65535	443
RADIUS Mgmt Auth	User has provision to control login to AP using RADIUS authentication. If enabled, every credential that is provided by the user undergo RADIUS authentication. If successful, allowed to login to UI of the device. This is applicable for both CLI and GUI.	-	Disabled
RADIUS Server	Provision to configure RADIUS IPv4 server for Management Authentication.	-	-
RADIUS Secret	Provision to configure RADIUS shared secret for Management authentication.	-	-

Figure 7 Administrator Access page

Administrator Access

Admin Password

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

Use SSH keys instead of password for authentication

☒ HTTP Enable HTTP access to the device GUI

HTTP Port

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

☒ HTTPS Enable HTTPS access to the device GUI

HTTPS Port

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

RADIUS server shared secret

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:

```
ap(config)# management proxy
https : Enable HTTPS proxy support
ap(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 (For example, `pool.ntp.org`). If NTP is not configured on the device, the device synchronizes the time with cnMaestro if onboarded.

To configure time parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **Time Settings** section.

[Table 11](#) lists configurable fields that are displayed in the **Time Settings** section.

Table 12 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. Note Accurate time on the AP is critical for features such as WLAN Scheduled Access and Syslogs.	-	-

Parameter	Description	Range	Default
NTP Server 1	Name or IPv4 address of Network Time Protocol server 1.	-	-
NTP Server 2	Name or IPv4 address of Network Time Protocol server 2.	-	-

Figure 8 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

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. 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.

To configure event logging, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **Event Logging** section.

[Table 13](#) lists configurable fields that are displayed in the **Event Logging** section.

Table 13 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 9 Event logging page

Event Logging

Syslog Server1

xxxxxxxxxxxx

514

Name or IPv4/IPv6 address of syslog server

Syslog Server2

xxxxxxxxxxxx

514

Syslog Severity

Debug (Level 7)

Specify severity of events forwarded to Syslog servers

SNMP

To configure SNMP, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Management** tab > **SNMP** section.

[Table 13](#) lists configurable fields that are displayed in the **SNMP** section.

Table 14 SNMP parameters

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



Note

The AP uses the AES-128 algorithm for encryption. It uses the SNMPv3 password configuration parameter for encryption and authentication.

Figure 10 *SNMP parameters*

 **SNMP**

☒ Enable Enable SNMP support on the device

SNMPv2c RO Community

SNMPv2c read-only community string (max 64 characters)

SNMPv2c RW Community

SNMPv2c read-write community string (max 64 characters)

Trap Receiver IP

SNMP trap server IP address

SNMPv3 Username

SNMPv3 user name (max 32 characters)

SNMPv3 Password

Show

SNMPv3 password (8 to 32 characters)

Authentication

☒ MD5 ☐ SHA

Access

☒ Read-Only ☐ Read-Write

Encryption

☒ On ☐ Off

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](#)
- [Boot loop detection](#)

Overview

Enterprise Wi-Fi AP devices support numerous configurable radio parameters to enhance the quality of service according to 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](#)
- [Software-Defined Radio \(SDR\) capabilities](#)
- [Enhanced Roaming](#)

Basic

To configure radio parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Radio** tab > **Basic** section.

[Table 15](#) lists the configurable fields that are displayed in the **Radio > Basic** section.

Table 15 Configure Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables the operation of radio.	-	Enabled
Band	Select the appropriate radio band, if the radio supports multiple bands.	-	-
Channel	Select the channel from the drop-down list. Channels in the drop-down list are populated based on the country configured.	Wi-Fi 6/6E APs • 2.4 GHz: 1 - 14 • 5 GHz: 36 - 173 • 6 GHz: 1 - 233	Auto
Channel Width	Specifies the channel widths for the operation. The following widths are supported: • For 2.4 GHz: Only 20 MHz channel width is supported. • For 5 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel widths are supported. • For 6 GHz: 20 MHz, 40 MHz, 80 MHz, 160 MHz, and 320 MHz channel widths are supported.	-	• 2.4 GHz: 20 MHz • 5 GHz: 40 MHz • 6 GHz: 80 MHz
Transmit Power	Total conducted transmit power, in decibel-milliwatt (dBm), of each radio based on coverage and SLA. The maximum transmit power of Enterprise Wi-Fi AP devices varies based on model number. Details of transmit power supported by each Enterprise Wi-Fi AP device are available at https://www.cambiumnetworks.com/products/wifi/ . Transmit power varies as per the country where the AP is deployed.. The default value is AUTO , which means radio transmit power is configured to the maximum as per the county configured.	• 2.4 GHz: 4 to 30 • 5 GHz: 4 to 30 • 6 GHz: 4 to 30	Auto

Parameter	Description	Range	Default
Beacon Interval	Specifies the time duration (in milliseconds) between two consecutive Beacons.	50ms - 3400ms.	100
Minimum Unicast rate	Specifies the coverage area of the Enterprise Wi-Fi AP device. The higher the rate selected, the lesser the range. You can configure this value based on the SLA in the deployment. The drop-down list contains all values advertised by Enterprise Wi-Fi AP devices, including legacy, HE, HT, and VHT rates.	Standard 802.11b and 802.11g data rates	1Mbps
Candidate Channels	Specifies selective channels based on user requirement. Options vary based on a band of operation and are as follows: • For 2.4 GHz: ◦ All ◦ Specific • For 5 GHz: ◦ All ◦ Specific ◦ Prefer Non-DFS ◦ Prefer DFS • For 6 GHz: ◦ All ◦ Specific	Wi-Fi 6/6E APs • 2.4 GHz: 1 - 14 • 5 GHz: 36 - 173 • 6 GHz: 1 - 233	All
Mode	All Enterprise Wi-Fi AP devices support either 802.11ax, 802.11ac Wave 1, or 802.11ac Wave 2, or 802.11be. Some legacy clients might not work as expected; therefore, this parameter can be tuned for backward compatibility based on wireless clients.  Note You can configure the <code>be</code> or <code>ax-be</code> radio mode by using the <code>mode</code> CLI command only:	Wi-Fi 6/6E APs • 2.4 GHz: b/g/n/ax • 5 GHz: a/n/ac/ax	All mode

Parameter	Description	Range	Default
	<pre>ap(config)# wireless radio <1-3> ap(config-radio-3)# mode be</pre>		
Short Guard Interval	Standard 802.11 parameter to increase the throughput of an Enterprise Wi-Fi AP device.	-	Enabled
Off Channel Scan (OCS)			
Enable	Provision to enable OCS on a device to capture neighbor clients and APs.	-	-
Dwell-time	Configure the time period to spend scanning of Wi-Fi devices on a channel.	50-300	50ms
Auto-RF (Dynamic Power)			
Enable	Enable or disable dynamic power management.	-	-
Mode	Select the required dynamic power modes. Two modes are supported: • By-Channel • By-Band	-	By-Channel
Minimum Transmit Power	The minimum transmit power that the AP can assign to radio when adjusting automatic cell sizes	5-15 dBm	8 dBm
Minimum Neighbour Threshold	The minimum number of neighbors to consider for power reduction by automatic cell logic.	1-10	2
Cellsize Overlap Threshold	Cell overlap will be allowed when the AP is determining automatic cell sizes.	0-100%	50%
Auto-RF (Dynamic Channel)			
Enable	Enable or disable the Dynamic Channel auto-RF functionality.		Disabled
Packet Error Rate	Enable channel change using unsuccessful packet transmissions by the AP.		
Packet Error Rate Threshold	Specifies the packet error rate threshold in percentage (%).	10-90%	30

Parameter	Description	Range	Default
Number of Packet Error Rate samples	Specifies the number of packet error rate samples needed to trigger a channel switch.	1-120	40
Channel Utilization	Enable channel change using the channel efficiency.		
Channel Utilization Threshold	Specifies the channel utilization threshold in percentage (%).	30-100%	70
Number of Channel Utilization samples	Specifies the number of channel utilization samples needed to trigger a channel switch.	5-300	100
Noise	Enable channel change with higher noise.		
Noise Threshold	Specifies the noise threshold in dBm.	-70 to -90 dBm	-70
Number of Noise samples	Specifies the number of noise samples needed to trigger a channel switch.	5-120	40
Auto-RF Iterations	Specifies the number of times the Auto-RF channel change function must run, at the configured frequency, before stopping. The iteration count resets when the AP restarts or when the radio resets. The default value is 0. It indicates that the Auto-RF channel change function will run at the frequency configured in either of the following parameters without stopping: • Enable time range for Auto-RF • Channel Hold Time  Note When the AP exceeds the configured iteration count, the Dynamic Channel Selection (DCS) method of channel selection takes over. For more information on Auto-RF, see Auto-RF.	0-100	0

Parameter	Description	Range	Default
Samples	Specifies the minimum number of samples required to run the channel selection.	1-20	3
Enable time range for Auto-RF	Specifies the time range (in the 24 hour format) at which the Auto-RF channel change function must run everyday. When enabled, select the start and end time.		
Channel Hold Time	Specifies the time (in minutes) for which the AP must hold the channel.		1440

To configure **Auto-RF (Dynamic Channel)** using the CLI, execute the following commands:

```
ap(config-radio-1)# auto-rf dynamic-channel

  acceptance-per-threshold : Configure Acceptance Packet Error Rate
(PER) threshold
  channel-hold-time       : specifies how much time AP needs to hold the
channel. Default is 1440 mins
  cmbnbr-minsnr          : Configure the cambium neighbour minimum SNR to
consider as part of autorf cambium neighbour factor
  congestion-channel-switch : Enable / Disable Congestion based channel
switch, disabled by default
  congestion-threshold    : Configure Congestion threshold
  count                  : Configure number of times autorf need to run;
'0' disables this feature
  dcs-monitor-interval   : Configure dcs monitor interval in minutes.
  dcs-trigger-threshold  : Configure dcs trigger threshold percentage
  per-channel-switch     : Enable / Disable PER based channel switch,
disabled by default
  samples                : Configure the minimum number of samples
required to run the channel selection
  schedule-time          : Configure time range (24 hour format) at which
autorf algorithm need to run everyday
  weightage-map-index    : Configure weightage map index
```

To configure **Auto-RF (Dynamic Power)** using the CLI, execute the following commands:

```
ap(config-radio-1)# auto-rf dynamic-power

  cellsize-overlap-threshold : Cell overlap that will be allowed when
the AP is determining automatic cell sizes
  maximum-transmit-power    : Maximum transmit power that the AP can assign
to a radio when adjusting automatic cell sizes
  minimum-neighbor-threshold : The Minimum number of neighbors to
consider for power reduction by autocell logic
```

minimum-transmit-power : Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes
mode : Set dynamic power mode by-channel/by-band

Figure 11 Radio parameters in the Basic page

Basic

Status

☒ Enabled
 ☐ Disabled
 Enable/Disable operation of this radio

Channel

Auto

 Only 'Auto' value is allowed. Configure static channel under the 'Advanced Settings' section available on the Access Point level configuration page. [Learn more](#)

Candidates Channel

All

 Candidate channels is a list of channels on which AP can operate. List of channels depend on the band and country.

Channel Width

20

 Operating width of the channel

Transmit Power

Auto

 Radio transmit power in dBm (4 to 30; subject to regulatory limit)

Beacon Interval

100

 Beacon interval in ms (50 to 3500) ⓘ

Minimum Unicast Rate

1

 Configure the minimum unicast management rate (Mbps)

Multicast Data Rate

Highest Basic

 Data-rate to use for transmission of multicast/broadcast packets

Mode

Default

 Allow 802.11 b/g/n clients to connect

☐ Airtime Fairness
 Enable Airtime Fairness to improve performance of 11n and 11ac clients by throttling legacy clients

☒ Short Guard Interval
 Enable Short Guard interval to increase device throughput

Figure 12 Channel Scan - Off Channel Scan option

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)

Figure 13 Channel Scan - Continuous Background Scan option

Channel Scan

☐ Off Channel Scan
 ☒ Continuous Background Scan
 ☐ None
 Enable/Disable operation of this radio

Continuous background scan (CBS) reduces the dwell time, controls the channel switches and also monitors the voice data queues.

Rest Time

6

 Rest Time — Interval between scans on different channels (5-15).

Wait Time

2

 Configure wait time in minutes to wait after all channels are scanned and before starting a new scan (1-10)

Dwell Split Time

25

 Configure dwell split time to spend on foreign channel

Dwell Rest Time

100

 Configure time interval between scans on same channel (100-1000)

☐ Channel Switch Announcement
 Use channel switch announcement as a part of channel change

Figure 14 Auto-RF - Dynamic Channel

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, etc.

Mode Selection

Dynamic Channel

Dynamic Power

☒ 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

Auto-RF Iterations

Configure number of times Auto-RF needs to run (0-100). 0 disables this feature

Samples

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

☐ Enable time range for Auto-RF. Configure time range (24 hour format) at which Auto-RF needs to run everyday.

Channel Hold Time

Channel hold time specifies how much time AP needs to hold the channel <1-44640> mins for build '6.6.0.1' and onwards. Range <1-4320> applies for AP running build below '6.6.0.1'.

Deprecated (Version 3.11.4 and 4.0)

Channel Selection Mode

Interference

Channel selection done based on interference

Channel Utilization Threshold

Configure channel utilization threshold in %(20-40)

Figure 15 Auto-RF - Dynamic Power

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, etc.

Mode Selection

Dynamic Channel

Dynamic Power

☐ Enable Enable Dynamic Power management

☐ By-Channel

☒ By-Band Set dynamic power mode by-channel / by-band

Maximum Transmit Power

Maximum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-30) dBm

Minimum Transmit Power

Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-20) dBm

Minimum Neighbour Threshold

The Minimum number of neighbors to consider for power reduction by autocell logic. (1-10)

Cellsize Overlap Threshold

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

Software-Defined Radio (SDR) capabilities

Table 16 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		
XV2-21X	✓	✓					
XV2-23T	✓	✓					
XV2-22H	✓	✓					

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



Note

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

Enhanced Roaming

[Table 17](#) lists configurable fields that are displayed in the **Radio > Enhanced Roaming** tab.

Table 17 Configuring Radio > Enhanced Roaming parameters

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

☒ **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

15

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

BSS Coloring

Multiple APs operate on a shared channel by mitigating co-channel interference. This is achieved through a spatial reuse technique known as BSS Coloring, which enables devices in one BSS to ignore frames from other BSSs on the same channel that 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 allowing the STA to 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 allows users to configure the receiver sensitivity per radio. The configuration hooks are exposed from both CLI and XMS-Cloud. cnMaestro does not expose any hooks for configuring receiver configuration. Receiver configuration determines the signal power required at the receiver to achieve the targeted or configured bit rate. Every RF receiver comes with a default sensitivity, which may not be sufficient for achieving the required RF performance in terms of meeting the bit rate. Therefore, 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
```

```
ap(config)# multicast-snoop
ap(config)# no multicast-snoop
ap(config)# save
ap(config)# wireless radio 1
ap(config-radio-1)# multicast-to-unicast
ap(config-radio-1)# multicast-to-unicast mode 802.3
ap(config-radio-1)# multicast-to-unicast mode amsdu
ap(config-radio-1)# multicast-to-unicast exclude-list 224.0.0.1
ap(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
ap(config-radio-1)#
```

Boot loop detection

When an AP turns off thrice due to a power outage, the radios are turned off automatically with the message—**WLAN Radios not active when enabled due to power boot loop detection. Reboot to**

reactivate.

After one hour, the AP automatically restarts and the radios turn on as expected. However, if the radios must be recovered before this duration, the Administrator must manually restart the AP.

This feature is enabled, by default. To disable this feature, configure the following CLI command in the **AP Groups > User Overrides** section in cnMaestro:

```
!  
no power bootloop  
!
```

Auto-RF

This topic contains the following sections:

- [Overview](#)
- [Dynamic Channel](#)
- [Dynamic Power](#)
- [Auto-RF](#)
- [Auto-RF Rx Sensitivity](#)
- [Configuring Dynamic Channel](#)
- [Configuring Dynamic Power](#)
- [Radio Configuration](#)

Overview

Auto-RF allows APs to obtain various RF statistics and utilize them to provide wireless clients with a better RF environment by choosing the proper channel and transmitting power to each radio. This results in better application performance and improved quality of calls for the end user.

Auto-RF consists of the following two functionalities:

- [Dynamic Channel](#)—Enables radios to choose the best channel both at device turn on and subsequently if the channel or RF conditions change.
- [Dynamic Power](#)—Aids radios in determining the proper transmit power to deal with coverage gaps and reduce RF interference.

Dynamic Channel

Channel selection by APs can involve any of the following methods:

- [Auto Channel Selection \(ACS\)](#)
- [Dynamic Channel Selection \(DCS\)](#)

Auto Channel Selection (ACS)

Auto-RF runs independently on each device in a deployment. You can enable the feature in all the bands (2.4 GHz, 5 GHz, and 6 GHz (if AP supports)). In 2.4 GHz, channels 1, 6, and 11 are considered for channel selection. AP continuously executes the Continuous Background Scan (CBS) to collect samples and feed them to the ACS to choose the best channel based on the channel score. The packet queue is verified and the RF is monitored continuously to ensure that high priority traffic is delivered before starting the CBS. CBS is performed so that the device avoids background scan while voice and video traffic is transmitted. The scan is split into multiple slots to avoid diverting from the operating channel for a longer duration which will affect the performance of the AP.

Dynamic Channel Selection (DCS)

If the environment has a lot of Wi-Fi interference or high packet error rate, Dynamic Channel Selection (DCS) takes over and initiates Packet Error Rate (PER) and Channel Utilization (CU) based channel switch methods. The AP monitors the error rate and Wi-Fi interference to see whether the threshold is crossed to initiate the channel switch. The AP sends the channel switch announcement in a beacon before any channel change occurs.

Dynamic Power

In multi-AP deployments, APs must automatically determine the cell size (coverage area), that is, increase or decrease transmit power to ensure the following:

- There are no coverage gaps—Increase transmit power
- There is no interference because of overlapping APs. Overlapping of APs creates interference and clients roam between multiple APs if they see more than one AP with a good transmit power. —
Decrease transmit power

Packets and scan results from CBS are parsed and neighbor entries are created which contain data about their transmission power and their neighbors. Periodically this data is processed and categorized to display how neighbors have seen their SNR.

Auto-RF behavior on device turn on

When the AP turns on the first time, it performs an initial scan (for about 0-300 seconds) to select the best operating channel. During this scan, CBS collects samples. The AP remains on the selected channel until one of the following scenarios occur:

- channel hold time expires
- configuration changes
- the radio restarts

After the hold time expires, the AP reinitiates the ACS algorithm to reassess and choose a new channel based on collected samples. If the current channel still has the highest score, it is retained. In cases of configuration changes or radio restarts, the collected samples are reset, but historical data remains, allowing CBS to automatically collect fresh samples.

Auto-RF Rx Sensitivity

When APs are depolyed close together, it leads to overlapping APs and co-channel interference. In such scenarios, the clients may connect to distant APs instead of the nearby ones that have the best signal. The Auto Power feature helps reduce transmit power to minimize the overlapping APs issue, but does not completely fix it.

The Auto-RF Rx sensitivity feature ensures the clients connected to distant APs are disconnected based on repeated radio connection retries and failed acknowledgements. The feature also ensures that the clients connect only to nearby APs.

This feature is available only as CLI command that you can configure in the **AP Groups > User Overrides** section in cnMaestro. A sample configuration snippet is shown below:

```
!  
Wireless radio 1  
auto-rf dynamic-power rx-sens  
auto-rf dynamic-power rx-sens-min-threshold -80  
!
```

Configuring Dynamic Channel

Dynamic channel configuration is achieved by the following methods:

- [ACS method](#)
- [DCS method](#)

ACS method

In the ACS method, to enable auto-RF Dynamic Channel in the cnMaestro UI, complete the following steps:

1. Go to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New**.
3. Associate an existing WLAN and configure other AP group parameters.
4. Click **Radio** on the left menu.
5. In the required radio band tab, expand the **Auto-RF** section.
6. In the **Dynamic Channel** tab, select the **Enable** check box.

Mode Selection

Dynamic Channel

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

Once Auto-RF Dynamic Channel is enabled, ACS runs at regular intervals based on the **Samples** and **Channel Hold Time**, or the **Enable time range for Auto-RF** configuration parameters. For information on these parameters, see [Configuring the Radio](#).

DCS method

DCS configuration helps in avoiding instances when there is a spike in packet error rate (PER) or Channel Busy. The following are the default configuration parameters and their values:

- DCS trigger threshold—80%

CLI command—`auto-rf dynamic-channel dcs-trigger-threshold`

- DCS monitor interval—10 minutes

CLI command—`auto-rf dynamic-channel dcs-monitor-interval`

Both these parameters are available only as CLI commands that you can configure in the **AP Groups > User Overrides** section in cnMaestro.

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

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
auto-rf dynamic-channel dcs-monitor-interval 10
auto-rf dynamic-channel dcs-trigger-threshold 80
!
```

Consider a scenario where the device detects that the PER or Congestion threshold is exceeded for a brief period in a day. If the threshold breach occurred because of a spike in PER or Congestion, the AP must not change the channel. You can avoid this scenario by configuring the DCS threshold and monitor interval. When configured, the AP switches to a different channel if the PER or Congestion threshold is breached continuously for the DCS duration and if the percentage of the breach exceeds the DCS threshold. DCS is enabled if either Channel Utilization (CU) or Packet Error Rate (PER) parameter is enabled.

Packet Error Rate (PER)

Consider a scenario where an AP must switch channels if the PER is more than 30% in a 10 minute interval. The AP monitors the PER, and if it exceeds 30% (default threshold) for 80% of the samples in a 10-minute interval, it will initiate a channel switch. However, when the PER threshold is breached, other configurations, such as sampling, channel hold time, and intervals are overridden. With the default DCS threshold and interval configured, Auto-RF manages the channel switch when the above conditions are met. Hence, the AP changes channels if the PER remains consistently high (above 30%) for most of a 10-minute period.

Packet Error Rate Threshold	30	Configure packet error rate threshold in %(10-90)
Number of Packet Error Rate samples	40	Configure number of packet error rate samples, needed to trigger a channel switch (1-120)

Congestion channel switch

Consider a scenario where an AP must switch channels if the channel utilization exceeds a threshold of 70% (default) in a 10-minute interval. The AP monitors channel utilization, and if it exceeds 70% (default threshold) for 80% of the samples in a 10-minute interval, it will initiate a channel switch. However, when the congestion threshold is breached, other configurations, such as sampling, channel hold time, and intervals are overridden. With the default DCS threshold and interval configured, Auto-RF will handle the channel switch when the above conditions are met. Hence, the AP changes channels if channel utilization remains consistently high (above 70%) for most of a 10-minute period.

☒ Channel Utilization Enable channel change using the channel efficiency		
Channel Utilization Threshold	70	Configure Channel Utilization threshold in %(30-100)
Number of Channel Utilization samples	100	Configure number of Channel Utilization samples, needed to trigger a channel switch(5-300)

Configuring Dynamic Power

To enable auto-RF Dynamic Power in the cnMaestro UI, complete the following steps:

1. Go to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New**.
3. Associate an existing WLAN and configure other AP group parameters.
4. Click **Radio** on the left menu.
5. In the required radio band tab, expand the **Auto-RF** section.
6. In the **Dynamic Power** tab, select the **Enable** check box.

Mode Selection	
Dynamic Channel	Dynamic Power
☐ Enable Enable Dynamic Power management ☐ By-Channel ☒ By-Band Set dynamic power mode by-channel / by-band	

Dynamic Power can be configured in the following two modes:

- **By-Band:** Considers neighbor APs across all channels of same band for operating Auto-RF dynamic transmit power.

This is the default option in the Dynamic Power configuration.

- **By-Channel:** Considers only operating channel neighbor APs (that also within the same AP group) for operating Auto-RF dynamic transmit power.

When Auto-RF Dynamic Power is enabled, by default, CBS runs in the background with a 50% overlap threshold between APs. The default minimum transmit power is set to 8 dBm. The dynamic-power algorithm cannot reduce the transmit power below this level, even if there is overlap in AP signals. The **Minimum Neighbor Threshold** parameter defines the minimum number of neighboring APs required to enable dynamic power selection.

With Auto-RF Dynamic Power enabled, the system manages transmit power while maintaining a minimum level and considering AP overlap and neighbor requirements.

☐ By-Channel
 ☒ By-Band
 Set dynamic power mode by-channel / by-band

Maximum Transmit Power	30	Maximum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-30) dBm
Minimum Transmit Power	8	Minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes. (5-20) dBm
Minimum Neighbour Threshold	2	The Minimum number of neighbors to consider for power reduction by autotcell logic. (1-10)
Cellsize Overlap Threshold	50	Cell overlap that will be allowed when the AP is determining automatic cell sizes (0-100) %

Radio Configuration

For Auto-RF feature to function correctly, the following configuration is recommended:

- [Basic section](#)
- [Channel Scan section](#)

Basic section

Configure the following parameters in the **Radio > Basic** section with the recommended values:

- **Channel**—Auto
- **Transmit Power**—Auto
- **Channel Width**—20, 40, 80, or 160 MHz based on the deployment
- **Candidates Channel**—All.

If you want to restrict the APs to operate on specific channels, you must configure the required channels.

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](#)

Candidate Channels

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) ⓘ

Channel Scan section

Configure the following parameters in the **Radio > Channel Scan** section with the recommended values:

- Select the **Continuous Background Scan (CBS)** option—Selected by default.
- **Wait Time** in minutes
- **Rest Time**, **Dwell Split Time**, and **Dwell Rest Time** in milliseconds
- Select the **Channel Switch Announcement** check box to enable the AP to send notifications before any channel change.

Channel Scan

☐ Off Channel Scan
 ☒ Continuous Background Scan
 ☐ None
 Enable/Disable operation of this radio

Continuous background scan (CBS) reduces the dwell time, controls the channel switches and also monitors the voice data queues.

Rest Time

6

Rest Time — Interval between scans on different channels (5-15 seconds).

Wait Time

2

Configure wait time in minutes to wait after all channels are scanned and before starting a new scan (1-10 minutes)

Dwell Split Time

25

▼

Configure dwell split time to spend on foreign channel

Dwell Rest Time

100

Configure time interval between scans on same channel (100-1000 milliseconds)

☐ Channel Switch Announcement Use channel switch announcement as a part of channel change

Configuring the Wireless LAN

This chapter describes the following topics:

- [Overview](#)
- [Configuring the WLAN parameters](#)
- [Link Aggregation Control Protocol \(LACP\)](#)
- [RADIUS attributes](#)
- [Enterprise PSK \(ePSK\)](#)
 - [Configuring ePSKs](#)
 - [ePSK registration for WPA3 clients](#)
 - [Creating a Personal Wi-Fi ePSK](#)
- [RADIUS-based ePSK](#)
- [Groupwise Transient Key \(GTK\) per VLAN](#)
- [Dynamic ARP Inspection](#)

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

To configure WLAN parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > WLANs** page.
2. Click **Add** and select **Enterprise Wi-Fi** from the **Type** drop-down list.

Following are the configurable parameters under the WLAN profile:

- [Basic](#)
- [Radius Server](#)
- [Guest Access](#)

- [Internal Access Point](#)
- [External Hotspot](#)
- [cnMaestro](#)
- [Usage Limits](#)
- [Scheduled Access](#)
- [Access](#)
- [Passpoint](#)

Basic

[Table 18](#) lists configurable fields that are displayed in the **WLANs > Basic Settings** section.

Table 18 Basic parameters

Parameters	Description	Range	Default
WLAN > Basic Settings			
Enable	Enables a WLAN profile. Once enabled, a Beacon is broadcasted with the SSID and the corresponding parameters configured in a WLAN profile.	-	-
SSID	Unique network name that wireless stations scan and associate.	-	-
Mesh	This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. This parameter supports the following options: • Base: A WLAN profile configured with a mesh-base will operate as a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients. • Client: A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-base AP to connect. • Recovery: WLAN profile configured as mesh-recovery will broadcast a pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on a mesh-base device. Meshclient will auto scan for mesh-recovery SSID upon failure of mesh link. • Off: Mesh support disabled on WLAN profile.	-	Off (Access Profile Mode)

Parameters	Description	Range	Default
VLAN	Segregates wireless station traffic from AP traffic in the network. Wireless stations obtain an IP address from the subnet configured in the VLAN field of the WLAN profile.	1-4094	1
Security	Determines key values that are encrypted based on the selected algorithm. Following security methods are supported: Open This method is preferred when Layer 2 authentication is built into the network. With this configured on an Enterprise Wi-Fi AP device, any wireless station will be able to connect. Open 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. OWE (Enhanced Open) This method ensures the communication between each pair of endpoints is protected from other endpoints. WPA2 Pre-Shared Keys This mode is supported with AES and TKIP encryption. WPA-TKIP can be enabled from the CLI with the <code>allow-tkip</code> CLI option. Note 6 GHz clients connect to the AP using the secure Simultaneous Authentication of Equals (SAE) method. WPA2 Enterprise This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication methods. WPA2/WPA3 Pre-shared Keys WPA3 comes with a transition mode where WPA2-only capable clients can connect to SSID. WPA2-only capable clients connect using the older PSK method while WPA3 capable clients connect using a more secure SAE method.	-	Open

Parameters	Description	Range	Default
	WPA3 Pre-shared Keys WPA3 replaces the Pre-Shared Key (PSK) exchange with SAE of Equals, which is more secure and provides forward-secrecy as well as resistance to offline dictionary attack.  Note When you select WPA2/WPA3 Pre-shared Keys or WPA3 Pre-shared Keys, you can enable registration flow for WPA3 clients. To enable the registration flow, you must create an ePSK passphrase and follow the procedure for the clients to undergo the registration flow. For more information, see ePSK registration for WPA3 clients. WPA3 Enterprise WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. WPA3 Enterprise CNSA WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite and is commonly used in high-security Wi-Fi networks in government, defense, Finance, and industrial verticals. User Pre-shared keys The U-PSK (User-PSK) Authentication settings are only used in conjunction with XMS Cloud's EasyPass Onboarding Portals. The Cloud automatically configures this setting for an WLAN when you create an Onboarding portal and you assign that WLAN to the portal. Thus, you should not normally change this setting manually. Note that the User- PSK settings are only available on the WLAN profile.		

Parameters	Description	Range	Default
Band	Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options are available to configure transmit mode of SSID: • 2.4 GHz • 5 GHz • 6 GHz	-	all
Client Isolation	Enable this feature when there is a need for restriction of wireless station-to-station communication across the network or on an AP.  Note • For client isolation to work correctly, it is recommended that clients obtain their IP addresses through DHCP. • You must manually update the default gateway addresses in the IP configuration of clients that are using static IP addresses. • If the gateway MAC address changes due to hardware replacement or any other reason, you must restart the AP for the AP to learn the new gateway MAC address and to make sure the client isolation functions correctly. The following options are available to configure based on requirement: • Disable This option when selected disables the client isolation feature. that is, any wireless station can communicate to other wireless stations. • Local This options when selected enable the client isolation feature. This option prevents wireless station communications connected to the same AP. • Network Wide		

Parameters	Description	Range	Default
	This options when selected enable the client isolation feature. It prevents wireless stations communications connected to different AP deployed in the same L2 network.  Note • Network-wide mode is not supported when Redundancy Gateway protocol is used on deployment. • In the Redundancy Gateway case, Network-wide static can be used to provide a list of Gateway MAC addresses. • Network Wide Static This option when configured enables client isolation feature across the network. Wireless stations can communicate only to statically added MAC list. Communication to rest other MAC addresses are blocked.  Note When Network Wide and Network Wide Static are selected, the user has the provision to add the whitelist MAC addresses to allow the communication. A maximum of 64 MAC addresses can be added.		
cnMaestro Managed Roaming	Provision to enable centralized management of roaming for wireless clients through cnMaestro.	-	-
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	-	Disabled
Session Timeout	This field applies to all wireless clients connected to the SSID. When a wireless station connects, a session timer is triggered. Once session time expires, the wireless station must undergo either re-authentication or re-association based on the state of the wireless station. By default, it is enabled.  Note Following priority takes precedence for the session timeout:	60-604800	28800

Parameters	Description	Range	Default
	a. Configured from the RADIUS server b. Configured from the AP		
Inactivity Timeout	Inactivity timer triggers whenever there is no communication between Enterprise Wi-Fi AP device and wireless station associated to Enterprise Wi-Fi AP device. Once the timer reaches the configured Inactivity timeout value, APs send a de-authentication to that wireless station. By default, it is enabled.  Note Following priority takes precedence for the inactivity timeout: a. Configured from the RADIUS server b. Configured from the AP	60-28800	1800

Figure 16 Basic parameters

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

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
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
Client Isolation

When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN
☐ cnMaestro Managed Roaming
Enable centralized Guest Access Session management of roaming for wireless clients through cnMaestro
☐ Hide SSID Do not broadcast SSID in beacons
Advanced Settings

Table 19 WLAN (Max clients) parameters

Number of clients	2.4 GHz	5 GHz	6 GHz	Concurrent
XV2-21X	128	128	NA	256
XV2-23T	128	128	NA	256
XV2-22H	128	128	NA	256

Maximum wireless client

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

Maximum clients per device

Most customers commonly use more than a single SSID. They prefer to set the maximum number of wireless clients connection per device, that is, 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:

```
ap(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:

```
ap(config)# wireless wlan 1
ap(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:

```
ap(config)# wireless wlan 1
```

```
ap(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 must 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:

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



Note

The OWE transition mode SSIDs do not apply to 6 GHz radios.

Table 20 Advanced parameters

Parameters	Description	Range	Default
WLAN > Advanced			

Parameters	Description	Range	Default																														
VLAN Pooling	This parameter is required when a user requires to distribute clients across multiple subnets. Different modes of VLAN pooling is supported by Enterprise Wi-Fi AP devices, based on infrastructure available at the deployment site. Modes supported are as follows: Disabled This feature is disabled for this WLAN. Radius Based The user is expected to configure WPA2 Enterprise for this mode to support. During the association phase, AP obtains pool name from RADIUS transaction and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IP address from the VLAN selected by Enterprise Wi-Fi AP device. Static For this mode to support, the user requires to configure VLAN Pool details available under Configure > Network > VLAN pool. During the association phase, AP obtains pool, and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4 address from the VLAN selected by the Enterprise Wi-Fi AP device.	–	Disabled																														
Max Clients	This specifies the maximum number of wireless stations that can be associated with a WLAN profile. This varies based on the Enterprise Wi-Fi AP device model number. Refer to Table 19 for more details.	1-512 (Refer Table 19)	256																														
UAPSD	When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming are in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by the Enterprise Wi-Fi AP device. <table><tr><th>Priority</th><th>802.1D Priority (= UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr><tr><td rowspan="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></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																																

Parameters	Description	Range	Default
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
Monitored Host			
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
Connection Logging Host	When enabled provides information of all IP connections accessed by a wireless station that is associated with WLAN and logs the connection data seamlessly onto an external syslog server.	–	Disabled
Band Steering	This feature when enabled steers wireless stations to connect to 5GHz. There are three modes supported by Enterprise Wi-Fi devices. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces the wireless station to connect to the 5 GHz band. • Low • Normal • Aggressive	–	Disabled
Proxy ARP	Provision to avoid ARP flood in a wireless network. When enabled, AP responds to ARP requests for the wireless stations connected to that AP. This is for IPv4 infrastructure.	–	Enabled

Parameters	Description	Range	Default
Proxy ND	When enabled, AP responds to IPv6 Neighbor Discovery (ND) requests for the wireless stations connected to that AP.		
Unicast DHCP	Provision to transmit DHCP offer and ACK/NACK packets as Unicast packets to wireless stations.	–	Enabled
Insert DHCP Option 82	When enabled, DHCP packets generated from wireless stations that are associated with APs are appended with Option 82 parameters. Option 82 provides a provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID: • Hostname • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom • All  Note In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered: 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration	–	Disabled
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ network either using L2TP or L2GRE.	–	Disabled

Parameters	Description	Range	Default
Fast-Roaming Protocol	One of the important aspects to support voice applications on a Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 ms to avoid any call drop. This is easily achievable when the WPA2-PSK security mechanism is in use. However, in enterprise environments, there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with the AAA server, and hence depending on the location of the AAA server the roaming time will be above 700 ms. Select any one of the following: OKC This roaming method is a Cambium Networks proprietary solution to share the client authentication information with other Cambium Networks APs on the same network by sending encrypted information on wire on SSID VLAN. This information sharing does not require cnMaestro so even in cases where AP is not connected to cloud, the roaming will be seamless. 802.11r Fast transition (FT) is an IEEE standard to permit continuous connectivity aboard wireless devices in motion, with fast and secure client transitions from one Basic Service Set (abbreviated BSS, and also known as a base station or more colloquially, an access point) to another, performed in a nearly seamless manner. The terms handoff and roaming are often used, although 802.11 transition is not a true handoff/roaming process in the cellular sense, where the process is coordinated by the base station and is generally uninterrupted.	–	Disabled
RRM (802.11k)	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 802.11k clients. The following parameter must be enabled: Enable RRM	–	Disabled
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled

Parameters	Description	Range	Default
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

Figure 17 Advanced parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Advanced Settings

Maximum Clients

127

Maximum number of clients assigned per Radio (1-512)

VLAN Pooling

Disabled

Configure VLAN Pooling

Session Timeout

28800

Session time in seconds (60 to 604800)

Inactivity Timeout

1800

Inactivity time in seconds (60 to 28800)

☐ Drop Multicast Traffic

Drop the send/receive of multicast traffic

☐ UAPSD

Enable WMM Power Save/UAPSD (for VoIP and streaming)

☐ QBSS

Append QBSS Load IE in management frame to improve AP selection

DTIM Interval

1

Configure Delivery Traffic Indication Message (1 – 255 beacon count)

Monitored Host

Host

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

Interval

300

Duration in seconds (60-3600)

Attempts

5

Number of attempts to check the reachability of monitored host (1-20)

DNS Logging Host

Port

514

Syslog server where all client DNS requests will be logged

Connection Logging Host

Port

514

Syslog server where all client connection requests will be logged

Band Steering

Disable

Steer clients across all Bands.

☒ Proxy ARP

Respond to ARP requests automatically on behalf of clients

☐ Proxy ND

Respond to IPv6 Neighbor Discovery (ND) requests automatically on behalf of clients

☒ Unicast DHCP

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

☐ Insert DHCP Option 82

Enable DHCP Option 82

☐ Tunnel Mode

Enable tunnelling of WLAN traffic over configured tunnel

Fast Roaming Protocol

☐ OKC

☐ 802.11r

Configure roaming protocol (not applicable when authentication type is Open)

☒ RRM (802.11k)

Enable Radio Resource Measurements (802.11k)

☒ 802.11v

Enable 802.11v BSS Transition Management

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

```

ap(config)# wireless wlan 1
ap(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:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# vlans-allowed
{vlan_list} <e.g 1-10,15,100>
ap(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:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# ipv6-router-advertisement-unicast
vlans : Configure vlans where IPV6 Router Advertisement unicast
conversion needed
ap(config-wlan-1)# ipv6-router-advertisement-unicast vlans
{vlan_list} <e.g 1-10,15,100>
ap(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

To configure a RADIUS server, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles WLAN** tab, select **Radius Server** tab and provide the details as given in [Table 21](#):

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.  Note The Realm parameter can be left blank, unless you would like to use this server only for certain usernames where the network domain is included. For example, in <username>@cambium.com or <domain-name>/<username>, the realms are @cambium.com and <domain-name>/, and this server will be selected only if the username has the appropriate realm.	-	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

Parameters	Description	Range	Default
Attempts	Parameter to configure many attempts that a device should send AAA request to server if no response is received within the configured timeout period.	1-3	1
Accounting Mode	This field is enabled based on customer requirements. The accounting packet is transmitted based on the mode selected. Start-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station is connected and then disconnects. Start-Interim-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects. None The accounting mode will be disabled.	-	Disabled
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Sync Accounting Records	Provision to configure accounting records to be synced across neighboring APs.	-	-
Server Pool Mode	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode. Load Balance—AP communicates with multiple servers and ensures that authorization and accounting are equally shared across configured servers. Failover—AP selects the RADIUS server which is up and running based on the order of configuration.	-	Failover
NAS-Identifier	This is a configurable parameter and is appended in the RADIUS request packet.	-	Hostname/ System Name
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled

Parameters	Description	Range	Default
Dynamic VLAN	When enabled, AP honors the VLAN information provided in the RADIUS transaction. Wireless station requests IP address from the same VLAN learned through RADIUS.	-	Enabled
Called Station ID	The following information can be communicated to the RADIUS server: • AP-MAC • AP-MAC: SITE-NAME • AP-MAC: SSID • AP-MAC: SSID-SITE-NAME • AP-NAME • AP-NAME: SITE-NAME • AP-NAME: SSID • SITE-NAME • SSID • CUSTOM	-	AP-MAC: SSID

Figure 18 The RADIUS Server parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Warning: AAA Servers are configured separately for each WLAN.

Authentication Server

1. Host Secret Port* Realm

2. Host Secret Port* Realm

3. Host Secret Port* Realm

Timeout
 Timeout in seconds for each request attempt (1-30)

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

☐ **Accounting Server**

1. Host Secret Port*

2. Host Secret Port*

3. Host Secret Port*

Timeout
 Timeout in seconds for each request attempt (1-30)

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

Accounting Mode
 Configure accounting mode

☐ Accounting Packet Enable Accounting-On messages

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

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

☐ **Advanced Settings**

Server Pool Mode
☒ Load Balance Load balance requests equally among configured servers
☐ Failover Move down server list when earlier servers are unreachable

NAS-Identifier
 NAS-Identifier attribute for use in Request packets (defaults to system name)

☐ Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)

☒ Dynamic VLAN Enable RADIUS assigned VLANs

Called Station ID:
 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 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:

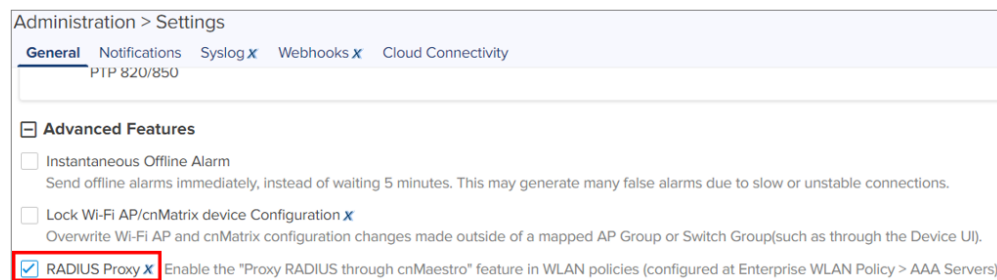
```
ap(config-wlan-1)# radius-server through-controller
```

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 **WLANs > Guest Access > Internal Access Point** page.

Table 22 Internal Access Point parameters

Parameters	Description	Range	Default
WLAN > Guest Access > Internal Access Point			

Parameters	Description	Range	Default
Enable	Enables the Guest Access feature.	-	Disabled
Access Policy	There are four types of access types provided for the user: 1. Clickthrough This mode allows the users to get access data without any authentication mechanism. User can access the internet as soon as he is connected and accepts Terms and Conditions 2. RADIUS This mode when selected, the user has to provide a username and password, which is then redirected to the RADIUS server for authentication. If successful, the user is provided with data access. 3. Local Guest Account Users must configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.	-	Clickthrough
Redirect Mode	This option helps the user to configure the HTTP or HTTPS mode of redirection URL. 1. HTTP AP sends an HTTP POSTURL to the associated client, in the <code>http://<Pre-defined-URL></code> format. 2. HTTPS AP sends HTTPS POSTURL to the success associated client, in the <code>https://<Pre-defined-URL></code> format.	-	HTTP
Redirect Hostname	Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.	-	-

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

Parameters	Description	Range	Default
	This option is selected by default. The following information is appended in the redirection URL: • SSID • AP MAC • NAS ID • AP IP • Client MAC • Redirection URL • Users can provide either HTTP or HTTPS URL		
Redirection user to Original URL	Users will be redirected to the URL that is accessed by the user before successful captive portal authentication. There are additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below: • Prefix Query Strings in Redirect URL This option is selected by default. The following information is appended in the redirection URL: • SSID • AP MAC • NAS ID	-	-
Success message	Provision to configure the text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	-	-
Redirect	• If enabled, only HTTP URLs will be redirected to the Guest Access login page. • If disabled, both HTTP and HTTPS URLs will be redirected to the Guest Access login page.	-	Enabled
Redirect User Page	IPv4 address configured in this field is used as logout URL for Guest Access sessions.	-	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy	1 - 65535	-

Parameters	Description	Range	Default
	port to be redirected to the login page.		
Session Timeout	This is the duration of time, the client will be allowed to access the internet if quota persists, after which AP sends de-authentication. The wireless station has to undergo Guest Access authentication after session timeout.  Note Following priority takes precedence for the session timeout: - Configured from the RADIUS server - Configured from the AP	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.  Note Following priority takes precedence for the inactivity timeout: - Configured from the RADIUS server - Configured from the AP	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to the Guest Access login page after any supported type of MAC address authentication fails.	-	Disabled
Whitelist	Provision to configure either IPv4 or URLs to bypass traffic, therefor user can access those IPs or URLs without Guest Access authentication.	-	-

Figure 20 The Internal Access Point parameters

The screenshot shows the 'WLANs > Add New' configuration page. The left sidebar lists various configuration categories: WLAN, AAA Servers, Guest Access (selected), Access Control, Pasaport, and ePSK. The main content area is divided into 'Basic Settings' and 'Advanced Settings'.

Basic Settings:

- Enable:** ☐
- Portal Mode:** ☒ Internal Access Point, ☐ External Hotspot, ☐ ePSK
- Access Policy:**
 - ☒ Clickthrough: Splash page where users accept terms and conditions to get on the network.
 - ☐ RADIUS: Splash page with username and 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.
- AP Server Protocol:**
 - ☒ HTTP: Use unsecured HTTP protocol for AP guest access server.
 - ☐ HTTPS: Use secured HTTPS protocol for AP guest access server.
- Redirect Hostname:** (Redirect Hostname for the splash page (up to 255 characters))
- Title:** (Title text in splash page (up to 255 characters))
- Contents:** (Main contents of the splash page (up to 255 characters))
- Terms:** (Terms and conditions displayed in the splash page (up to 255 characters))
- Logo:** (Logo to be displayed on the splash page, e.g., http://domain.com/logo.png)
- Background Image:** (Background image to be displayed on the splash page, e.g., http://domain.com/backgroundimage.jpg)
- Success Action:**
 - ☒ Internal Logout Page
 - ☐ Redirect User to External URL
 - ☐ Redirect User to Original URL
- Success Message:**

Advanced Settings:

- Redirect:**
 - ☒ HTTP only: Enable redirection for HTTP packets only.
- Redirect User Page:** (Configure IP address for redirecting user to guest portal splash page, e.g., 192.168.1.1)
- Redirection Port:** (Port number (1 to 65535), e.g., 8080)
- Session Timeout:** (Session time in seconds (60 to 2592000), e.g., 3600)
- Inactivity Timeout:** (Inactivity time in seconds (60 to 2592000), e.g., 1800)
- ☐ 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)

Pre-Login Allowed Domains:

IP Address / Domain Name	Action
No IP Address or Domain Name Available	

Captive Portal Bypass User Agent:

Index	User Agent String	HTTP Code	HTML Reply	Action
No User Agent rule available				

External Hotspot

Below table lists the configurable fields that are displayed in the **WLANs > Guest Access > External Hotspot** tab.

Table 23 External Hotspot parameters

Parameters	Description	Range	Default
WLAN > Guest Access > External Hotspot			
Access Policy	There are four types of access types provided for the end user: Clickthrough This mode allows users to get access data without any authentication mechanism. The user can access the internet as soon as he is connected and accepts the Terms and Conditions.	–	Clickthrough

Parameters	Description	Range	Default
	2. RADIUS The user has to provide a username and password, which is then redirected to a RADIUS server for authentication. If successful, the user is provided with data access. 3. Local Guest Account The user has to configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.		
Redirect Mode	Provision to configure the HTTP or HTTPS mode of redirection URL. 1. HTTP AP sends an HTTP POSTURL to the associated client, in the <code>http://<Pre-defined-URL></code> format. 2. HTTPS AP sends an HTTPS POSTURL to the associated client, in the <code>http://<Pre-defined-URL></code> format.	–	HTTP
Redirect Hostname	Users can configure a friendly hostname, which is added to the DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with an IP address in the redirection URL provided to wireless stations.	-	-
External Page URL	Users can configure a landing/login page that is posted to wireless stations that are not Guest Access authenticated.	–	–
External Portal Post Through cnMaestro	This is required when HTTPS is only supported by an external guest access portal. This option when enabled minimizes certification. The certificate is required to install only in cnMaestro On-Premises.	–	Disabled
External Portal Type	Enterprise Wi-Fi AP products are supported by standard mode configuration. • Standard	–	Standard

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

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

Parameters	Description	Range	Default
Session Timeout	This is the duration of time, the client will be allowed to access the internet if quota persists, after which AP sends de-authentication. The wireless station has to undergo Guest Access authentication after session timeout.  Note Following priority takes precedence for the session timeout: - Configured from the RADIUS server - Configured from the AP	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.  Note Following priority takes precedence for the inactivity timeout: - Configured from the RADIUS server - Configured from the AP	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to the Guest Access login page after any supported type of MAC address authentication failures.  Note This feature works only when Guest Access is configured with RADIUS authentication under WLANs > Guest Access > Access Policy > RADIUS.	–	Disabled
Extend Interface	Provision to support the Guest Access on the Ethernet interface.	–	Disabled

Figure 21 External Hotspot parameters

The screenshot displays the configuration interface for a new WLAN profile, specifically the 'Guest Access' section under 'cnMaestro'. The interface is divided into several sections:

- Basic Settings:** Includes options to enable/disable the feature, select the portal mode (Internal Access Point, External Hotspot, or cnMaestro), and choose an access policy (Clickthrough, RADIUS, LDAP, or Local Guest Account).
- AP Server Protocol:** Options to use unsecured HTTP or secured HTTPS for the AP guest access server.
- Redirect Hostname:** A text field for the redirect hostname, with a note that it can be up to 255 characters.
- External Page URL:** A text field for the external page URL.
- External Portal Post Through cnMaestro:** A checkbox to enable this feature.
- External Portal Type:** A dropdown menu currently set to 'Standard'.
- Success Action:** Options to redirect the user to the external URL or the original URL.
- Success Message:** A text field for a custom success message.
- Advanced Settings:** Includes checkboxes for 'Redirect User Logout Page', 'Redirect User to External URL', and 'Redirect User to Original URL'. It also has a 'Success Message' field.
- Pre-Login Allowed Domains:** A section for adding domains that are allowed to log in before the main authentication process.
- Captive Portal Bypass User Agent:** A section for adding user agents that can bypass the captive portal.

cnMaestro

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

Table 24 The *cnMaestro* parameters

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	—	—
Redirect	- If enabled, only HTTP URLs will be redirected to the Guest Access login page. - If disabled, both HTTP and HTTPS URLs will be redirected to Guest Access login page.	—	Enabled
Redirect User Page	The IP address configured in this field is used as a logout URL for Guest Access sessions. The IP address configured should be not	—	1.1.1.1

Parameters	Description	Range	Default
	reachable to the internet.		
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	–
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.  Note Following priority takes precedence for the inactivity timeout: - Configured from the RADIUS server - Configured from the AP	60 - 2592000	1800
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	–	–

Figure 22 *cnMaestro parameters*

The screenshot shows the 'WLANs > Configuration' page with the 'Guest Access' tab selected. The left sidebar lists 'WLAN', 'AAA Servers', 'Guest Access' (highlighted), 'Access Control', 'Passpoint', and 'ePSK'. The main content area is titled 'Basic Settings' and includes the following sections:

- Basic Settings:**
 - ☐ Enable
 - Portal Mode: ☐ Internal Access Point, ☐ External Hotspot, ☒ cnMaestro
 - Portal Name:
- Advanced Settings:**
 - Redirect: ☒ HTTP-only (Enable redirection for HTTP packets only)
 - Redirect User Page: (Configure IP address for redirecting user to guest portal splash page)
 - 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)
 - Extend Interface: (Configure the interface which is extended for guest access)
- Pre-Login Allowed Domains:**
 -
 - Table with columns: IP Address / Domain Name, Delete
 - Message: No IP Address or Domain Name Available
- Captive Portal Bypass User Agent:**
 -
 - Table with columns: Index, User Agent String, HTTP Code, HTML Reply, Delete
 - Message: No User Agent rule available

Usage Limits

Below table lists configurable fields that are displayed in the **WLANs > Access Control > Usage Limits** section.

Table 25 *Usage Limits parameters*

Parameters	Description	Range	Default
Rate Limit per Client	Provision to limit throughput per client. Default allowed throughput per client is unlimited, that is, 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]

Parameters	Description	Range	Default
Rate Limit per WLAN	Provision to limit throughput 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]

Figure 23 The Usage Limits parameters

The screenshot shows the 'WLANs > Add New' configuration page. On the left is a sidebar menu with options: WLAN, AAA Servers, Guest Access, Access Control (highlighted in blue), Passpoint, and ePSK. The main content area is titled 'Usage Limits' and contains two sections, each with a checkbox and input fields. The first section, 'Rate Limit per Client', has checkboxes for 'Upstream' and 'Downstream', both with input fields set to '0' and a 'Kbps' unit label. The second section, 'Rate Limit for WLAN', also has checkboxes for 'Upstream' and 'Downstream', both with input fields set to '0' and a 'Kbps' unit label.

Scheduled Access

Below table lists configurable fields that are displayed in the **WLANs > Access Control > Scheduled Access** section.

Table 26 The Scheduled Access parameters

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

Parameters	Description	Range	Default
	From release version 6.3 onwards, users are allowed to configure up to a maximum of 12 scheduled access rules per day on a particular WLAN instead of one rule per day.		

Figure 24 The Scheduled Access parameters

WLANs > Add New

WLAN	Scheduled Access Sunday Start Time (HH:MM) End Time (HH:MM) Monday Start Time (HH:MM) End Time (HH:MM) Tuesday Start Time (HH:MM) End Time (HH:MM) Wednesday Start Time (HH:MM) End Time (HH:MM) Thursday Start Time (HH:MM) End Time (HH:MM) Friday Start Time (HH:MM) End Time (HH:MM) Saturday Start Time (HH:MM) End Time (HH:MM)
AAA Servers	
Guest Access	
Access Control	
Passpoint	
ePSK	

CLI Configuration:

```

ap(config)# wireless wlan 1
ap(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
ap(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 **WLANs > Access Control** tab.

Table 27 The Access parameters

Parameters	Description	Range	Default
DNS-ACL			
Precedence	Provision to configure index of ACL rule. Packets are validated and processed based on the Precedence value configured.	-	1
Action	Provision to configure whether to allow or deny traffic.	-	Deny
Domain	Provision to configure domain names and rules are applied based on Action configured.	-	-
MAC Authentication			
MAC Authentication Policy	Enterprise Wi-Fi AP supports multiple methods of MAC authentication. Following are the details of each mode: Permit Wireless station MAC addresses listed will be allowed to associate to AP. Deny When the user configures a MAC address, those wireless stations shall be denied to associate and the non-listed MAC address will be allowed. RADIUS For every wireless authentication, AP sends a RADIUS request and if RADIUS acceptance is received, then the wireless station is allowed to associate. In case authentication fails, you can enable AP to assign the default WLAN VLAN to the clients. For this, you must configure the <code>failed-allow-traffic</code> CLI command. For more information, see Fallback to WLAN VLAN when RADIUS-based MAC authentication fails. cnMaestro This option is preferable when the administrator prefers a centralized MAC authentication policy. For every wireless authentication, AP a sends query to cnMaestro if it is allowed or disallowed to connect. Based on the configuration, wireless stations are either allowed or denied.	-	Deny

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 25 The Access parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Access Control Lists

Policy Based ACL
① Policy Based ACLs are supported only by 6.x firmware. These are defined under Wi-Fi Profiles > Access Control Policies.
☒ Enable Access Control
Access Control Policy
None

Legacy ACL
① Legacy ACLs are supported by both 4.x and 6.x firmware. For 6.x APs Policy Based ACLs are recommended.

Add New

Precedence...	Policy	Direction	Type	Rule	Description	Edit	Delete
No Rule Available							

MAC Authentication
Policy
☒ Deny ☐ Allow ☐ RADIUS ☐ cnMaestro

Add New

MAC	Description	Delete
No Rule Available		

☒ **DNS ACL**

Add New

Precedence...	Policy	Domain	Edit	De
No Rule Available				

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 26 Sample DNS-ACL configuration

WLANs > Ent_Access_Profile_6GHz														
Configuration Devices														
WLAN	DNS ACL <table> <tr> <th>Precedence</th><th>Policy</th><th>Domain</th></tr> <tr> <td>1</td><td>deny</td><td>*facebook.com</td></tr> <tr> <td>2</td><td>deny</td><td>*youtbe.com</td></tr> <tr> <td>256</td><td>permit</td><td>.*</td></tr> </table>		Precedence	Policy	Domain	1	deny	*facebook.com	2	deny	*youtbe.com	256	permit	.*
Precedence	Policy	Domain												
1	deny	*facebook.com												
2	deny	*youtbe.com												
256	permit	.*												
AAA Servers														
Guest Access														
Access Control														
Passpoint														
ePSK														

Fallback to WLAN VLAN when RADIUS-based MAC authentication fails

When a client passes RADIUS-based MAC authentication, the RADIUS server assigns the configured VLAN. However, if clients fail the authentication, you can configure the AP to assign the default WLAN VLAN. This enables the AP to allow limited access to clients, or redirects the clients to a captive portal page, that are not available in the RADIUS MAC authentication list. Once the captive portal authentication is successful, the RADIUS server dynamically disconnects the client and assigns the RADIUS VLAN when the clients try to connect later.

To assign the default WLAN VLAN to such clients, you must include the `mac-authentication radius failed-allow-traffic` CLI command in the **AP Groups > User Overrides** section in cnMaestro.

This feature is only available for RADIUS-based MAC authentication. The use case for this feature is to provide limited access to clients not included in the approved RADIUS MAC authentication list, such as granting access to a walled garden, the internet, or redirecting the clients to go through the captive portal authentication.

Figure 27 failed-allow-traffic in RADIUS-based MAC authentication

AP Groups > Add New	
Basic	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.
Management	
Radio	
Network	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.
Security	
Access Control	
Services	
User-Defined Overrides	<pre>! wireless wlan-1 mac-authentication radius failed-allow-traffic !</pre>

Passpoint

Below table lists configurable fields that are displayed in the **WLANs > Passpoint** tab.

Table 28 Passpoint parameters

Parameters	Description	Range	Default
Passpoint parameters			
Enable	Passpoint (Release 2) enables secure hotspot network access, online sign-up, and policy provisioning.	–	Disabled
DGAF	Downstream Group Addressed Forwarding when enabled the WLAN does not transmit any multicast and broadcast packets.	–	Disabled
ANQP Domain ID	ANQP domain identifier is included when the HS 2.0 indication element is in Beacon and Probe Response frames.	0-65535	0
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with Guest • Test • Wildcard	–	Private
ASRA	This indicates that the network requires a further step for access.	–	Disabled
Internet	The network provides connectivity to the Internet if not specified.	–	Disabled
HESSID	Configures the desired specific HESSID network identifier or the wildcard network identifier.	–	–
Venue Info	Configure venue group and venue type.	–	–
Roaming Consortium	The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.	–	–
ANQP Elements	Select any one of the following: • 3GPP Cellular Network Information • Connection Capability • Domain Name List • Icons • IP Address Type information • NAI Realm List	–	–

Parameters	Description	Range	Default
	• Network Authentication Type • Operating Class Indication • Operator Friendly Names • OSU Provider List • Venue Name Information • WAN Metrics		

Figure 28 Passpoint parameters

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Basic Settings

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

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

ANQP Domain ID
0

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

Comeback Delay
0

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

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

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

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

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

Venue Group
-- select -- Configure Venue group and Venue type

Venue Type
-- select --

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

[Add New](#)

Roaming Consortium
No Entries

ANQP (Access Network Query Protocol)

☒ 3GPP Cellular Network Information

☒ Connection Capability

☒ Domain Names

☒ NAI (Network Access Identifier) Realm List

☒ Operator Friendly Names

☒ IP Address Type Information

☒ Network Authentication

☒ Operating Class Indication

☒ Venue Name Information

☒ WAN Metrics

RADIUS attributes

The table below shows the RADIUS attributes describes their interpretation.

Table 29 Radius attributes parameters

Type	Attribute Name	Attribute Number	Purpose
Standard	Acct-Interim-Interval	85	Specifies the interval between accounting interim updates

Type	Attribute Name	Attribute Number	Purpose
Standard	Acct-Session-Id	44	Session identification (RFC 5176)
Standard	Calling-Station-Id	31	Session identification (RFC 5176)
Standard	Class	25	Accounting classification
Standard	Event-Timestamp	55	Replay protection (RFC 5176)
Standard	Filter-ID	11	- Assign station to a user group - Re-assign station to a different user group (RFC 5176)
Standard	Framed-IP-Address	8	Session identification (RFC 5176)
Standard	Idle-Timeout	28	Specifies the amount of time a station may remain idle before its session is terminated
Standard	NAS-IP-Address	4	NAS identification (RFC 5176)
Standard	NAS-Identifier	32	NAS identification (RFC 5176)
Standard	Session-Timeout	27	Specifies the interval at which session is terminated
Standard	Termination-Action	29	Specifies the action to take when the session is terminated
Standard	Tunnel-Type	64	Dynamic VLAN assignment (1 of 3 required), should be set to VLAN (Integer = 13)
Standard	Tunnel-Medium-Type	65	Dynamic VLAN assignment (2 of 3 required), should be set to 802 (Integer = 6)
Standard	Tunnel-Private-Group-ID	81	Dynamic VLAN assignment (3 of 3 required), should be set to the VLAN ID or name
Standard	User-Name	1	- Station username update - Session identification (RFC 5176)
Microsoft Vendor-Specific	MS-MPPE-Send-Key	16	Session key distribution
Microsoft Vendor-Specific	MS-MPPE-Recv-Key	17	Session key distribution
Cambium	Cambium-Vlan-	157	Radius based VLAN pool

Type	Attribute Name	Attribute Number	Purpose
Vendor-Specific	Pool-Id		
Nas Port ID	NAS-Port-Id	87	NAS identification (RFC 5176)

Enterprise PSK (ePSK)

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

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



Note:

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

Configuring ePSKs

To create an ePSK, complete the following steps:

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

The **Add ePSK** window is displayed.

9. Select **Mode** type as one of the following options and configure the corresponding parameters:

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

Add ePSK

Mode
☒ Single ☐ Bulk

User Name *

The number of characters allowed is between 1 and 31

Expiry by
None

Passphrase

The number of characters allowed is between 8 and 32

MAC Address

VLAN

VLAN ID should be in between 1 and 4094

Save



Note:

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

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

Add ePSK

Mode
☐ Single ☒ Bulk

Count*

This allows values between 2 and 2000

User Name Prefix*

Username and Passphrase will be auto generated i.e prefix-1

Expiry by
None

VLANs

Use comma "," separated VLANs. To provide a range use "-".

Save

WLANs > Default Enterprise

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

☐ Base WLAN for Personal Wi-Fi SSID **X**
Turning on this setting will disable this WLAN's SSID. Use the Wi-Fi AP device configuration tab i.e. Advanced Settings -> WLANs section to enable it with a personalized SSID name.

Mode
☒ Local ☐ RADIUS **X** Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected.

Passphrase Strength
☐ Easy ☒ Strong ☐ Number This allows Alphanumeric and Special Characters (up to 16 Characters)

Add New Import Export Delete

☐	User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN		
☐	admin	N/A	12345678	Wed, Aug 30, 2023	-	Active	N/A		
☐	test-1	N/A	#N\$V6i9YzAZBjHS*	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		
☐	test-10	N/A	<1LJhN8BtBgtap	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
☐	test-100	N/A	pH4cFsvF8a"Z"Rek	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
☐	test-1000	N/A	%j8JIBH5&[q4]	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
☐	test-101	N/A	uFdFA99>ZM16E%	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		
☐	test-102	N/A	kgwHF<T2yu2e:GS	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
☐	test-103	N/A	gy2mWfYjBjAE13fb	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		
☐	test-104	N/A	joch_~4jKRvUfJc	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	20		
☐	test-105	N/A	ZA6bSQ>8POTCp&n	Wed, Aug 30, 2023	Aug 30 2024 16:5...	Active	10		

Showing 1 - 10 Total: 1001 10 < Previous 1 2 3 4 5 ... 101 Next >

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



Note:

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

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

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

Expiry by

Date and Time 12/04/2024 03:05 PM

Set expiration time for the created ePSK. Expired ePSKs will not be pushed to the APs when the configuration is pushed manually or applied automatically by Auto Sync.

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

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

Expiry by Expiry in

Duration 1 Years

Set expiration time for the created ePSK. Expired ePSKs will not be pushed to the APs when the configuration is pushed manually or applied automatically by Auto Sync.



Note:

- The configured expiry time appears in the **Expiration Date** column on the **WLANs > <WLAN name>** page.

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

ePSK registration for WPA3 clients

For the ePSK feature, when you configure WPA3-WPA2 (mixed mode)-PSK or WPA3-PSK as the WLAN security, the clients connection in the WPA3 mode must go through an additional registration phase. This is different from the flow when you configure WPA2-PSK as the WLAN security, where users can authenticate by using only a passphrase.

When clients use WPA3-PSK security, Simultaneous Authentication of Equals (SAE) is the authentication mechanism where an extra authentication is added, which is more secure than WPA2. For WPA2-PSK clients, the passphrase is matched against a database to identify the user. However, this is not possible for WPA3-PSK clients because of the extra authentication in WPA3-SAE. When WPA2-PSK security is used, the Pairwise Master Key (PMK) is the same for every connection made by the client. This is due to the underlying weaknesses in WPA2-PSK, which make it easier to validate the passphrase. In contrast, when WPA3-PSK security is used, a new PMK is generated each time a client joins the network. Therefore, registration will help us to know the passphrase upfront when a client tries to connect. This mandates the users to register themselves with the ePSK passphrase to bind the client MAC with the passphrase to successfully connect to the Wi-Fi network.

For WPA3 clients to connect to the network using ePSK flow:

1. First connect to the WLAN with the WLAN passphrase.

A simple password is recommended to be configured, for example, `signmeup`, or any other appropriate passphrase.

2. Register themselves with the WPA3-ePSK unique passphrase.

After the MAC binding is complete, users can use the WPA3-ePSK unique passphrase for subsequent WLAN connections.

This section describes the following topics:

- [ePSK with WPA3 feature recommendations](#)
- [Scenarios while registering clients](#)
- [Enabling ePSK registration flow using the AP CLI](#)
- [Configuring ePSK registration for WPA3 clients](#)
- [Registration flow screenshots](#)
- [Recommended best practices](#)

ePSK with WPA3 feature recommendations

The following are the recommendations for this feature:

- This feature is supported only on cnMaestro Cloud 5.1.0 onwards.
- Supported AP firmware version is 6.6.1 or 7.0 and above.
- Security mode must be configured to either **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys**.
- APs must be managed from cnMaestro Cloud for client registration.
- The WLAN VLAN must be able to provide DHCP to clients and must have internet connectivity.
- This feature is not supported on Enterprise Wi-Fi 5 APs and Xirrus APs.

Scenarios while registering clients

When a client connects to the WLAN, the following scenarios are possible:

- When a client connects for the first time using WPA2 security and ePSK passphrase (either on 2.4 GHz or 5 GHz radios), the AP performs an ePSK lookup. The following are the outcome:
 - If a match is found, the MAC binding is created with the respective ePSK key.
AP shares this MAC binding information with the other APs in the network.
 - If a match is not found, the connection fails.
- If the WPA2 client is connected using the WLAN passphrase, client registration steps are performed to bind the passphrase to the client.
- When a client connects for the first time using WPA3 security, the following two possibilities may occur:
 1. If MAC binding is not available for the client on the AP, the following procedure must be completed for successful registration of clients:
 - a. User must authenticate using the configured *WLAN* passphrase, for example, *signmeup*.
If the user tries to sign in with some other password other than the configured *WLAN* password (*signmeup*), the connection fails.
 - b. If the connection with the configured password (*signmeup*) is successful, the AP redirects the client to the registration page.
This is the only traffic allowed for the client with this *WLAN* passphrase.
 - c. User must now enter the configured *ePSK* passphrase and register.
The AP redirects the client to the registration page with instructions.

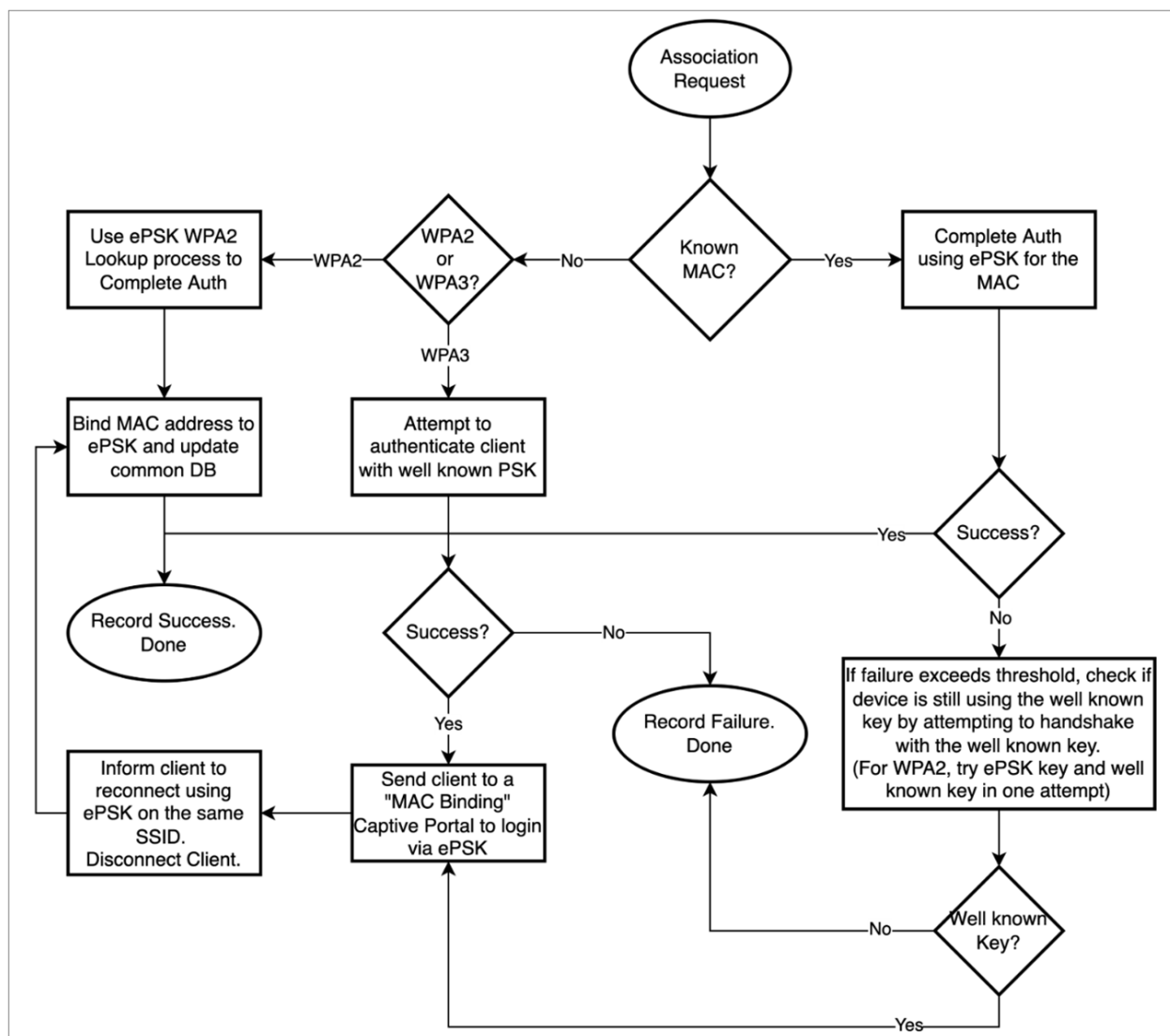
- d. Users must select the checkbox after reading the instructions (provided for different clients, such as Android, Windows, and iOS), and then disconnect from the network.
- e. User must forget the WLAN/SSID and reconfigure using the ePSK passphrase.

User then reconnects with ePSK passphrase and gets authenticated.

For a more detailed information, see [Registration flow screenshots](#).

2. When MAC binding is available for the client on the AP, users can authenticate the client with the passphrase present in the MAC binding, that is the ePSK passphrase.

Figure 29 Client registration flow for WPA3 clients



Enabling ePSK registration flow using the AP CLI

To enable ePSK registration for WPA3 clients in the AP CLI, execute the following commands:

```
ap(config)# wireless wlan 1
ap(config-wlan-1)# epsk-registration-flow
```

Configuring ePSK registration for WPA3 clients

To enable WPA3-ePSK registration, you must create a WLAN profile and add ePSK entries in the ePSK grid.

To create WLAN profile and add ePSK entries, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles** page.
 2. Select **WLANs** tab and click **Add**.
 3. Select **Enterprise Wi-Fi** from the **Type** drop-down list and configure the WLAN parameters.
 4. In the **Basic Settings** section, ensure either the **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option is selected in the **Security** drop-down list.
 5. Enter the WLAN passphrase.
 6. Click **Save**.
- When ePSK passphrase is not configured in the **WLANs > ePSK** page, the following message is displayed explaining the registration flow.

Figure 30 Message on the ePSK page when no ePSK entries are added

WLANs > Add New

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

☐ Base WLAN for Personal Wi-Fi SSID **x**
Turning on this setting will disable this WLAN's SSID. Use the Wi-Fi AP device configuration tab i.e. Advanced Settings -> WLANs section to enable it with a personalized SSID name.

Mode
☒ Local ☐ RADIUS **x** Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected.

Passphrase Strength
☐ Easy ☒ Strong ☐ Number This allows Alphanumeric and Special Characters (up to 16 Characters)

☐ This WLAN uses WPA3 security. Client registration flow is required and will be enabled when ePSK entries are added. Use the QR code to guide users for registering their clients. Note that the WLAN Passphrase will be used to verify that the client is attempting registration. Ensure that the client will get DHCP IP on the WLAN VLAN and will be able to reach cnMaestro Cloud.

Add New **Import** **Export** **Delete**

☐	User Name	MAC Address	Passphrase	Creation Date	Expiration Da...	Status	VLAN
No Data Available							

Showing 0 - 0 Total: 0 10 < Previous Next >

Save **Close**

- For existing WLANs where ePSK entries are present and when **WPA2/WPA3 Pre-shared Keys** or **WPA3 Pre-shared Keys** option is selected in the **Security** drop-down list, the following messages appear respectively

Figure 31 When **WPA3 Pre-shared Keys** option is selected

The screenshot shows the WLAN configuration interface. The 'SSID' section has 'Enable' checked and 'ePSK WPA3' entered. The 'Mesh' dropdown is set to 'Off'. The 'VLAN' is set to '1'. The 'Security' dropdown is set to 'WPA3 Pre-Shared Keys'. A message below the dropdown states: 'For best client experience with ePSK, use WPA2/WPA3-PSK or WPA2-PSK security mode. Registration flow is enabled for WPA3 clients. [Learn more](#) on how to enable WPA3 with ePSK.' The 'Passphrase' field contains 'wlanpassword' and is marked as hidden.

Figure 32 When **WPA2/WPA3 Pre-shared Keys** option is selected

The screenshot shows the WLAN configuration interface. The 'SSID' section has 'Enable' checked and 'ePSK WPA3' entered. The 'Mesh' dropdown is set to 'Off'. The 'VLAN' is set to '1'. The 'Security' dropdown is set to 'WPA2/WPA3 Pre-Shared Keys'. A message below the dropdown states: 'Registration flow for ePSK is enabled for WPA3 clients. [Learn more](#) on how to enable WPA3 with ePSK.' The 'Passphrase' field contains 'wlanpassword' and is marked as hidden.

7. Click the **ePSK** tab and add the passphrase.

After the ePSK passphrase is added, the following message is displayed explaining the registration flow.

Figure 33 Message on the ePSK page when ePSK entries are added

The screenshot shows the ePSK management page. At the top, there are radio buttons for 'Passphrase Strength': 'Easy', 'Strong' (selected), and 'Number'. A message box states: 'This WLAN uses WPA3 security. Client registration flow is active. Use the QR code to guide users for registering their clients. Note that the WLAN Passphrase will be used to verify that the client is attempting registration. Ensure that the client will get DHCP IP on the WLAN VLAN and will be able to reach cnMaestro Cloud.' Below the message is a table with columns: User Name, MAC Address, Passphrase, Creation Date, Expiration Date, Status, and VLAN. The table contains one entry for 'ePSK' with a status of 'Active'. At the bottom, it says 'Showing 1 - 1 Total: 1'.

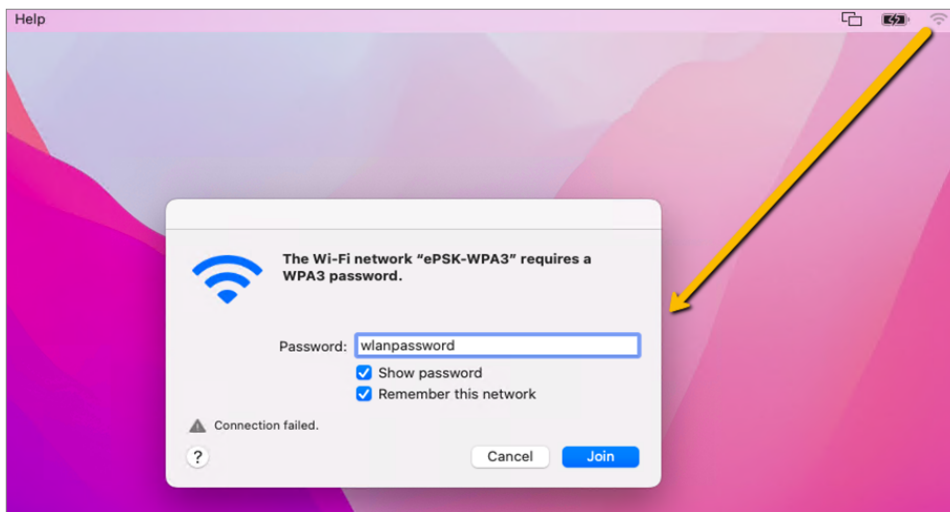
User Name	MAC Address	Passphrase	Creation Date	Expiration Date	Status	VLAN
ePSK	N/A	epskpassword@1234	Thu, Jun 13, 2024	Jun 13 2025 12:47:05	Active	1

Registration flow screenshots

To register the clients to the network using the ePSK passphrase, users must complete the following steps:

1. Connect the client to the network using the WLAN passphrase.

Figure 34 Using WLAN passphrase for connecting to network



2. Click **Join**.

Clients are redirected to the **Client Registration** page for providing the ePSK passphrase.

3. Enter the ePSK passphrase in the **Passphrase** field and click **Register**.

Figure 35 Using ePSK passphrase for client registration

The screenshot shows a web browser window titled "Join 'ePSK-WPA3'". Inside the window is a "Client Registration" form. The form has a "Passphrase*" label and a text input field containing "epskpassword@1234". Below the input field is a "Register" button. Underneath the button is a section titled "How to get passphrase?" with a paragraph of instructions. At the bottom of the browser window, the address bar shows the URL "qa-us-e1-guest.cloud.cambiumnetworks.com" and a "Cancel" button. A yellow arrow points to the address bar.

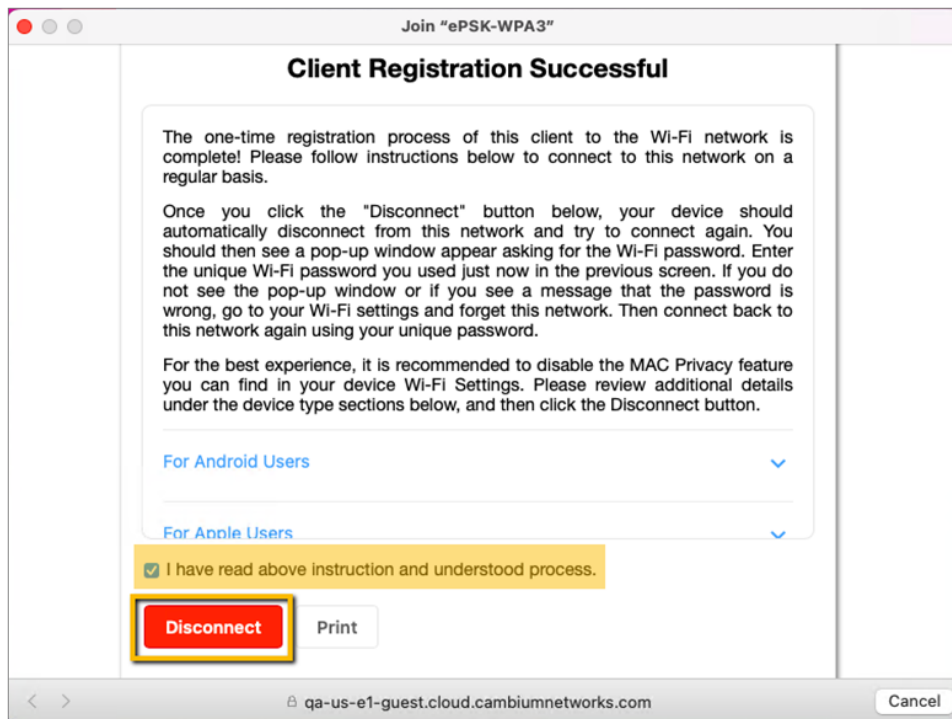
The registration success page is displayed along with a set of instructions.

4. Read the instructions (provided for different devices, such as Android, Windows, and iOS) and select the checkbox for confirmation.

The instructions provide details of the next steps for different devices.

The **Disconnect** button is enabled.

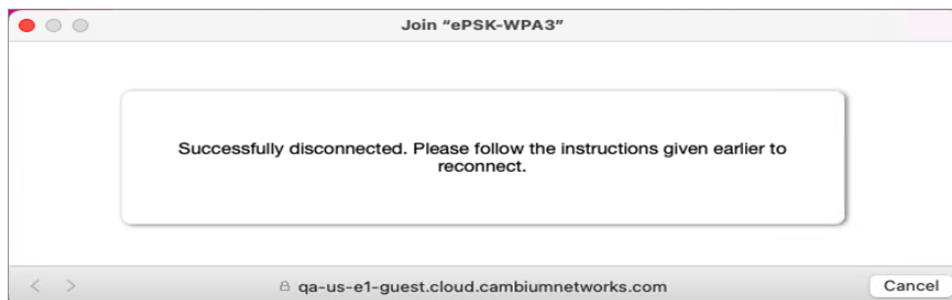
Figure 36 Registration success page with instructions



5. Click **Disconnect**.

The client is disconnected and a disconnect success message is displayed.

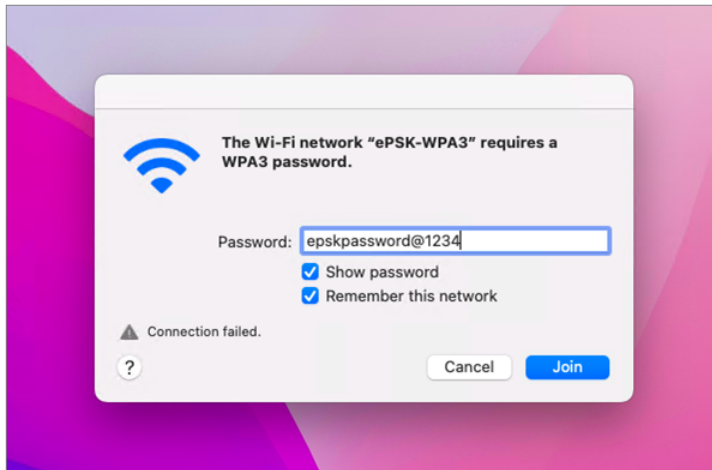
Figure 37 Disconnect success page



6. Reconnect to the network using the ePSK passphrase that you provided in the **Client Registration** page earlier.

The client connects to the network with the mapped VLAN.

Figure 38 Using ePSK passphrase for connecting to network



Recommended best practices

Following are some of the best practices you can follow while configuring ePSK registration for WPA3 clients:

- WPA3 PSK is not recommended for unmanaged (BYOD) clients (For example, multi-dwelling unit (MDU), hospitality, and educational institutions).

In MDUs, with IoT clients, making WPA3 mandatory with a single SSID may not be a successful deployment.

- WPA2/WPA3 PSK is recommended for unmanaged clients and to transition from the current (WPA2-PSK).
- Most of the WPA3-capable clients favor WPA3 PSK when available. This behavior is different among other clients, where some fallback to WPA2 and some which do not.
- When the SSID is mapped to 2.4 GHz and 5 GHz radios, WPA2 PSK or WPA2/WPA3 PSK security is recommended.
- When the SSID is mapped to 2.4 GHz, 5 GHz, and 6 GHz radios, or only the 6 GHz radio, then WPA3 PSK security is recommended.

Creating a Personal Wi-Fi ePSK



Note

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

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

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

1. Add and enable the SSID details (to be used as personal Wi-Fi) in the **WLANs** tab, under **Manage and Operation > Networks > <network name> > Configuration > Device Configuration > Advanced Settings** section.
 - a. Select the **Enable SSID** checkbox.
 - b. In the **Passphrase** field, configure the passphrase.
 - c. Configure the VLAN with which the SSID must be associated.
2. Enable personal Wi-Fi on the ePSK page for the WLAN profile by selecting the **Base Personal SSID** checkbox.

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

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

RADIUS-based ePSK Premium feature

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

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



Note

ePSK feature is not supported with WPA3.

Configuring RADIUS-based ePSK

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

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

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

☐ **Base WLAN for Personal Wi-Fi SSID X**
Turning on this setting will disable this WLAN's SSID. Use the Wi-Fi AP device configuration tab i.e. Advanced Settings -> WLANs section to enable it with a personalized SSID name.
Mode
☐ Local ☒ **RADIUS X** Configure LOCAL DB based ePSK or RADIUS based ePSK. Please configure AAA server when RADIUS based ePSK is selected.

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

WLANs > Add New

WLAN
AAA Servers
Guest Access
Access Control
Passpoint
ePSK

Warning: AAA Servers are configured separately for each WLAN.

Authentication Server

Host	Secret	Port*	Realm
1. Host eg. xxx.xurp	Show	1812	
2. Host eg. xxx.xurp	Show	1812	
3. Host eg. xxx.xurp	Show	1812	

Timeout: Timeout in seconds for each request attempt (1-30)

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

Accounting Server

Host	Secret	Port*
1. Host eg. xxx.xurp	Show	1813
2. Host eg. xxx.xurp	Show	1813
3. Host eg. xxx.xurp	Show	1813

Timeout: Timeout in seconds for each request attempt (1-30)

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

Accounting Mode: Configure accounting mode

☐ Accounting Packet Enable Accounting On messages

☐ Sync Accounting Records Configure accounting records to be synced across neighboring APs

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

Advanced Settings

Server Pool Mode

☒ Load Balance Load balance requests equally among configured servers

☐ Failover Move down server list when earlier servers are unreachable

NAS-Identifier: NAS-identifier attribute for use in Request packets (defaults to system name)

☐ Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)

☒ Dynamic VLAN Enable RADIUS assigned VLANs

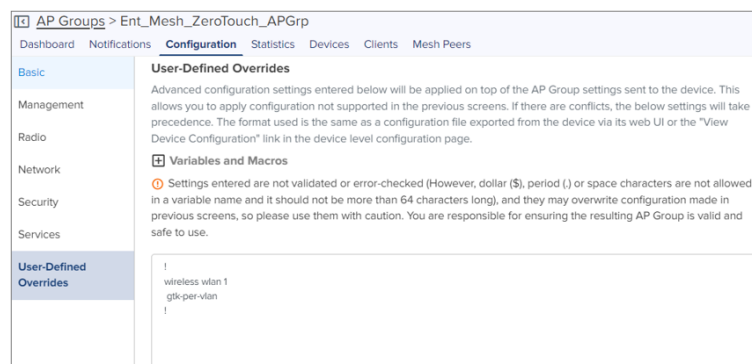
Called Station ID: Configure AP-MAC:SSID as Called-Station-Id in the RADIUS packet

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

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
!
```

Dynamic ARP Inspection

Dynamic ARP Inspection detects and prevents ARP spoofing by validating ARP packets against a trusted IP-to-MAC address mapping. When a client sends an ARP packet, such as one claiming to be the gateway, the system checks whether the claimed IP matches the client's registered IP in the wireless client table. If there's a mismatch, the packet is identified as spoofed and is dropped. Gateway IPs are learned dynamically from DHCP packets (router option) during client associations, allowing the system to build a mapping table for validation. It does not track gateway MAC addresses, as IP validation is sufficient for detecting spoofing.

Spoofed ARP events are logged and visible via CLI commands, such as `show events` and `show wireless spoofed-arp-stats`.

This feature is available only as CLI command that you can configure in the **AP Groups > User Overrides** section in cnMaestro. A sample configuration snippet is shown below:

```
!
wireless wlan 1
dynamic-arp-inspection
!
```

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 configuration parameters related to LAN, VLAN, Routes, DHCP server, ACL, and Firewall.

Configuring Network parameters

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

- [VLAN](#)
- [Routes](#)
- [Ethernet Ports](#)
 - [Port Control—802.1X Authentication](#)
- [DHCP](#)
- [Tunnel](#)
- [PPPoE](#)
- [VLAN Pool](#)

IPv4 network parameters

VLAN



Note

By default, the XRP messages are sent through the native VLAN. From release version 6.6.2 onwards, a new CLI command (`roam management-vlan`) is added to enable XRP messages to be sent through any VLAN other than the native VLAN. When configured, the roaming VLAN must have an L3 interface on the AP.

To configure network parameters, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Network** tab > **VLANs** section.

Figure 39 *Network > VLANs section*

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control

VLANs

Add New

VLANs	IPv4	NAT	Zeroconf IP	Management Access	DHCP Relay Agent	IPv6
1	dhcp	disable	enable	Allow from Wired and Wireless	Disabled	

10 • < Previous 1 Next >

4. Click **Add New** and configure the IPv4 parameters described in the following table.

Table 30 *VLAN IPv4 parameters*

Parameters	Description	Range	Default
VLAN > IPv4			
Address	Provision to configure the mode of IPv4 address configuration for an interface selected. Two modes are supported: • DHCP—This is the default mode in which the Enterprise Wi-Fi AP device tries to obtain an IPv4 address from the DHCP server. • Static IP—Users must explicitly configure the IPv4 address and Netmask for a VLAN selected.	—	DHCP
NAT	This option enables wireless traffic gets NAT'ed with APs respective uplink interface IP. This option is recommended when DHCP pools are configured in AP.	—	Disabled
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only in the VLAN1 configuration section. If VLAN 1 is not allowed in Ethernet interfaces, this IP will not be accessible.	—	Enabled
DHCP Relay Agent	This option is enabled when DHCP server is hosted on a VLAN which is not same as client that is requesting the DHCP IP. Enabling this appends Option 82 in the DHCP packets. Following information is allowed to configure: • DHCP Option 82 Circuit ID Configurable parameters under this option are as follows: ◦ Hostname ◦ APMAC ◦ BSSID ◦ SSID ◦ Custom	—	Disabled

Parameters	Description	Range	Default
	• DHCP Option 82 Remote ID Configurable parameters under this option are as follows: ◦ Hostname ◦ APMAC ◦ BSSID ◦ SSID ◦ Custom  Note In case DHCP Option 82 is configured at the device-, WLAN profile-, and L3 interface-levels, the following priority order is considered: 1. Device-level configuration 2. WLAN profile-level configuration 3. L3 interface-level configuration		
Request Option All	This configuration decides the interface on which Enterprise Wi-Fi AP will learn the following: • IPv4 default gateway • DHCP client options like Option 43 and Option 15 (Controller discovery like controller host name / IPv4 address) • DNS Servers • Domain Name	–	Enabled on VLAN1

Figure 40 VLAN IPv4 parameters

Add VLAN

VLAN ID

1

Please enter VLAN ID (1 to 4094)

IPv4

IP Address

☒ DHCP
 ☐ Static IP

xxxxxx.xxxx.xx

xxxxxx.xxxx.xx

Netmask

xxxxxx.xxxx.xx

NAT

When NAT is enabled, IP addresses under this Switched Virtual Interface are hidden

Zeroconf IP Support 169.254.x.x local IP address

DHCP Relay Agent

xxxxxx.xxxx.xx

Enable relay agent and assign DHCP server

DHCP Option 82 Circuit ID

None

DHCP Option 82 Remote ID

None

Request Option All

Enable DHCP request option all on this interface

IPv6

General

Add

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 31 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

Options	Description	Usage	Reference CLI
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.	<code>show ip name-server</code>
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.	<code>show ip dhcp-client info</code>
Option 26	This option specifies MTU size in a network.	More details are provided in Configuring the Network .	<code>show ip dhcp-client info</code>
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	<code>show ip dhcp-client-info</code>
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).	<code>show ip dhcp-client info</code>
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.	<code>show ip dhcp-client info</code>
Option 54	DHCP clients use the contents of the server identifier field as the destination address for any DHCP messages unicast to the DHCP server.	Enterprise Wi-Fi AP learns DHCP server IP for all VLAN interfaces configured.	<code>show ip dhcp-client info</code>
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.	<code>show ip dhcp-client info</code>

DHCP Option 43—Zero-touch onboarding

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

This option is used to learn HTTPS proxy server address from the DHCP server as well.

DHCP Option 43 format

If HTTP proxy needs to be configured, then the following format must 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 URL configuration is needed then Option 43 payload can contain only that too without key-value format as described above.

Routing and DNS

Table 32 AP Groups > Network > VLAN > Routes > IPv4 Routing and DNS 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. Note DNS Proxy is allowed only when NAT mode is enabled for the WLAN.	–	Disabled

Figure 41 IPv4 Routing and DNS parameters

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Routes

☒ **IPv4 Routing and DNS**

Default Gateway
 IP address of default gateway

Domain Name
 Domain name

DNS Server 1
 Primary domain name server

DNS Server 2
 Secondary domain name server

☐ DNS Proxy

Routes

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

Table 33 IPv4 Gateway Source Precedence, Route entries, and Port forwarding parameters

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

Figure 42 IPv4 Gateway Source Precedence, Route entries, and Port forwarding parameters

IPv6 network parameters

VLAN

Table 34 VLAN IPv6 parameters

Parameters	Description	Range	Default
Address	Provision to configure the mode of IPv6 address configuration for an interface selected. Five modes are supported: - Disabled - AutoConfig - Static - Stateless DHCPv6 - Stateful DHCPv6	–	AutoConfig
Request Option All	This configuration decides the interface on which AP will learn the following: IPv6 default gateway	–	Enabled on VLAN1

Parameters	Description	Range	Default
	- DHCP client options like Option 52 and Option 24 (Controller discovery like controller hostname / IPv6 address) - DNS Servers - Domain Name		

Figure 43 VLAN IPv6 parameters

The screenshot shows a web-based configuration window titled "Add VLAN" with a close button (X) in the top right corner. Inside the window, there is a "VLAN ID" input field with a placeholder text "Please enter VLAN ID (1 to 4094)". Below this, there are two expandable sections: "IPv4" (collapsed) and "IPv6" (expanded). The "IPv6" section contains a "Mode" dropdown menu set to "Static", an "IPv6 Address" input field, and a "Prefix Length" input field. Below these fields is a checkbox labeled "Request Option All" with a subtext "Use IPv6 Gateway, DNS, DHCPv6 options received on this interface". At the bottom of the "IPv6" section is a "General" section (collapsed). A blue "Add" button is located at the bottom right of the window.

Routing & DNS

Table 35 IPv6 Routing and DNS 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

Figure 44 IPv6 Routing and DNS parameters

Routes

Table 36 IPv6 Gateway Source Precedence and Multiple Route Entries 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: - Destination IP/prefix - Gateway	—	—

Figure 45 IPv6 Gateway Source Precedence and Multiple Route Entries parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Routes

- IPv4 Routing and DNS
- IPv6 Routing and DNS
- IPv4 Gateway Source Precedence
- IPv6 Gateway Source Precedence**

1 Static

2 Auto-config/DHCPv6

IPv4 Multiple Route Entries

IPv6 Multiple Route Entries

Add New

Destination IP	Gateway
No Multiple Routes configured	

Port Forwarding

General network parameters

Table 37 VLAN - General parameters

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

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

Figure 46 VLAN - General parameters

Add VLAN

VLAN ID

Please enter VLAN ID (1 to 4094)

☐ IPv4

☐ IPv6

☒ **General**

Management Access

Allow from Wired and Wireless

CLI/GUI/SNMP access via this interface

Add

Ethernet Ports

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

Table 38 Ethernet Ports 1 to 4 parameters

Parameters	Description	Range	Default
Ethernet Port <1-4>	Enterprise Wi-Fi AP devices Ethernet port is provisioned to operate in the following modes: Access Single VLAN—Single VLAN traffic is allowed in this mode. Trunk Multiple VLANs—Multiple VLANs are supported in this mode.	–	Access Single VLAN
VLAN	VLAN ID to be associated with the Ethernet port.	1 to 4094	1
Port Speed	Specifies the port speed in Mbps. Following values are supported: - Auto 10 Mbps 100 Mbps 1000 Mbps 2500 Mbps 5000 Mbps	–	Auto
Port Duplex	Specifies the type of duplex communication configured for the port.	–	Full Duplex

Parameters	Description	Range	Default
	Following values are supported: • Full Duplex • Half Duplex		
Tunnel Mode	Only applicable for Ethernet ports 2, 3, and 4. Specifies whether tunneling of wired traffic is enabled or not.		

Figure 47 Ethernet Ports parameters

Port Control—802.1X Authentication

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



Note

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

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

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

Table 39 RADIUS Server parameters

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

Parameters	Description	Range	Default
	• Secret—Text string that is used to encrypt data in RADIUS packets shared between the AP and the sever. Format—Text string • Port—Port number of the accounting server. Default—1813 A maximum of three RADIUS accounting servers can be configured.		
Timeout	Time (in seconds) to wait for a response from the RADIUS server.	1–30	3
Attempts	Number of retry attempts for contacting the RADIUS server.	1–3	1
Accounting Mode	Specifies the accounting mode to be used. The following modes are supported: • Start-Stop—Accounting packets are transmitted by APs to the AAA server when a wireless client is connected and when the client disconnects. • Start-Interim-Stop—Accounting packets are transmitted by APs to the AAA server when a wireless client connects, then at regular intervals (configured in the Interim Update Interval field) and also when the client disconnects. • None—Disables the accounting mode. This is the default mode.	-	None (Disabled)
Server Pool Mode	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode. • Load Balance—AP equally distributes the requests between the configured RADIUS servers, • Failover—AP selects the RADIUS server that is functional based on the order of configuration.	-	Failover
Interim update interval	Time (in seconds) to wait for sending RADIUS interim accounting update packets. Note: This interval is applicable only when you select the Start-Interim-Stop option in the Accounting Mode parameter.	10–65535	1800
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled

Figure 48 RADIUS Server parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

RADIUS Server

Authentication Server

1. Host Secret Port*
2. Host Secret Port*
3. Host Secret Port*

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

Accounting Server

1. Host Secret Port*
2. Host Secret Port*
3. Host Secret Port*

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

Accounting Mode

None Configure accounting mode

Server Pool Mode

☒ Load Balance Load balance requests equally among configured servers
☐ Failover Move down server list when earlier servers are unreachable

Interim Update Interval

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

☒ Dynamic Authorization Enable RADIUS dynamic authorization (COA, DM messages)

DHCP

Below table lists the fields that are displayed in the **AP Groups > Network > DHCP** page.

Figure 49 DHCP Pool parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control

DHCP Pool

Add New

DHCP Pool	Address Range	Default Router	Domain Name	DNS Address	Network	Lease
No DHCP Pool configured						

Table 40 DHCP parameters

Parameters	Description	Range	Default
DHCP Pool	Specifies the DHCP pool ID.	1 to 16	–

Parameters	Description	Range	Default
Address Range	Indicates the start and end addresses for the DHCP Pool.	–	–
Default Router	Specifies the default router IP address.	–	–
Domain Name	Specifies the domain name for the DHCP pool.	–	–
DNS Address	Specifies the primary and secondary addresses of the DNS server for a DHCP pool.	–	–
Network	Specifies the network IP address and subnet mask for the DHCP pool.	–	–
Lease	Duration (in days, hours, and minutes) for which the IP address must be leased to the client.	–	1 day
Add Bind List			
	For every DHCP pool configured, the user can bind MAC and IP from the address pool defined, so that the wireless station gets the same IP address every time they connect. Following parameters are required to bind IP address: • MAC Address • IP Address	–	–

Figure 50 Add DHCP window

The screenshot shows the 'Add DHCP' configuration window. It includes the following sections and fields:

- DHCP Pool:** A text field for 'Pool Number'.
- Address Range:** Two text fields for 'Start' and 'End' IP addresses.
- Default Router:** A text field.
- Domain Name:** A text field.
- DNS Address:** Two text fields for 'Primary' and 'Secondary' addresses.
- Network:** Two text fields for 'IP' and 'Mask'.
- Lease:** Three text fields for 'Lease' time in 'Days', 'Hours', and 'Minutes'.
- Bind List:** A section with two text fields for 'MAC' and 'IP' addresses, and an 'Add' button.
- Footer:** A message 'No Bind List configured' and an 'Add' button.

Tunnel

The following table lists the fields that are displayed in **AP Groups > Network > Tunnel** page.

Figure 51 Tunnel - L2TP parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Tunnels

Basic Settings

Tunnel Encapsulation

L2TP

L2TP

Remote IP

IP address or domain

Username

admin

Password

.....

Show

Authentication Type

Default

TCP MSS

1400

☒ TCP Maximum Segment Size (422-1410 bytes)

☒ PMTU Discovery Enable Path Maximum Transmission Unit discovery to avoid IP fragmentation

L2GRE

Figure 52 Tunnel - L2GRE parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

Tunnels

Basic Settings

Tunnel Encapsulation

L2GRE

L2TP

L2GRE

Remote IP

IP address or domain

DSCP

0

Differentiated Service Code Point

TCP MSS

1410

☒ TCP Maximum Segment Size (472-1460 bytes)

☒ PMTU Discovery Enable Path Maximum Transmission Unit discovery to avoid IP fragmentation

MTU

1460

Configure MTU for L2GRE tunnel (850-1460 bytes)

☐ Cambium GRE Enable Cambium Generic Routing Encapsulation

☐ GRE in UDP Enable GRE in UDP encapsulation

Table 41 Tunnel parameters

Parameters	Description	Range	Default
Tunnel Encapsulation	Provision to enable tunnel type. Following tunnel types are supported by Enterprise Wi-Fi AP devices: • L2TP • L2GRE • OFF	–	OFF
L2TP			
Remote IP	Configure L2TP end point. IPv4 address or Primary hostname of the endpoint is supported.	–	–
Username and Password	Credentials required for L2TP authentication.	–	admin/admin
Authentication Type	Provision to select the PPP authentication method. Following are the options available: • DEFAULT • CHAP • MS-CHAP • MS-CHAPv2 • PAP	–	DEFAULT
TCP MSS	TCP Maximum Segment Size (MSS) in bytes.	422- 1410	1400
PMTU Discovery	Provision to enable to discover PMTU in network.	–	Enabled
L2GRE-1 You can configure a maximum of two L2GRE tunnels. Configure L2GRE-1 tunnel by configuring the below parameters in the AP Groups > Network > Tunnel tab. However, configuring L2GRE-2 tunnel is allowed only using the device CLI. The following parameters for L2GRE-1 are also applicable for L2GRE-2.			

Parameters	Description	Range	Default
Remote IP	Configure L2GRE endpoint. IPv4 address or primary hostname of an endpoint is supported.	–	–
DSCP	Users can configure priority of GRE packets.	–	0
TCP MSS	TCP Maximum Segment Size (MSS) in bytes.	472-1460	1410
PMTU Discovery	Provision to enable to discover PMTU in a network.	–	–
MTU	Maximum Transmission Unit in bytes.	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

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 **AP Groups > Network > PPPoE** page.

Figure 53 PPPoE parameters

AP Groups > Add New

Basic
Management
Radio
Network
Security
Access Control
Services
User-Defined Overrides

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

Table 42 PPPoE parameters

Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disabled
VLAN ID	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.	–	admin/admin
MTU	Maximum Transmission Unit.	500-1492	1492
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

VLAN Pool

The following table lists the fields that are displayed in **AP Groups > Network > VLAN Pool** page.

Table 43 The VLAN Pool parameters

Parameters	Description	Range	Default
VLAN Pool Name	Name for the VLAN pool.	–	–
VLAN ID List	List of VLAN IDs for the VLAN pool. You can configure either a single VLAN ID or multiple VLAN IDs. Multiple VLAN IDs can be configured either separated by comma or hyphen. For example, 2-7, 45, 67.	–	–

Figure 54 The VLAN Pool parameters

AP Groups > Add New

Management
Radio
Network
Security
Access Control
Services

☐ VLAN Pool

Add New

VLAN Pool Name	VLAN ID List
----------------	--------------

No VLAN Pool configured

Configuring Access Control

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

Figure 55 Access Control page

The screenshot shows the 'Access Control' page in a management interface. The left sidebar contains a navigation menu with options: Basic, Management, Radio, Network, Security, **Access Control**, Services, and User-Defined Overrides. The main content area is titled 'AP Groups > GE_TEST' and includes tabs for Dashboard, Notifications, Configuration (active), Statistics, Reports, Devices, Clients, and Mesh Peers. The 'Access Control' section is expanded, showing three sub-sections: 'Access Control' with an 'Enable Access Control' checkbox and a dropdown for 'Access Control Policy' (set to 'None'); 'User Group Policy' with an 'Apply Filter(s)' button and a table with columns 'Policy Name', 'RADIUS Filter-ID', 'Access Control Policy', and 'VLAN'; and 'Device Policy' with an 'Apply Filter(s)' button and a table with columns 'Policy Name', 'Device Class', 'Device Type', and 'Access Control Policy'. Both tables show 'No Data Available'. At the bottom of each table, there is a pagination bar indicating 'Showing 0 - 0 Total: 0 10' and navigation links for 'Previous' and 'Next'.



Note

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

This chapter describes the following topics

- [Enabling Access Control Policy](#)
- [User Group Policy](#)
- [Device Policy](#)

Enabling Access Control Policy

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

Figure 56 Enabling Access Control Policy

The screenshot shows the 'Access Control' section of the management interface. It includes a checkbox labeled 'Enable Access Control' which is checked. Below it is a dropdown menu for 'Access Control Policy' with the value 'test' selected. To the right of the dropdown is a button labeled 'View Rules' which is highlighted with a red border.

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

Figure 57 Access Control Policy Rules

Name	Status	Action	Type	Application / Category	Protocol	Source IP Mask	Destination IP Mask	Schedule
lperf_app	Enabled	Allow	Layer7-filter	lperf	-	-	-	-
speedtest_APP	Enabled	Allow	Layer7-filter	speedtest.net	-	-	-	-
allow_instagram	Enabled	Allow	Layer7-filter	Instagram	-	-	-	-
ap_gp_deny_ndtv	Enabled	Deny	Layer7-filter	NDTV	-	-	-	-
Ap_Gp_allow_whatsapp	Enabled	Allow	Layer7-filter	WhatsApp	-	-	-	-
Ap_GP__Allow_Facebook	Enabled	Allow	Layer7-filter	Facebook	-	-	-	-

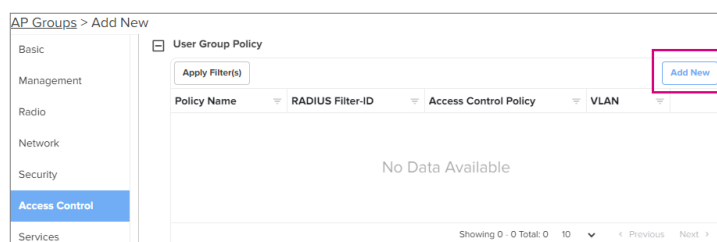
User Group Policy

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

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

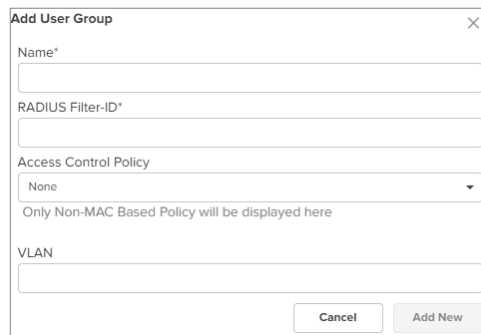
1. Navigate to **Configuration** > Wi-Fi Profiles > AP Groups > **Access Control** page.
2. Click **Add** to create a new AP group.
3. Click the **Access Control** tab in the **Add New** page.
4. Click **Add New** in the **User Group Policy** section.

Figure 58 User Group Policy



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

Figure 59 Add User Group



The 'Add User Group' dialog box contains the following fields and controls:

- Name***: A text input field.
- RADIUS Filter-ID***: A text input field.
- Access Control Policy**: A dropdown menu with 'None' selected. Below it, a note states: 'Only Non-MAC Based Policy will be displayed here'.
- VLAN**: A text input field.
- Buttons**: 'Cancel' and 'Add New' buttons at the bottom right.



Note

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

Device Policy

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

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

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

Figure 60 Device Policy

AP Groups > Add New

Management
Radio
Network
Security
Access Control
Services
User-Defined
Overrides

Device Policy

Apply Filter(s)

Policy Name Device Class Device Type Access Control Policy

No Data Available

Showing 0 - 0 Total: 0 10 < Previous Next >

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

Figure 61 Add Device Policy

Add Device Policy

Name*

Device Class* Device Type*

Any Any

Access Control Policy*

None

Only Non-MAC Based Policy will be displayed here

Cancel Add New



Note

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

Managing Filters

This chapter describes the following topics:

- [Overview](#)
- [Filter list](#)
- [Device class filter](#)
- [Wi-Fi Calling support](#)
- [Air cleaner](#)
- [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).

```
ap(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:

```
ap(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.

```
ap(config-filter-list-1)# filter precedence {1-50}
```

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

```
(config-list-1-filter-precedence-1)# exit
(config-filter-list-1)# filter precedence 1
(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.

```
(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

```
(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.

```
(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-protocol or port number-based rules, select IP.

```
(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:

```
(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.

```
(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. ap(config-list-1-filter-precedence-1) # layer2-filter permit mac

```
(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 !1.1.1.1/8 any any
```

12. ap(config-list-1-filter-precedence-1) # layer2-filter permit proto

```
(config-list-1-filter-precedence-1)# layer2-filter permit proto  
  
layer2-filter permit proto (tcp|udp|arp|icmp|igmp|srp|sctp|any) (SOURCE-MAC/IPv4/IPv6[{mask|prefix-length}]|any) (SOURCE-PORT|any) (DESTINATION-MAC/IPv4/IPv6[{mask|prefix-length}]|any) (DESTINATION-PORT|any) (in|out|any) <(optional)//Filter_name>
```

Example:

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

Sample configuration

```

filter global-filter
  stateful
  application-control

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

```

13. To attach the filter list into the WLAN profile, filter-list < filter-list ID>.

```

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

```

14. To show filter statistics:

```

(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:

```

ap(config)# device-class-filter 1
ap(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
ap(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
ap(config-device-class-filter-1)# class notebook linux
ap(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:

```

ap(config)# filter global-filter
ap(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:

```
ap(config-global-filter)# air-cleaner all
ap(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.

This topic describes the following content:

- [Deep Packet Inspection \(DPI\)](#)
 - [Application control policy](#)
 - [Risk and productivity](#)
 - [Selection criteria](#)
 - [DPI CLI configuration](#)
 - [Global application policy](#)
 - [SSID application policy](#)
- [Custom Applications X](#)

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).

```
(config)# show application-statistics by-application
```

Applications Count = 24

Application Statistics for All Applications

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

```
ap(config)# show application-statistics by-category
```

Application Category Statistics for All Applications

```
=====
```

Application	Productivity Index & Risk	TX Packets	TX Bytes	RX Packets	RX 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.

```
ap(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.

```
(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 & 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.

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

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

MAC	IP	VLAN	SSID
	10.10.0.113	1	TIGER_XV3_8_OPEN_SSID

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

VLAN	STA_COUNT
1	1

```
ap(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
------	-----------

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

```
(config)# show application-statistics by-application vlan 1
```

Applications Count = 24

Application Statistics for VLAN 1

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	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

```
ap(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).

```
(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

```
ap(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
```

```
ap(config)#
```

DPI CLI configuration

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

To enable DPI support:

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

To disable DPI support:

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

Global application policy

Per application policy

```
(config)# filter global-filter
(config-global-filter)# filter precedence 1
(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

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

SSID application policy

```
ap(config)# filter filter-list 1
ap(config-filter-list-1)# filter precedence 1
ap(config-list-1-filter-precedence-1)# application-control facebook deny
ap(config-list-1-filter-precedence-1)#
ap(config-list-1-filter-precedence-1)# wireless wlan 1
ap(config-wlan-1)# filter-list 1
ap(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
!
(config-filter-list-1)#

```

Custom Applications X

Custom applications allow you to configure applications with a specific IP address or a domain name, and apply filter rules, such as enable or disable traffic from these applications. By default, these applications are applied on the devices along with the AP group configuration.

After creating the custom application, when you click **Apply**, cnMaestro creates a job for devices in the AP group that has auto sync enabled. Devices in AP groups that do not have auto sync enabled, are marked as **Not in Sync**, and users must manually apply the configuration on to the devices.

To disable cnMaestro from applying the custom application configuration on the devices, clear the **Enable Custom Application** check box from the **AP Groups > Services** tab > **Application Visibility X** section.

To add a new custom application, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > Custom Applications X**.

Configuration > Wi-Fi Profiles

AP Groups WLANs Association ACL Access Control Policies **Custom Applications X**

ⓘ Configure Custom Applications corresponding to an FQDN or IP Address to capture statistics or control web access. Applications are pushed to the devices along with AP Groups by default. After creating them, click the Apply button to create Auto Sync Jobs for devices under AP Groups with Auto Sync enabled. Devices under AP Groups without Auto Sync enabled will be marked as Not in Sync, and configuration needs to be pushed manually. Disable the flag "Enable Custom Application" from AP Group -> Services Tab to stop applying them.

Apply Filter(s) Managed Account: All Accounts Add New Import Delete Export

☐ Application Name	Managed Account	☐ Enabled	Category	Productivity Index ⓘ	Risk Index ⓘ	FQDN/IP Address	
☐ test	Base Infrastructure	☐ Disabled	Remote Access	Medium	High	5.6.7.8	
☐ hghkhsdckjldkj	Base Infrastructure	☒ Enabled	Streaming Media	Medium	High	3.3.3.3	
☐ test_test	Base Infrastructure	☒ Enabled	Custom	Low	Low	1.1.1	

Showing 1 - 3 Total: 3 10 < Previous 1 Next >

2. Click **Add New** on the **Custom Applications X** page.

The **Add Custom Application(s)** window is displayed.

Add Custom Application(s)

ⓘ This interface allows to add multiple custom applications, which will be saved and pushed to the device.

Name*

Scope
Base Infrastructure
Category*
Custom
FQDN/IP Address*
Productivity Index*
Low
Risk Index*
Low
Add
No Data
Cancel
Save and Apply

Configure the following parameters:

Table 44 Custom Application Parameters

Parameter	Description
Name	Specifies the name for the custom application. Supports a maximum of 20 characters.
Scope	Specifies the availability of the custom application across managed accounts. The following values are supported: - Base Infrastructure—Custom application is available only for the global account. It is not shared with other managed accounts. - Shared—Custom application is shared across all managed accounts. It can be mapped to devices in the managed account, but it cannot be modified. To modify the configuration, it must be copied into the managed account and then updated. - Managed Account—Custom application is available only for that specific managed account.  Note Once the scope has been configured on a custom application, it cannot be modified.
Category	Specifies the category to which the application must belong. Select the appropriate category from the drop-down list.
FQDN/IP Address	Specifies the IPv4 address or the domain name of the custom application.
Productivity Index	Indicates how appropriate an application is useful for business purposes. The higher the rating number, the more business-oriented an application is.

Table 44 *Custom Application Parameters*

Parameter	Description
Risk Index	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.
Enable	Select the check box to enable this custom application.

3. Click **Add**.
4. To apply this configuration on the AP, click **Save and Apply**.

**Note**

WIDS and WIPS are beta features.

This section describes the following topics:

- [Wireless Intrusion Detection Systems \(WIDS\)](#)
 - [Wireless flood detection](#)
 - [Neighbor AP detection](#)
 - [Rogue APs](#)
 - [Honeypot APs](#)
 - [Ad Hoc network detection](#)
 - [Wired Devices](#)
 - [Configuring WIDS](#)
- [Wireless Intrusion Prevention System \(WIPS\)](#)

Wireless Intrusion Detection Systems (WIDS)

Wireless Intrusion Detection Systems (WIDS) is a powerful feature within cnMaestro that helps administrators monitor and protect their wireless networks from unauthorized access and potential security threats. WIDS works by continuously scanning the wireless spectrum to detect and mitigate potential intrusions, ensuring the integrity and security of your network infrastructure.

Wireless flood detection

Wireless flood detection helps in identifying and mitigating flood attacks in wireless networks. A flood attack occurs when a rogue client sends a large number of packets of a specific type to the AP to disrupt the normal working of the AP. This feature can detect the following types of flood attacks:

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

CLI configuration:

```
ap(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
```

Neighbor AP detection

The AP can detect all neighbor APs. By default, all neighbors in the home channel are detected. To detect neighbors in all channels, go to **Radio > Basic > Off Channel Scan** and select the **Enable** check box.

Rogue APs

Rogue APs are unauthorized APs that are not onboarded to cnMaestro, which may include Cambium or non-Cambium devices causing interference. The authorized or onboarded APs scan all available channels and collect details about neighboring APs. They send this information to cnMaestro for monitoring and management.

CLI configuration:

To enable rogue AP detection:

```
ap(config)# wids
rogue-ap-detection : Enable unsanctioned AP detection
```

Honeypot APs

Honeypot APs are unauthorized APs that advertise the same SSID as managed or onboarded APs. Detecting and monitoring these APs is crucial to prevent threats to the network infrastructure.

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:

```
ap(config)# wids
ad-hoc-detection : Detect ad-hoc networks
```

To display ad hoc networks:

```
ap(config)# show wids adhoc-networks
```

Wired Devices

The Wired Devices section within cnMaestro provides administrators with insights into the wired devices connected to the network infrastructure. This feature allows administrators to monitor and manage wired devices effectively to ensure optimal network performance and security.

CLI configuration:

To enable wired devices discovery:

```
ap(config)# wids
wired-neighbour-discovery : Enable wired neighbour discovery
```

Configuring WIDS

To enable WIDS feature perform the following steps on the cnMaestro UI:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** tab.
2. Select the **AP Group** and navigate to the **Security** page.
3. Select the **Enable Wireless Intrusion Detection System (WIDS)** checkbox.

Figure 62 Configuring WIDS

The screenshot shows the 'AP Groups > Add New' configuration page. On the left is a sidebar with tabs: Basic, Management, Radio, Network, Security (selected), Access Control, Services, and User-Defined Overrides. The main content area is divided into two sections. The top section is 'DoS Protection' with four checkboxes: 'IP Spoof' (checked), 'Smurf Attack' (unchecked), 'IP Spoof Log' (checked), and 'ICMP Fragment' (checked). The bottom section is 'WIDS x' with a checked checkbox 'Enable Wireless Intrusion Detection System (WIDS)'. Below this is a 'Wireless Flood Detection' section with a dropdown for 'Packets' set to '500' and a dropdown for 'Per Minutes' set to '2', with a note 'Default is 500 packets per 2 minutes'. There are five checkboxes for flood detection: 'Association', 'Authentication', 'Deauthentication', 'Disassociation', and 'EAP', all of which are currently unchecked. At the bottom of the form are 'Save' and 'Close' buttons.

4. In the **Wireless Flood Detection** section, configure the number of packets and duration from the **Packets** and **Per Minutes** drop-down lists.

This indicates the number of flood attack packets that cnMaestro must detect in the specified duration to identify and report the type of attack.

5. Select the type of flood attack detection types that you want to configure in the **Wireless Flood Detection** section.

Table 45 *Wireless Flood Detection parameters*

Field	Description
Association	Detect floods of client associations from clients.
Authentication	Detect floods of client authentication from clients.
Deauthentication	Detect floods of client deauthentications from clients.
Disassociation	Detect floods of client disassociations from clients.
EAP	Detect floods of EAP messages from clients.

Wireless Intrusion Prevention System (WIPS)

WIPS is a critical feature within cnMaestro designed to enhance the security of wireless networks. When enabled, WIPS triggers Wi-Fi devices to deauthenticate rogue APs and clients by sending spoofed deauthentication messages to the rogue APs and clients. You can also trigger Wi-Fi devices to deauthenticate honeypot APs and clients by enabling this feature.

CLI configuration:

To configure AP to detect honeypot and rogue APs, and send deauth requests to respective connected clients:

```
ap(config)# wips
deauth-honeypot-clients : Detect honeypot APs and send deauth to
respective clients
deauth-rogue-ap-clients : Detect rogue APs and send deauth to respective
clients
```

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.

To configure the services for the AP, complete the following steps:

1. Navigate to **Configuration > Wi-Fi Profiles > AP Groups** page.
2. Click **Add New** and select **Enterprise Wi-Fi (E-Series, XE/XV/X7-Series)** from the **Type** drop-down list.
3. Click **Services** tab and configure the following services:
 - [Lightweight Directory Access Protocol \(LDAP\)](#)
 - [NAT Logging](#)
 - [User Groups](#)
 - [Wi-Fi API](#)
 - [Bluetooth API](#)
 - [Speed Test](#)
 - [DHCP Option 82](#)
 - [Bonjour Gateway](#)
 - [Link Aggregation Control Protocol \(LACP\)](#)
 - [Real-Time Location System \(RTLS\)](#)

Lightweight Directory Access Protocol (LDAP)

The following table lists the fields that are displayed in the **AP Groups > Services > Network > LDAP** page.

Table 46 LDAP parameters

Parameters	Description	Range	Default
Server Host	IP address or hostname of the LDAP server.	–	–
Server Port	Port number of the LDAP server.	–	–

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

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

Figure 63 LDAP parameters

The figure displays two screenshots of the LDAP configuration interface. The top screenshot, titled 'Network', shows a sidebar with 'LDAP' selected. It contains two input fields: 'Server Host' with a placeholder 'LDAP server IP address' and 'Server port' with a placeholder 'LDAP server port'. The bottom screenshot, titled 'LDAP', shows a more detailed view with two rows. The first row is for 'Server Host', with an input field and a link 'Configure LDAP server IP address'. The second row is for 'Server Port', with an input field and a link 'Configure LDAP server port address'.

NAT Logging

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

Table 47 PDU type code: 0x82

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

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

Table 48 NAT Logging packet structure

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

Below table lists the fields that are displayed in **AP Groups > Services > Network > NAT Logging** page.

Table 49 NAT Logging parameters

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

Figure 64 NAT Logging parameters

Network

+

LDAP

+

NAT Logging

☒

Enable

Server IP

NAT Logging server IP address

Server Port

NAT Logging server port address

Interval

NAT logging interval (5-3600 seconds)

User Groups Premium feature

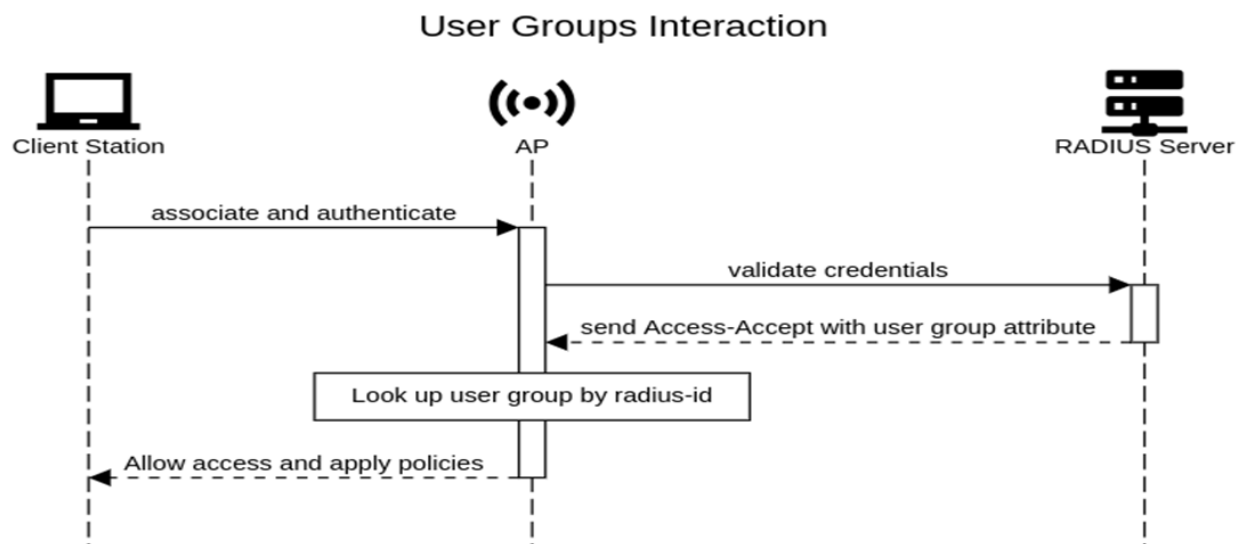
Some policies, like VLAN, require many RADIUS attributes to be sent by the RADIUS server and processed by the AP. Some wireless network administrators do not have administrative access to the RADIUS server, so making changes to wireless policies would require waiting for the RADIUS administrator to make 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 65 User Groups interaction



CLI Configuration:

```
ap(config)# group
Specify user group number <1-16>
ap(config)# group 1
ap(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
ap(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

Real-Time Location System (RTLS)

RTLS 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.

The following RTLS systems are available:

- [Wi-Fi API](#)
- [Bluetooth API](#)
- [Stanley AeroScout Premium feature](#)

Wi-Fi API

Below table lists the fields that are displayed in the **AP Groups > Services Network > RTLS (Real-Time Location System) > Wi-Fi API** page.

Table 50 *Wi-Fi API parameters*

Parameters	Description	Range	Default
Enable	Provision to enable or disable Wi-Fi API services.	-	-
Server URL	Provision to configure HTTP or HTTPS server to send a report with the port number.	-	-
Interval	Provision to configure the custom frequency of information to be shared on server.	2-3600	5
Ignore Anonymized MACs	Avoid populating locally administrated MAC addresses in the Wi-Fi API client list.	-	-

Figure 66 *Wi-Fi API parameters*



RTLS (Real-Time Location System)

☒ Wi-Fi API

☒ Enable

☐ Ignore Anonymized MACs ⓘ

Server URL

Interval

Configure Location API interval (2-3600 seconds)



Note

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

Bluetooth API

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 displayed in the **AP Groups > Services Network > RTLS (Real-Time Location System) > Bluetooth API** page..

Figure 67 Bluetooth API

RTLS (Real-Time Location System)

☒ Wi-Fi API

☐ Bluetooth API

☐ Enable

Server URL Port

Interval Configure Bluetooth API interval (10-3600 seconds)

Table 51 Bluetooth API parameters

Parameters	Description	Range	Default
Enable	Enable or disable Bluetooth API services.	-	-
Server URL and Port	Configure HTTP or HTTPS server and the port number, to send a report.	-	-
Interval	Configure the custom frequency of information to be shared on server.	2-3600	5

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:

```
ap(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:

```
ap(config)# no location-bt-api
```

Bluetooth API data elements

Table 52 Bluetooth 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': 'X7-35X-B0007C',
  'ap_name': 'XV3-8-EC7708',
  'ble_discoverd_clients': {Array of 0-250 devices}
}
```

Bluetooth API Data Format

```
{
  bt_rssi': u' -80 dBm ',
  bt_mac': 14-8F-21-FD-37-18', u
  'bt_uuids': Garmin International, Inc. (0xfe1f)\n',
  'bt_timestamp': u' 1.811127'
}
```

Stanley AeroScout [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.

CLI Configuration:

```
ap(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
```

Below table lists the fields that are displayed in the **AP Groups > Services Network > RTLS (Real-Time Location System) > Stanley AeroScout** page..

Figure 68 Stanley AeroScout

RTLS (Real-Time Location System)

☒ Wi-Fi API

☒ Bluetooth API

☒ Stanley - AeroScout X

☐ Enable Wi-Fi ⓘ

☐ Enable Bluetooth ⓘ

Host

Port

Table 53 Stanley AeroScout parameters

Parameters	Description	Range	Default
• Enable Wi-Fi • Enable Bluetooth	Enable or disable Wi-Fi or Bluetooth Stanley AeroScout services.	-	-
Server URL and Port	Configure HTTP or HTTPS server and the port number, to send a report.	-	Port: 12092

Speed Test

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

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

In this case, Wi-Fiperf endpoint should be enabled in Enterprise Wi-Fi AP through UI shown below.

To configure the above parameter, navigate to the **AP Groups > Services > Network > Speed Test** page.

Select the **Wi-Fiperf** checkbox to enable the speed test.

Figure 69 Speed Test parameters

☒ **Speed Test**

☐ **Wi-Fiperf** Enable Wi-Fiperf Endpoint

DHCP Option-82

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

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

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

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

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

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

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

Following are the supported values:

- **None**
- **All**
- **Hostname**
- **APMAC**
- **SSID**
- **VLANID**

- **SITEID**
- **Custom**

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

Following are the supported values:

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

4. Enter the VLAN ID in the **VLAN ID** text box.

5. Click **Save**.

Figure 70 DHCP Option 82 parameter

☐ **DHCP Option 82**

☒ Insert DHCP Option 82 for all wireless and guest enabled wired clients.

Option 82 Circuit ID
 Insert DHCP Option 82 circuitID information

Option 82 Remote ID
 Insert DHCP Option 82 remoteID information

VLAN ID
 Configure VLAN to have DHCP Option 82 (1-4094)

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 and devices available between the different wireless and local networks.

Below table lists the fields that are displayed in the **AP Groups > Services > Bonjour** page.

Figure 71 Bonjour page

Figure 72 Add Bonjour Gateway

Table 54 Bonjour Gateway parameters

Parameters	Description	Range	Default
Enable Bonjour Gateway	Provision to enable or 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.	-	-

CLI Configuration:

1. Enable Bonjour Gateway on AP.

```
ap(config)# Bonjour-gw
```

2. To configure Bonjour rule.

```
ap(config)# Bonjour-fw rules
```

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

3. To control mDNS repeated packet to WAN side.

```
ap(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:

```
ap(config)# interface portchannel 1
ap(config-portchannel-1)# exit
ap(config)# interface eth 1
ap(config-eth-1)# channel-group 1
ap(config-eth-1)# exit
ap(config)# interface eth 2
ap(config-eth-2)# channel-group 1
ap(config-eth-2)#
```

Port-channel configuration:

```
ap(config)# interface portchannel 1
ap(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:

```
ap(config)# interface portchannel 1
ap(config-portchannel-1)# switchport mode trunk
ap(config-portchannel-1)# switchport trunk allowed vlan 1
ap(config-portchannel-1)# switchport trunk native vlan 1
ap(config-portchannel-1)#
```

Operations

This chapter describes the following topics:

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

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, you must not restart the AP or power cycle until the process completes, as this might leave the AP inoperable.

To initiate a firmware update on the AP, complete the following steps:

1. Navigate to **Monitor and Manage > System > Software Update**.
2. Select **Enterprise Wi-Fi (XE/XV/X7-Series)** from the **Device Type** drop-down list.
3. Select the appropriate firmware version from the **Versions** drop-down list.
4. From the list of devices, select the devices for which you want to update the firmware.
5. Select the time when you want to perform the update from the **Update** section.
6. Select the appropriate options from the **Job Options** section.
7. If you select multiple devices, specify how many devices must be updated simultaneously in the text box.

A maximum of 500 devices can be updated simultaneously.

8. Click **Add Software Job to <no. of devices selected> devices**.

Figure 73 Software update

System

Dashboard
Notifications
Configuration
Statistics
Reports X
Software Update
Applications X
Clients
Mesh Peers
Analytics X
Assists X

Device Type

Enterprise Wi-Fi (XE/XV/X7 Series)

Versions

7.0-r5 (X7-35X Build)

Managed Account:

All Accounts

☐ Devices	Managed Account	Status	Client Count	Active	Inactive
☐ X7-35X-B000A0	Base Infrastructure	Offline (27d 14h 18m)	N/A	7.0-b12	7.0-a27
☐ X7-35X-B000B2	Base Infrastructure	Online (2d 3h 17m)	1	7.0-r5	7.0-r3
☐ X7-35X-B000B8	Base Infrastructure	Offline (27d 20h 13...	N/A	7.0-b14	7.0-b14
☐ X7-35X-B000D0	Base Infrastructure	Offline (3d 14h 18m)	N/A	7.0-r1	7.0-b18
☐ X7-35X-B000D4	Base Infrastructure	Offline (0d 10h 53m)	N/A	7.0-r3	7.0-b16
☐ X7-35X-B000E8	Base Infrastructure	Online (3d 16h 21m)	0	7.0-a0	7.0-b15
☐ X7-35X-B000EE	Base Infrastructure	Online (8d 3h 4m)	0	7.0-b18	7.0-b17
☐ X7-35X-B000F0_MC	Base Infrastructure	Offline (2d 19h 33m)	N/A	7.0-r3	7.0-r3
☐ X7-35X-B001A4	Base Infrastructure	Offline (2d 18h 44m)	N/A	7.0-r1	7.1-a0
☐ X7-35X-B001D6	Base Infrastructure	Online (4d 14h 59m)	0	7.1-a0	7.1-a0

Showing 1 - 10 Total: 28 10 < Previous 1 2 3 Next >

Update

☒ Now
☐ Schedule

☒ Job Options

☐ Stop update on critical error
☒ Retry skipped/offline device(s) on reconnect
☐ Update both partitions
☐ Perform sequential updates within a site
☐ Perform batch updates followed by reboot

10
Devices to update in parallel (1-500)

Notes

Add Software Job to 0 device(s)
View Update Jobs

System

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

[Table 55](#) lists the fields that are displayed in the **Operations > System** tab:

Table 55 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.	—	—

Parameters	Description	Range	Default
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 (in seconds).	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 74 System parameters

System

Reboot
Download Tech Support
Disconnect All Clients

Flash LEDs
Flash LED (1-120) seconds

Factory Default

LED Test flashing pattern

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

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

CLI commands:

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

Troubleshoot

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:

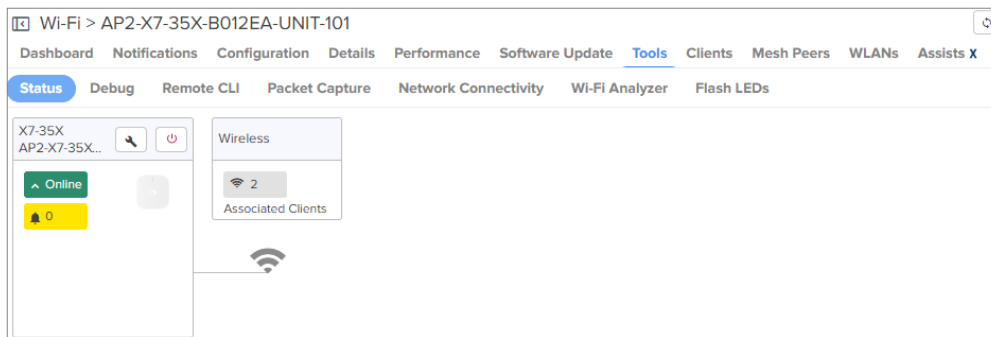
- [Status](#)
 - [Downloading tech support file](#)
- [Logging](#)
 - [Debug Logs](#)
- [Radio Frequency \(RF\)](#)
 - [Wi-Fi Analyzer](#)
- [Packet capture](#)
- [Performance](#)
 - [Network Connectivity](#)
- [Remote CLI](#)
- [Flash LEDs](#)
- [XIRCON tool support](#)
 - [XIRCON tool support for Linux 1.0.0.40](#)

Status

The Status page displays the status of link between the Enterprise Wi-Fi AP and clients. it also displays any mesh connections present. You can download the tech support file for further troubleshooting from this page.

To view the status of the link between the Enterprise Wi-Fi AP and clients, access the **Status** page under **Monitor and Manage** > <Enterprise-AP-name> > **Tools**.

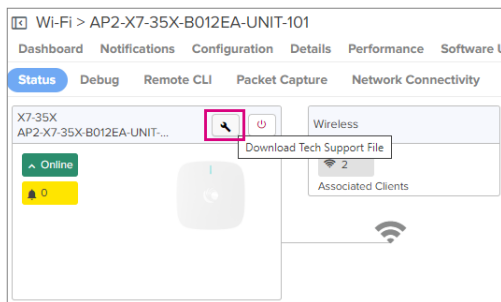
Figure 75 Status page



Downloading tech support file

To download the tech support file, click the Download Tech Support File () icon on the **Status** page.

Figure 76 Downloading tech support file



Logging

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

Debug Logs

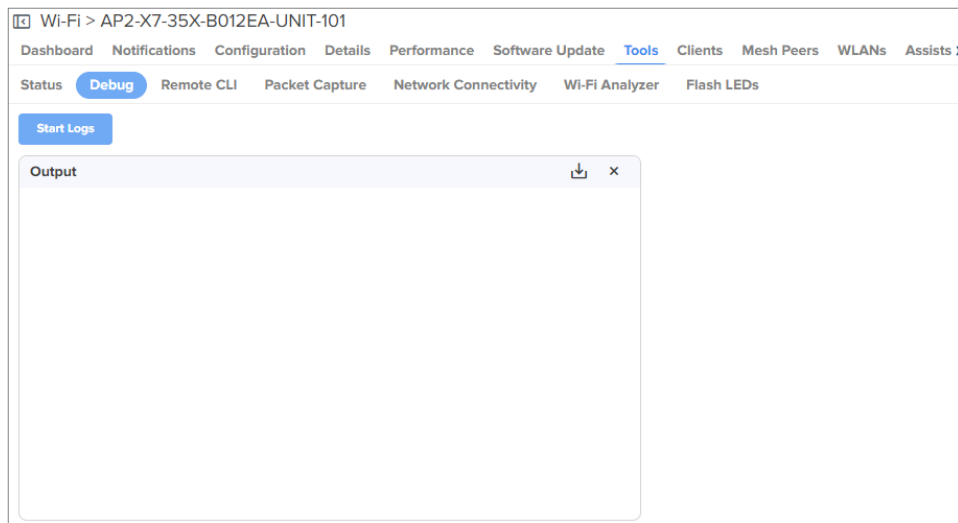
Enterprise Wi-Fi AP provisions enhanced debugging of each module as events generated by system and scope of debugging is limited. Debug logs are triggered when the user clicks **Start Logs** and terminates when user clicks **Stop Logs**. By default, debug logs auto terminate after 1 minute after initiating.

The Debug page displays log information of the Enterprise Wi-Fi AP. To view the debug information, complete the following steps:

1. Navigate to the **Monitor and Manage > <Enterprise-AP-name> > Tools > Debug** tab.
2. Click **Start Logs**.

The log information is displayed in the **Output** window.

Figure 77 Debug page



Radio Frequency (RF)

Wi-Fi Analyzer

Wi-Fi Analyzer enables customers to scan the supported channels 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 neighbor APs

- Number of APs

This tool shares more information about each channel as below:

- Noise
- Number of neighbor APs
- List of neighbor APs

To view the channel information, complete the following steps:

1. Navigate to the **Monitor and Manage** > <Enterprise-AP-name> > **Tools** > **Wi-Fi Analyzer** tab.
2. Select the radio band for which you want to view the information.

The following options are supported:

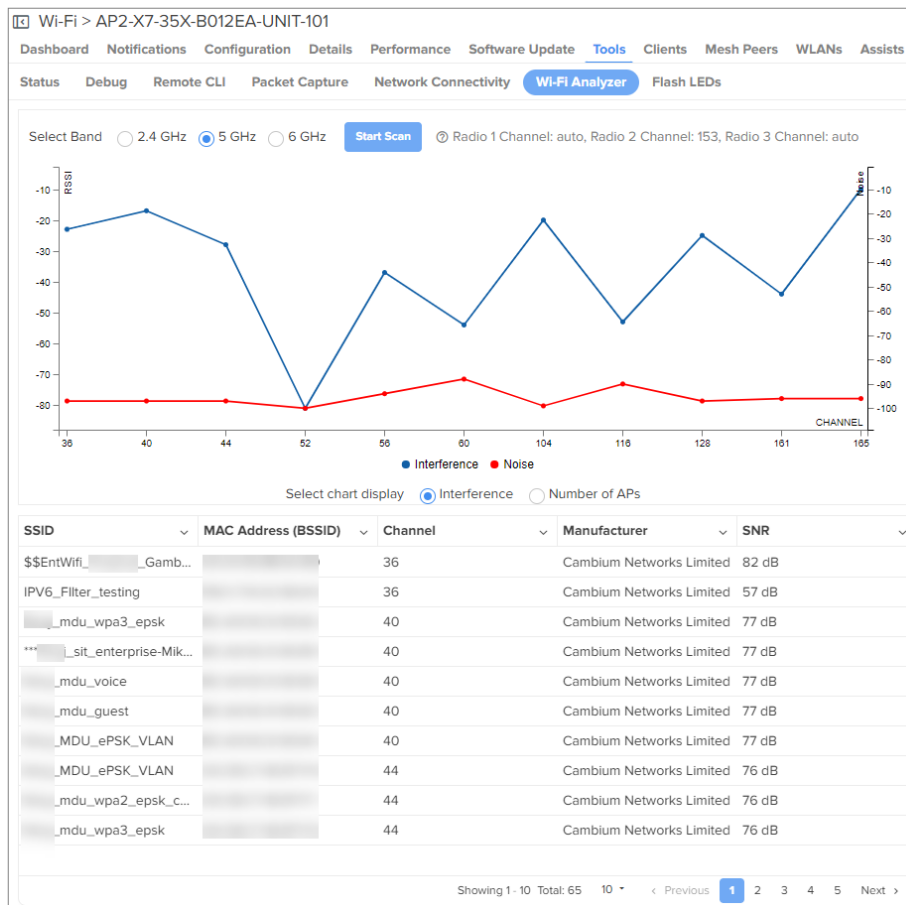
- 2.4 GHz
- 5 GHz
- 6 GHz (displayed only for supported APs)

3. Click **Start Scan**.

The channel information is displayed as follows:

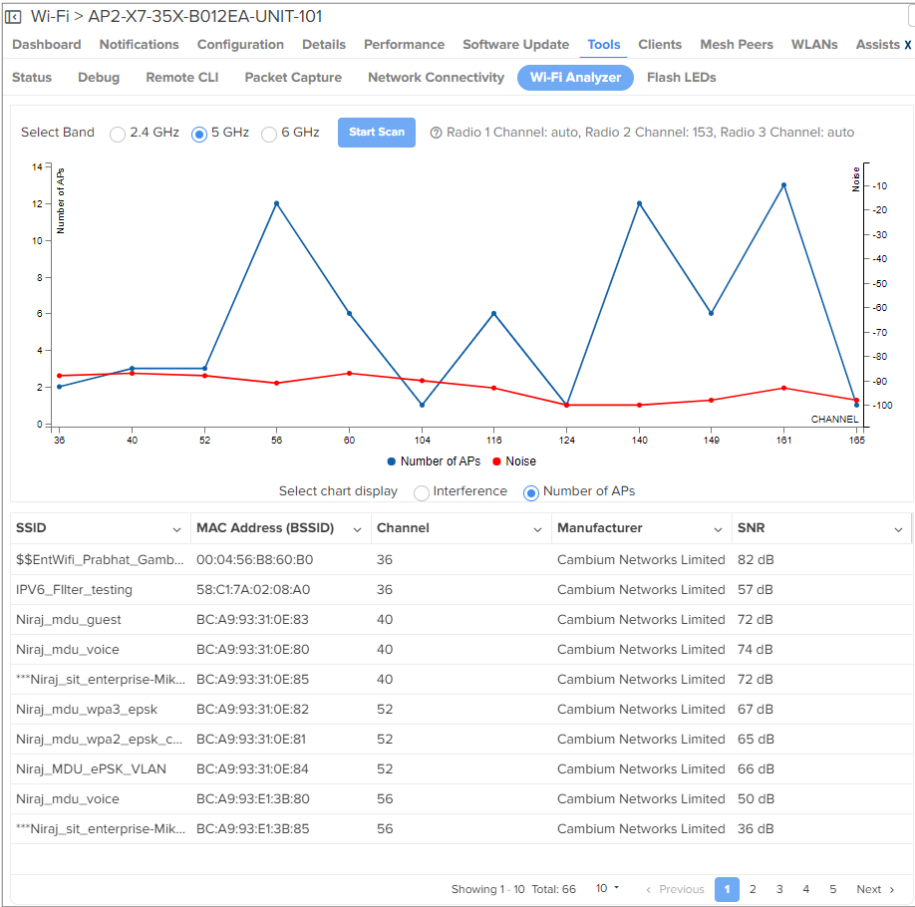
- **Interference** display mode

Figure 78 Interference display mode



- **Number of APs** display mode

Figure 79 Number of APs display 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
- PPPoE



Note

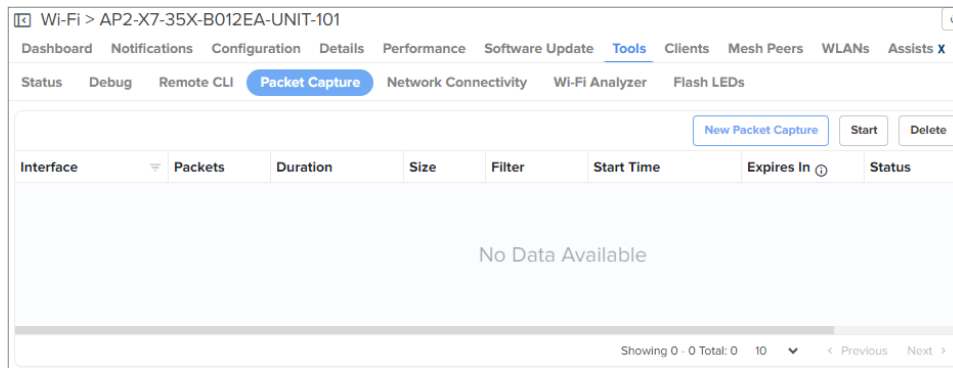
When AP packet capture is configured for the radio or wireless LAN interface, the AP records data only from the nearby APs. It does not capture its own transmissions like beacon frames or SSID broadcasts.

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

To generate and view the packet information, complete the following steps:

1. Navigate to the **Monitor and Manage > <Enterprise-AP-name> > Tools > Packet Capture** tab.

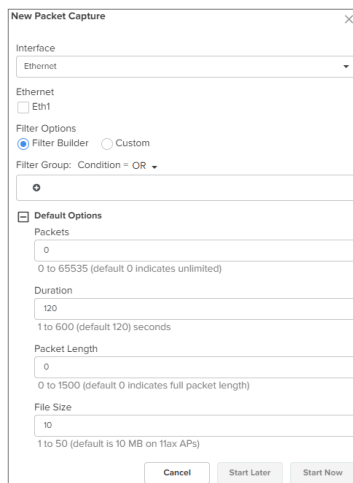
Figure 80 Packet Capture page



2. Click **New Packet Capture**.

The New Packet Capture window is displayed.

Figure 81 New Packet Capture window



3. Configure the required interface and the corresponding parameters, and the filter options.

4. Click **Start Now** or **Start Later** depending on whether you want to start packet capture now or at a later time.

When you select **Start Later**, you must click the start (▶) icon to start the packet capture.

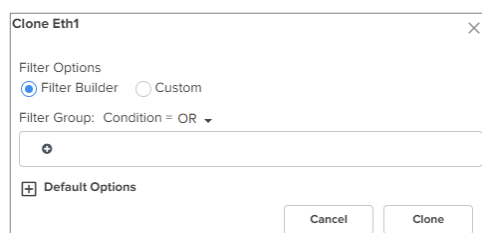
5. After the capture starts, the **Status** column displays **Running**.

Click the stop (⊗) icon to stop the capture.

6. To download the packet capture file, click the download (⬇) icon.

7. To replicate an existing packet capture with different filter options, click the clone (📄) icon corresponding to the packet capture. Specify the filter options and click **Clone**.

Figure 82 Clone packet capture



Performance

Network Connectivity

This tool helps to check the accessibility of remote hosts from Enterprise Wi-Fi AP devices. The following tools are supported:

- Ping / Ping6
- DNS Lookup / DNS Lookup6
- Traceroute

To test network connectivity of the router, complete the following steps:

1. Navigate to the **Monitor and Manage** > <Enterprise-AP-name> > **Tools** > **Network Connectivity** tab.
2. Select the required test type from the **Test Type** dropdown list and configure the corresponding parameters required for the test as described in the following table:

Table 56 Troubleshoot: Connectivity

Parameters	Description	Range	Default
Ping / Ping6			

Parameters	Description	Range	Default
IP Address or Hostname	IPv4 address or hostname to validate the reachability of the destined Host.	-	-
Number of Packets	Number of request packets that are required to be transmitted to validate the reachability of the destined Host.	1-10	3
Buffer Size	ICMP packet size to be transmitted.	1-65507	56
Ping Result	Displays the ICMP results.	-	-
DNS Lookup / DNS Lookup6			
Host Name	Hostname whose IP must be resolved.	-	-
DNS Test Result	Displays the IPs that are associated with configured hostname.	-	-
Traceroute			
IP Address or Hostname	IPv4 address or hostname to validate the reachability of the destined Host.	-	-
Fragmentation	Indicates whether to allow or deny fragment packets.	-	Off
Trace Method	Payload mechanism to check the reachability of destined IPv4 address of 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.	-	-

3. Click **Start <Test Type>**.

cnMaestro initiates the test and displays the result in the **<Test Type> Result** window.

Wi-Fi > AP2-X7-35X-B012EA-UNIT-101

Dashboard Notifications Configuration Details Performance Software Update **Tools** Clients Mesh Peers WLANs Assists X

Status Debug Remote CLI Packet Capture **Network Connectivity** Wi-Fi Analyzer Flash LEDs

Test Type
 Ping Network ping to a hostname or IP address.

IP Address or Hostname
 www.cambiumnetworks.com

Number of Packets (-c)
 3 Min = 1, Max = 10

Buffer Size (-s)
 56 Min = 1, Max = 65507

Start Ping

Ping Result
Complete
 Hostname www.cambiumnetworks.com

PING www.cambiumnetworks.com (141.193.213.11): 56 data bytes
 64 bytes from 141.193.213.11: seq=0 ttl=54 time=23.479 ms
 64 bytes from 141.193.213.11: seq=1 ttl=54 time=23.958 ms
 64 bytes from 141.193.213.11: seq=2 ttl=54 time=23.635 ms

--- www.cambiumnetworks.com ping statistics ---
 3 packets transmitted, 3 packets received, 0% packet loss
 round-trip min/avg/max = 23.479/23.690/23.958 ms

Remote CLI

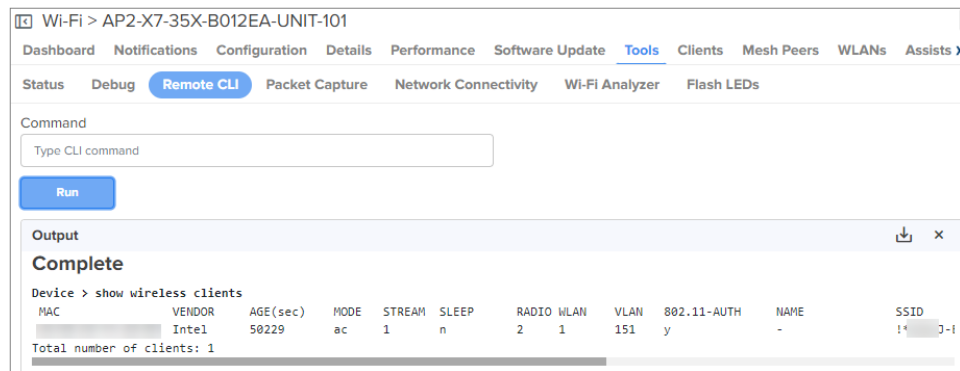
This tool allows users to execute device CLI commands, such as `service show` and `show through cnMaestro`.

To execute CLI commands, complete the following steps:

1. Navigate to the **Monitor and Manage** > *<Enterprise-AP-name>* > **Tools** > **Remote CLI** tab.
2. Enter the command in the **Command** box.
3. Click **Run**.

The command output is displayed in the **Output** window.

Figure 83 Remote CLI page



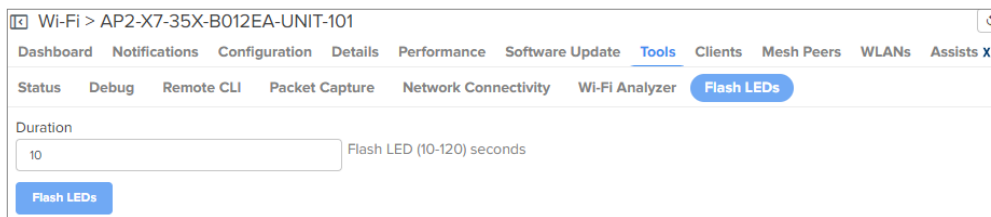
4. To download the output, click the download (📄) icon.

Flash LEDs

Flash LEDs indicate that a device is ready to receive the signal.

To flash the LEDs of an AP, access the **Flash LEDs** page under **Monitor and Manage** > <Enterprise-AP-name> > **Tools** and specify the duration (10-120 seconds) of flash.

Figure 84 Flash LEDs page



XIRCON tool support

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

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

- Xircon detects APs by listening for Xircon beacon packets. These packets are sent via UDP to a defined port and multicast address. These are the existing Multicast beacons sent by AOS.
- Control is established over unicast UDP on a different port from discovery. Only one client device can control an AP at any given time.

- Individual packets are RC4 encrypted. The payload includes a hash to ensure that any tampering or packet corruption is detected, and the packet discarded.
- Starting with Release 6.2, Enterprise Wi-Fi APs can be detected by Xirrus AOS APs and the Xircon client. It is not possible to establish a Xircon console connection to XV series APs – for that identify the IP address from Xircon and use standard SSH to connect.

XIRCON tool support for Linux 1.0.0.40

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

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 or update password.

Device configuration

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

1. Navigate to **AP Groups > Management** section.
2. Enter the administrator password in the **Admin Password** field.
3. Click **Save**.

Figure 85 Configure/update default password of the `admin` user

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Administrator Access

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

☐ Telnet Enable Telnet access to the device CLI

☒ SSH Enable SSH access to the device CLI

SSH Key Click here to view SSH key instead of password for authentication

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 from cnMaestro. Navigate to **AP Groups > Management** section and complete the following steps.

1. Select the **SSH** checkbox.
2. Provide the public key generated from the steps described in the [SSH Key generation](#) section.

Figure 86 Management parameters

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

Administrator Access

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

☐ Telnet Enable Telnet access to the device CLI

☒ **SSH** Enable SSH access to the device CLI

SSH Key Use SSH keys instead of password for authentication

☒ HTTP Enable HTTP access to the device GUI

SSH Key generation

Windows

You may use a tool, such as PUTTY 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 .

Figure 87 Generating public/private Key

PuTTY Key Generator

File Key Conversions Help

Key

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

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key:

PuTTY Key Generator

File Key Conversions Help

Key

No key.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

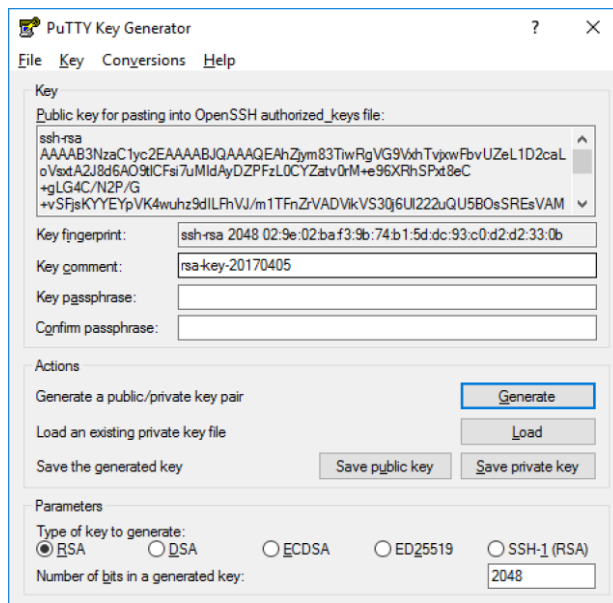
Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ ED25519 ☐ SSH-1 (RSA)

Number of bits in a generated key:

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

Figure 88 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 [Figure 89](#).

Figure 89 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 as mentioned in [Figure 89](#).
PATH = "Enter the file to which to save the key"
3. The private key (identification) is now saved in PATH as mentioned in [Figure 90](#).
PATH = "Your identification has saved in <>"

Figure 90 Private Key saved path

```
pk@ubuntu:~$ cat /home/pk/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDfZq+gc13qG8DlckyfU2JqyW5pI9q8POMrVtrM9Vu5
P851kbIiCtsTmPm6Ewrfq/nhWWsn6k4p20pTZ/laX/Ww9BWf4jjw8nOqNY95z1JUD9mV48gqrOY8qbXv
5gybXLZ+A0LarSgDaeoasM34xiJEqL+/GWkJw9/ckyueliSwAeX8ki++zJeIOQZrJWcJ6mlYHZfd4Yyb
1LRg78L+q4YbHZAdkooUkTNXJ0kaBwR2i3OJjHxD1D+SRE3DrP9xAAD1lcB5MvgQNWeBJ4ale4rwkphP
QetH/lisY/DI9nkr8Hwul2JEDeMq5yII7Fdh6ALJb+b2mtZnbGBxdsM4HrTt pk@ubuntu
pk@ubuntu:~$
```

4. Save the public key generated in step above as described in the [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 from cnMaestro. Navigate to **AP Groups > Management** and configure the following:

1. Select the **RADIUS Mgmt Authentication** check box.
2. Configure RADIUS IPv4/Hostname and shared secret in the **RADIUS Server** and **RADIUS Secret** parameters respectively.
3. Click **Save**.

Figure 91 RADIUS Server and RADIUS Secret parameters

AP Groups > Add New

Basic

Management

Radio

Network

Security

Access Control

Services

User-Defined Overrides

Administrator Access

Admin Password
[Text Field] Configure password for authentication of GUI and CLI sessions (max 32 characters)

☐ Telnet Enable Telnet access to the device CLI

☒ SSH Enable SSH access to the device CLI

SSH Key
[Text Field] Show Use SSH keys instead of password for authentication

☒ HTTP Enable HTTP access to the device GUI

HTTP Port
[Text Field: 80] Port for HTTP access to the device GUI (1-65535)

☒ HTTPS Enable HTTPS access to the device GUI

HTTPS Port
[Text Field: 443] Port for HTTPS access to the device GUI (1-65535)

☐ RADIUS Mgmt Authentication Enable RADIUS authentication of GUI/CLI sessions

RADIUS Server
[Text Field] RADIUS server IP/Hostname

RADIUS Secret
[Text Field] RADIUS server shared secret

Mesh

From Release 6.4 onwards, Enterprise Wi-Fi Access Points support mesh connections between radios. The suggested maximum hops are two. Mesh links can form between radios of the same band of operation (2.4 GHz, 5 GHz, and 6 GHz), but the two peers of the mesh link do not have to be of the same AP type. For example, a link between Wi-Fi 6 XV2-21X and XV2-23T is supported. Given the larger set of available channels and typically cleaner RF environment, Cambium Networks recommends using the 6 GHz radio for mesh backhaul if the AP is 6 GHz-capable, else use the 5 GHz band.

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

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

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

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

Deployment scenarios

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

Enterprise Wi-Fi APs support the following deployment scenarios:

- Between Cambium APs
- With third-party APs, such as TP-Link, MikroTik, and LigoWave

Enterprise Wi-Fi APs support the following deployment scenarios:

- Between Wi-Fi 6 APs
- Mixed deployment (between Wi-Fi 6 APs and Wi-Fi 5 APs)
- With third-party APs - TP-Link, MikroTik, and LigoWave

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

Figure 92 Single hop mesh connection in 5 GHz with two Mesh Clients

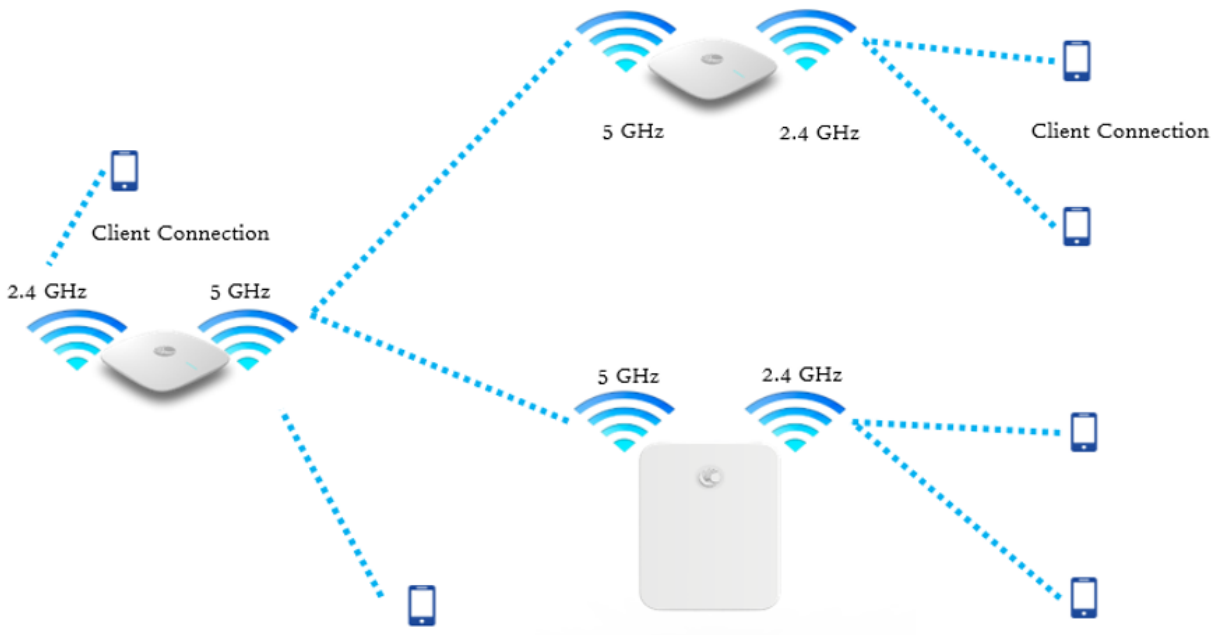


Figure 93 Single hop mesh connection in 5 GHz with two Mesh Clients and 2.4 GHz and 5 GHz as access

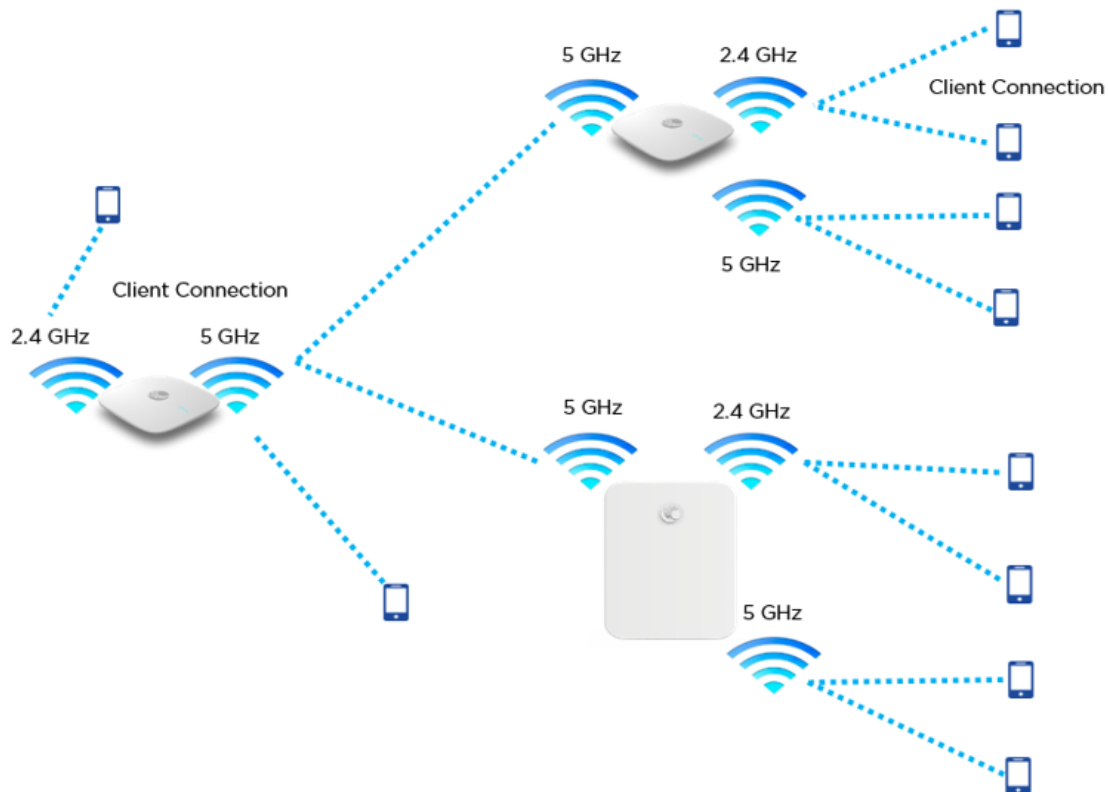
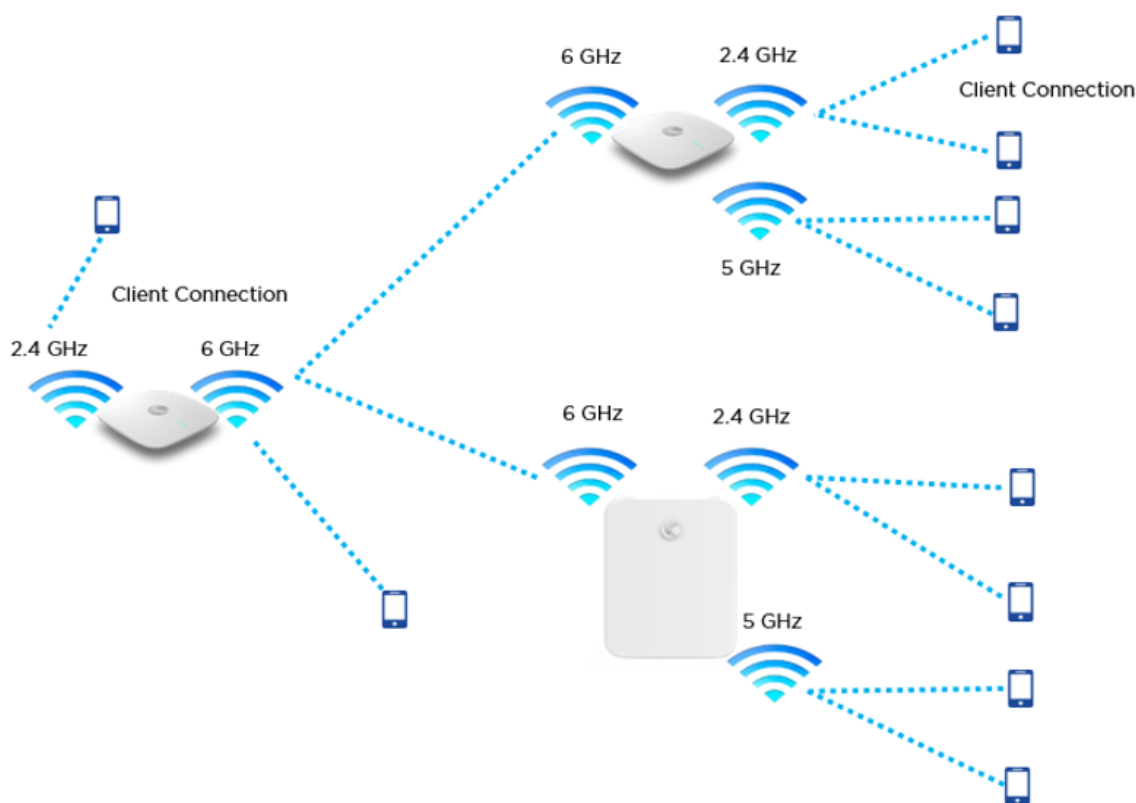


Figure 94 Single hop mesh Connection in 6 GHz with two Mesh Clients



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

- Mesh Base (MB)

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

- Mesh Client (MC)

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

- Mesh Recovery (MR)

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

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

Mesh configurable parameters

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

Table 57 Mesh configurable parameters

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

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

Order of Mesh profile configuration

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

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

- WLAN profile 3: Mesh Recovery

Mesh Base (MB)

To configure the MB:

cnMaestro configuration:

The screenshot shows the 'WLANs > Ent_Mesh_Base' configuration page in the cnMaestro interface. The page is divided into two main sections: 'Basic Information' and 'Basic Settings'.

Basic Information:

- Type:** Enterprise Wi-Fi (dropdown menu)
- Name:** Ent_Mesh_Base (text input)
- Description:** (empty text input)

Basic Settings:

- SSID:**
 - ☒ Enable
 - SSID:** CAMBIUM_MESH_BASE (text input). The SSID of this WLAN (up to 32 characters)
- Mesh:**
 - Mode:** Base (dropdown menu). Mesh Base/Client/Recovery mode
- VLAN:**
 - VLAN:** 1 (text input). Default VLAN assigned to clients on this WLAN (1-4094)
- Security:**
 - Security:** WPA2 Pre-Shared Keys (dropdown menu). Set authentication and encryption type
 - Passphrase:** (password input field with a 'Show' button). 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:**
 - Client Isolation:** Disable (dropdown menu). When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN
- Advanced Settings:**
 - ☐ 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:

```
ap(config-wlan-1)# Mesh Base
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# VLAN 1
```

```
ap(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 Wi-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

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:

```

ap(config)# wireless wlan 1
ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-recovery-interval 30
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(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:

[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:

```

ap(config-wlan-1)# mesh recovery
ap(config-wlan-1)# vlan 1
ap(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:

```

ap(config-wlan-1)# mesh snr-threshold 60

```

Mesh Mode

Enterprise Wi-Fi 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:

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 3
allowed-wlan-modes mesh
!
```

CLI configuration:

```
ap(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:

MAC Authentication

Policy

☐ Deny ☒ Permit ☐ RADIUS ☐ cnMaestro

MAC	Description	Delete
00:04:56:11:22:33	Mesh client-Cambium	

[Add New](#)

Showing 1 - 1 Total: 1 10 < Previous 1 Next >

CLI configuration:

```
ap(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:

MAC Authentication

Policy
☒ Deny ☐ Permit ☐ RADIUS ☐ cnMaestro

MAC	Description	Delete
00:04:56:11:22:33	Mesh client-Cambium	

[Add New](#)

Showing 1 - 1 Total: 10 < Previous **1** Next >

CLI configuration:

```
ap(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:

MAC Authentication

Policy
☐ Deny ☐ Permit ☒ RADIUS ☐ cnMaestro

Delimiter

☒ Password
☐ Upper Case

CLI configuration:

```
ap(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:

MAC Authentication

Policy
☐ Deny ☐ Permit ☐ RADIUS ☒ cnMaestro

CLI configuration:

```
ap(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 APs are multi-radio and multi-ethernet supported, hence there are multiple ways of configuring this feature based on the number of ethernet ports of a device.

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

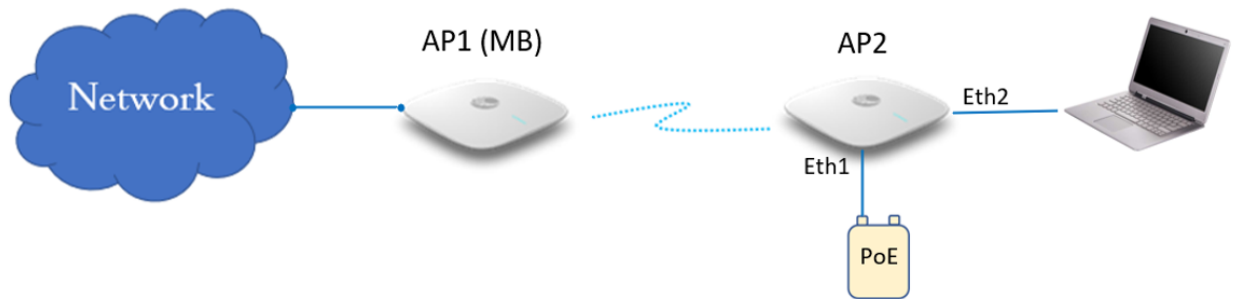
Scenario 1

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

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

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

Figure 95 Deployment Scenario 1

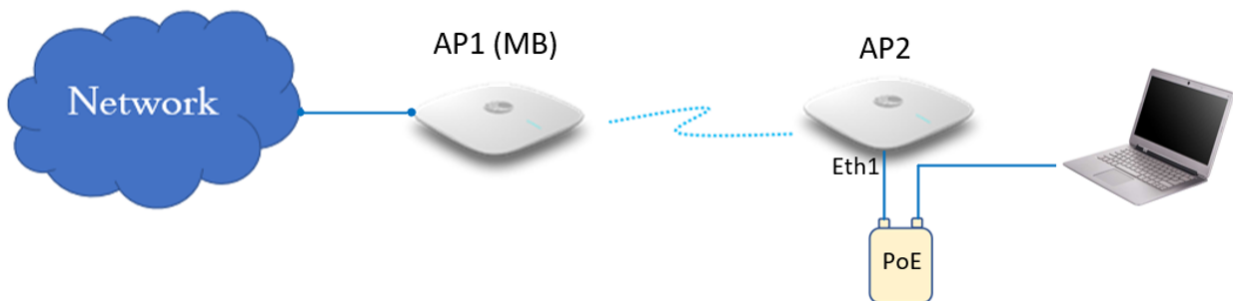


Scenario 2

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

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

Figure 96 Deployment Scenario 2

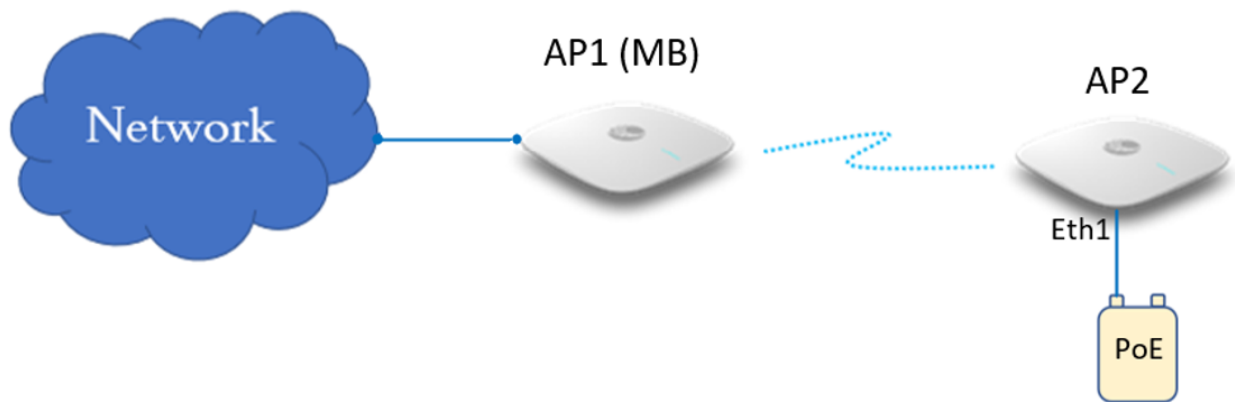


Scenario 3

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 97 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 vian 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

```
ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 1
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(config-wlan-1)# mesh-client-monitor host 8.8.8.8
```

Mesh Base

```
ap(config-wlan-7)# mesh base
ap(config-wlan-7)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-7)# vlan 1
ap(config-wlan-7)# security wpa2-psk
ap(config-wlan-7)# passphrase 12345678
ap(config-wlan-7)# band 5GHz
ap(config-wlan-7)# mesh-auto-detect-backhaul
ap(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 98 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:

```

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

```

Mesh Roaming

From Release 6.4 onwards Enterprise Wi-Fi 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 radio 2
mesh-client-bgscan
mesh-client-bgscan channel-list all-channels
mesh-client-bgscan roaming-rssi-threshold -65
mesh-client-bgscan long-interval 300
!
wireless wlan 1
mesh client
band 5 ghz
fast-roaming 802.11r
!
```

CLI configuration:

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

Mesh link-Sample configuration

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

VLAN 1 as the management interface

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

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

- WLAN MB profile

cnMaestro configuration:

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*
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:

```
ap(config-wlan-1)# mesh base
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# VLAN 1
ap(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:

```
ap(config-wlan-1)# mesh recovery
ap(config-wlan-1)# vlan 1
ap(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* 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
 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

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

Advanced Settings

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

Mesh Monitor Duration
 30 Duration in minutes (5-60)

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

CLI configuration:

```

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

```

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

cnMaestro configuration:

The screenshot shows the 'Configuration' tab for 'Ent_Mesh_ZeroTouch_APGrp'. The left sidebar has 'Network' selected. The main area is titled 'Ethernet Ports' and contains four tabs: 'Ethernet Port 1' (active), 'Ethernet Port 2', 'Ethernet Port 3', and 'Ethernet Port 4'. Under 'Ethernet Port 1', the configuration includes: 'Ethernet Port 1' dropdown set to 'Trunk Multiple VLANs', 'Native VLAN' text box with '1', a 'Tagged' checkbox (unchecked) with the label 'Tag the native VLAN', 'Allowed VLANs' text box with '2-4094' and a hint 'Eg: 1-3 or 4,10,22', 'Port Speed' dropdown set to 'Auto', and 'Port Duplex' dropdown set to 'Full Duplex'.

CLI configuration:

```
ap(config)# interface vlan 1
ap(config-vlan-1)# ip address dhcp
ap(config-vlan-1)# exit
ap(config)# interface eth 1
ap(config-eth-1)# switchport mode trunk
ap(config-eth-1)# switchport trunk native vlan 1
ap(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

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

Client Isolation

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:

```
ap(config-wlan-1)# mesh base
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# VLAN 10
ap(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:

```
ap(config-wlan-1)# mesh recovery
ap(config-wlan-1)# vlan 10
ap(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* CAMBIUM_MESH_BASE The SSID of this WLAN (up to 32 characters)

Mesh
 Client 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

☒ Mesh Vlan Tagging Enable the vlan tagging over mesh link

Advanced Settings

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

Mesh Monitor Duration
 30 Duration in minutes (5-60)

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

CLI configuration:

```
ap(config-wlan-1)# mesh client
ap(config-wlan-1)# ssid CAMBIUM_MESH_BASE
ap(config-wlan-1)# vlan 10
ap(config-wlan-1)# security wpa2-psk
ap(config-wlan-1)# passphrase 12345678
ap(config-wlan-1)# band 5GHz
ap(config-wlan-1)# mesh-recovery-interval
ap(config-wlan-1)# mesh-recovery-interval 30
ap(config-wlan-1)# mesh-client-monitor
ap(config-wlan-1)# mesh-client-monitor duration 5
ap(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:

Add VLAN

VLAN ID: 10

Please enter VLAN ID (1 to 4094)

IPv4

IP Address:

☒ DHCP

☐ Static IP:

Netmask:

☐ NAT

When NAT is enabled, IP addresses under this Switched Virtual Interface are hidden

DHCP Relay Agent:

Enable relay agent and assign DHCP server

DHCP Option 82 Circuit ID:

DHCP Option 82 Remote ID:

☒ Request Option All

Enable DHCP request option all on this interface

IPv6

General

VLAN ID	IP Address	DHCP Relay Agent	IPv6	Actions
1	dhcp	disable	enable	Allow from Wired and Wireless
10	dhcp	disable	disable	Allow from Wired and Wireless

CLI configuration:

```

ap(config)# interface vlan 10
ap(config-vlan-10)# ip address dhcp
ap(config-vlan-10)# ip dhcp request-option-all
ap(config)# interface eth 1
ap(config-eth-1)# switchport mode trunk
ap(config-eth-1)# switchport trunk native vlan 1
ap(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

Additional mesh topology supported



Note

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



Wired devices behind mesh client AP

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

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

Guest Access Portal - Internal

Introduction

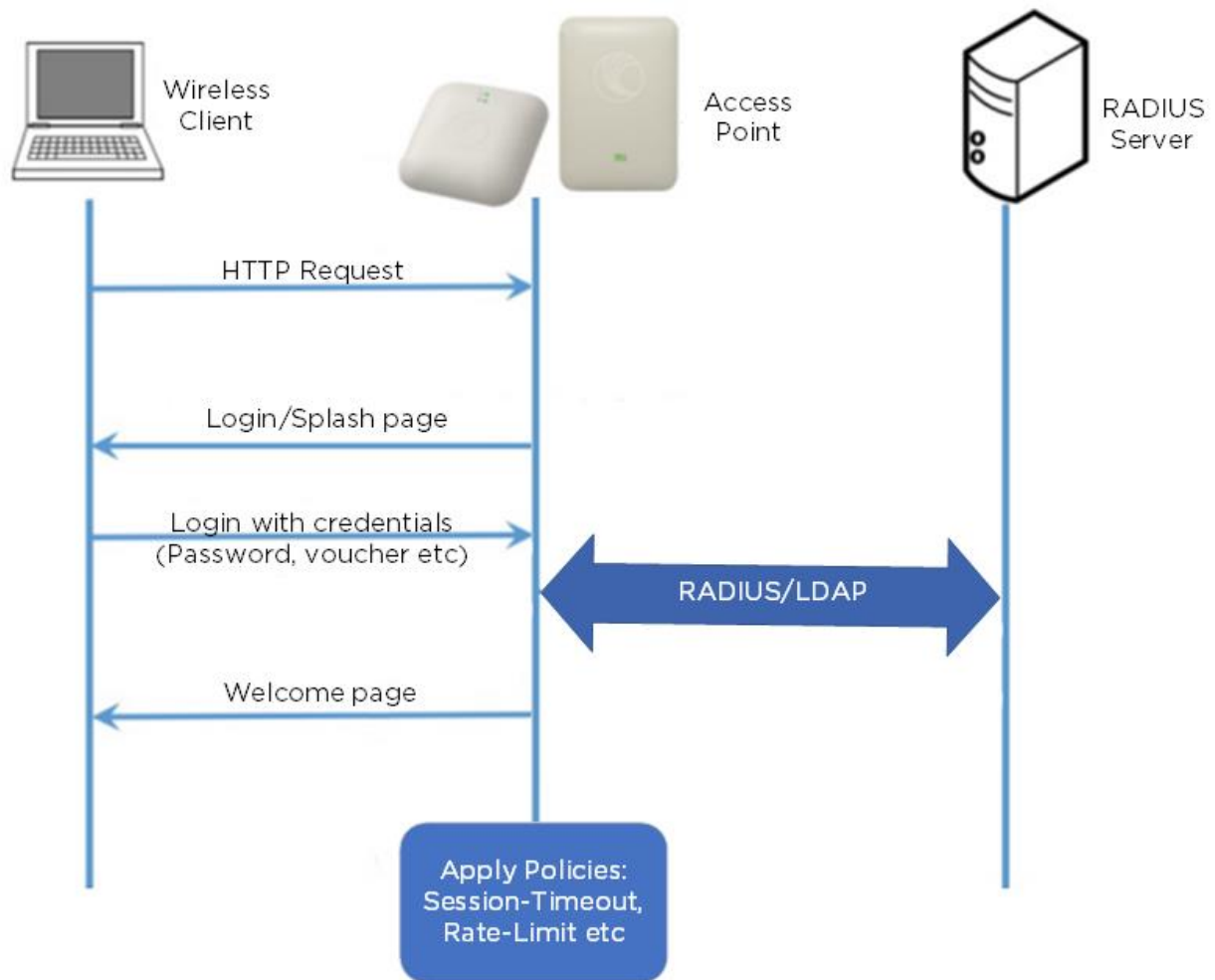
Guest Access Portal services offer a simple way to provide secure access to the internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browser's session to a captive portal login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

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

- **Internal Access:** Captive Portal server is hosted on the access point and is local to the AP.
- **External Access:** Enterprise Wi-Fi AP is integrated with multiple third-party Captive Portal services vendors. Based on the vendor, the device needs to be configured. For more information, see [Guest Access Portal - External](#).
- **cnMaestro:** Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login, and Paid login are supported. For more information, see [Guest Access – cnMaestro](#).
- **EasyPass:** EasyPass Access Services enable you to easily provide secure and controlled access to users and visitors on your Wi-Fi network.

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

Figure 99 Topology



Configurable parameters

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

Figure 100 Guest Access Internal Access Point parameter

The screenshot shows the configuration page for 'WLANs > cm_test' under the 'Configuration' tab. The left sidebar lists various configuration areas: WLAN, AAA Servers, Guest Access (selected), Access Control, Passpoint, and ePSK. The main content area is titled 'Basic Settings' and includes the following sections:

- Basic Settings**
 - ☐ Enable
 - Portal Mode
 - ☒ Internal Access Point
 - ☐ External Hotspot
 - ☐ cmMaestro
- Access Policy**
 - ☒ Clickthrough: Splash page where users accept terms and conditions to get on the network
 - ☐ RADIUS: Splash page with username and 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
- AP Server Protocol**
 - ☒ HTTP: Use unsecured HTTP protocol for AP guest access server
 - ☐ HTTPS: Use secured HTTPS protocol for AP guest access server
- Redirect Hostname**: Redirect Hostname for the splash page (up to 255 characters)
- Title**: Title text in splash page (up to 255 characters)
- Contents**: Main contents of the splash page (up to 255 characters)
- Terms**: Terms and conditions displayed in the splash page (up to 255 characters)
- Logo**: Logo to be displayed on the splash page (Eg: http:domain.com/logo.png)
- Background Image**: Background image to be displayed on the splash page (Eg: http:domain.com/backgroundimage)
- Success Action**
 - ☒ Internal Logout Page
 - ☐ Redirect User to External URL
 - ☐ Redirect User to Original URL
- Success Message**:
- Advanced Settings**
 - Redirect**
 - ☒ HTTP-only: Enable redirection for HTTP packets only
 - Redirect User Page**: 1111 Configure IP address for redirecting user to guest portal splash page
 - Redirection Port**: Port number (1 to 65535)
 - Session Timeout**: 28800 Session time in seconds (60 to 2592000)
 - Inactivity Timeout**: 1800 Inactivity time in seconds (60 to 2592000)
 - ☐ MAC Authentication Fallback: Use guest-access only as fallback for clients failing MAC authentication
 - Extend Interface**: Configure the interface which is extended for guest access

Access policy

Click through

When this policy is selected, 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.

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.

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

Timeout

Session

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

Inactivity

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

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

Figure 101 Authentication – redirected splash page

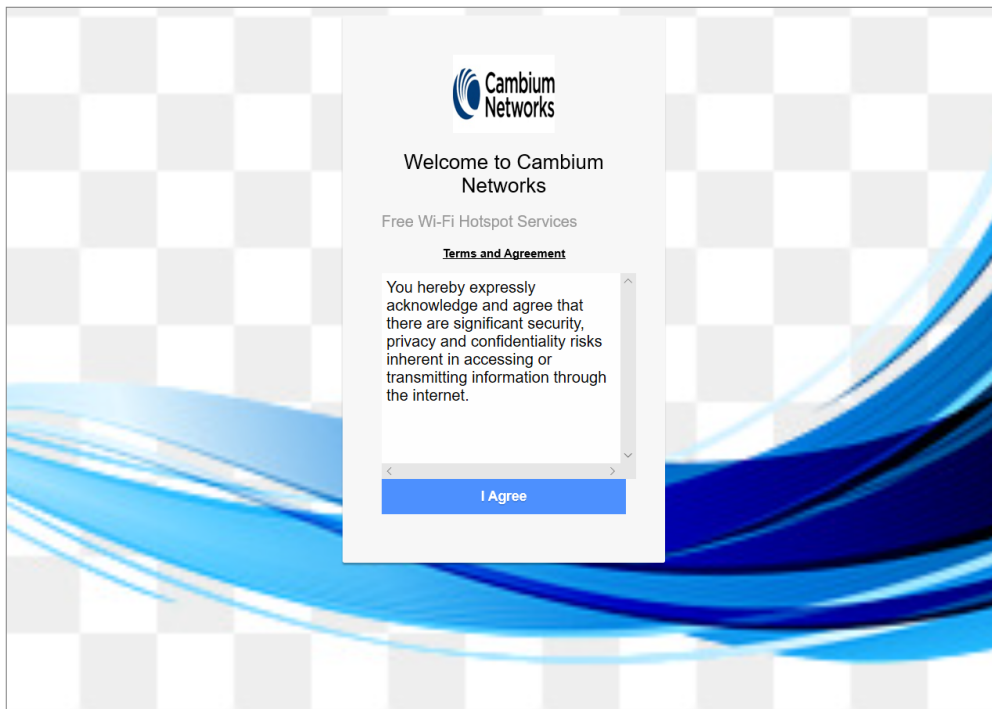
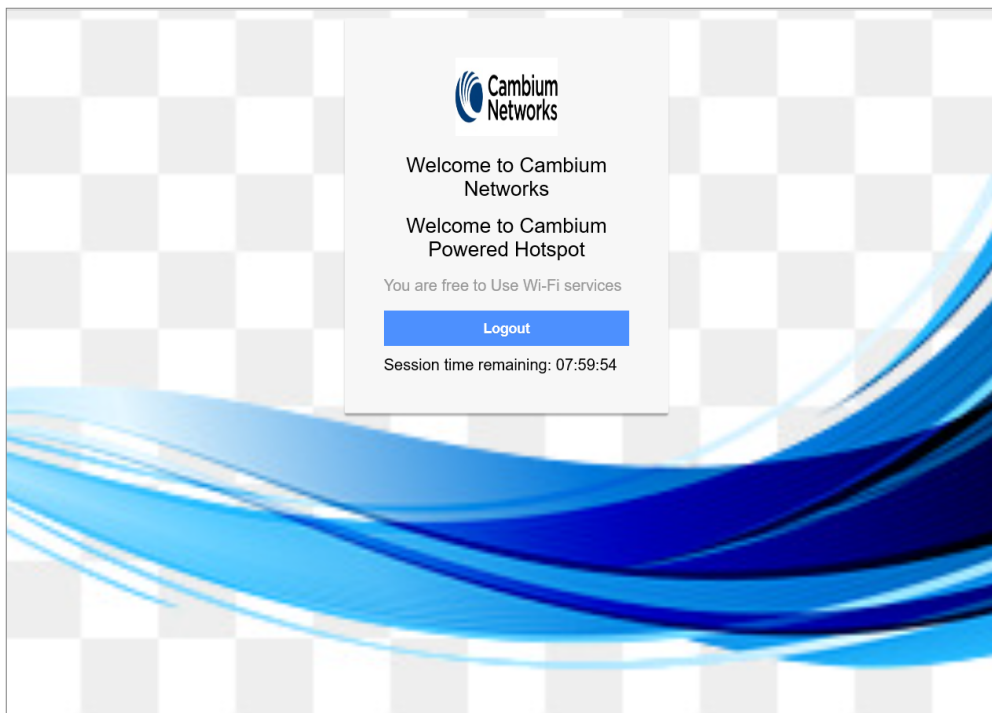


Figure 102 Successful login – redirected splash page



Guest Access Portal - External

Introduction

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

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

Configurable parameters

[Figure 103](#) displays multiple configurable parameters supported for External Guest Access hosted on AP.

Figure 103 External Hotspot parameter

The screenshot displays the 'Guest Access' configuration page for a WLAN named 'cm_test'. The page is divided into two main sections: 'Basic Settings' and 'Advanced Settings'.

Basic Settings:

- Enable:** A checkbox that is currently unchecked.
- Portal Mode:** Three radio buttons: 'Internal Access Point' (unchecked), 'External Hotspot' (checked), and 'onMaestro' (disabled).
- Access Policy:** Four radio buttons: 'Clickthrough' (checked), 'RADIUS' (unchecked), 'LDAP' (unchecked), and 'Local Guest Account' (unchecked).
- AP Server Protocol:** Two radio buttons: 'HTTP' (checked) and 'HTTPS' (unchecked).
- Redirect Hostname:** A text input field with a placeholder 'Redirect Hostname for the splash page (up to 255 characters)'.
- WSPi Clients External Server Login:** A checkbox that is currently unchecked.
- External Page URL:** A text input field.
- External Portal Post Through onMaestro:** A checkbox that is currently unchecked.
- External Portal Type:** A dropdown menu set to 'Standard'.
- Success Action:** Three radio buttons: 'Internal Logout Page' (checked), 'Redirect User to External URL' (unchecked), and 'Redirect User to Original URL' (unchecked).
- Success Message:** A text input field.

Advanced Settings:

- Redirection URL Query String:** Three checkboxes: 'Client IP' (unchecked), 'RSSI' (unchecked), and 'AP Location' (unchecked).
- Redirect:** A checkbox 'HTTP-only' is checked.
- Redirect User Page:** A text input field with the value '1111'.
- Redirection Port:** A text input field.
- Session Timeout:** A text input field with the value '28800'.
- Inactivity Timeout:** A text input field with the value '1800'.
- MAC Authentication Fallback:** A checkbox that is currently unchecked.
- Extend Interface:** A text input field.

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.

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.

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

Timeout

Session

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

Inactivity

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

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

Figure 104 Authentication – redirected splash page

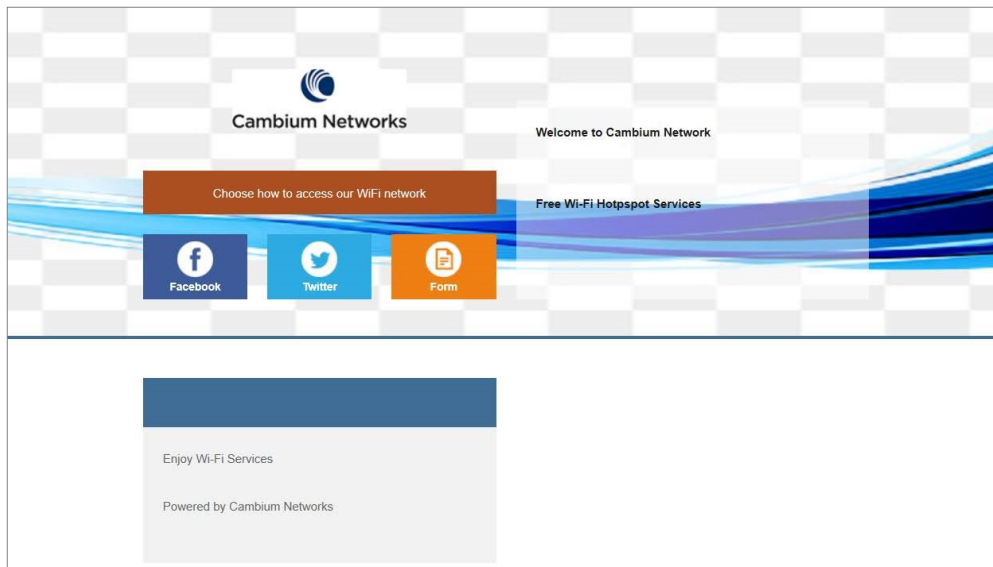
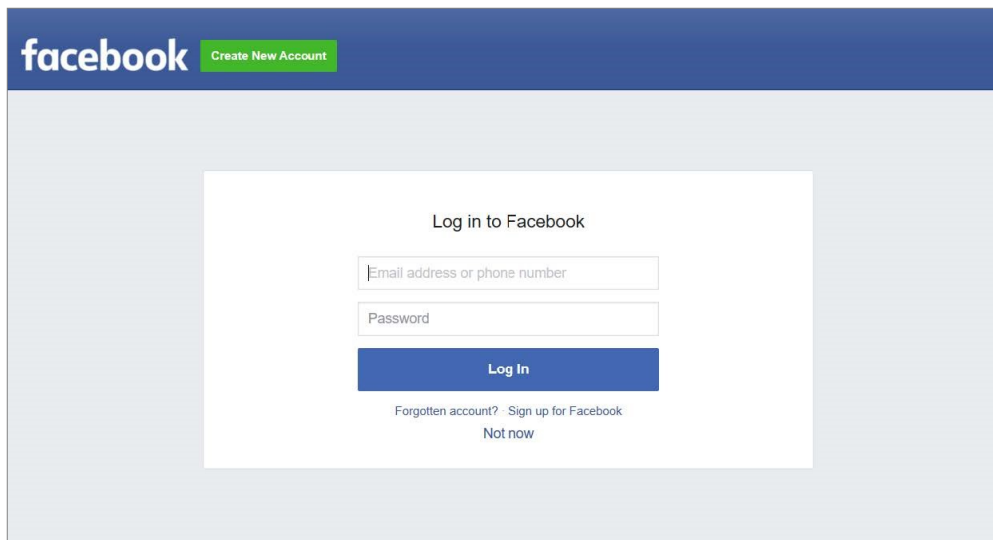


Figure 105 Successful Login – redirected splash page



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, refer to the *cnMaestro Cloud User Guide*.

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 59 *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:

```
ap(config)# lldp
ap(config)# lldp pba-auth-key
```

Example:

```
ap(config)# lldp pba
ap(config)# lldp pba-auth-key 123456789
```

Device Recovery Methods

Factory reset via 'RESET' button

Table 60 Factory reset via RESET button

Access Point	Procedure	LED Indication
XV2-21X	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-23T	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-22H	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber

Boot partition change via power cycle

Table 61 Boot partition change via power cycle

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

Disable factory Reset Button

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

```
ap(config)# no system hw-reset
```



Warning

The **Reset Button** is a key recovery option in situations when an AP gets misconfigured and you are unable to connect to the AP.

By disabling the **Reset Button**, you lose the ability to recover the AP in such scenarios.

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 62 Show commands supported in Enterprise Wi-Fi AP

SL No	CLI Command	Description
Deep Packet Inspection (DPI)		
1	<code>show application-statistics by-application</code>	Displays statistics of each application that is accessed by the station connected to the AP.
2	<code>show application-statistics by-category</code>	Displays statistics of application category that is accessed by the station connected to the AP.
Network Information		
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 <Index number></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.

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

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

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

Service commands

Service show

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

Table 63 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.

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

Service system

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

Table 64 Service system commands supported in Enterprise Wi-Fi AP

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

cnMaestro X Assurance



Note

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

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

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

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

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

MarketApps

The MarketApps feature in cnMaestro offers customized solutions for efficiently managing Wi-Fi services in residential settings, such as multi-dwelling units (MDUs) and apartment complexes. It provides specialized tools (applications or Apps) that enhance operational efficiency and cater to the distinct requirements of both property managers and residents.

Target audience

- **Property managers**—The MarketApps feature empowers property managers to centrally administer Wi-Fi access across their properties. They can set up community-wide Wi-Fi networks and manage personal Wi-Fi networks for local residents.
- **Residents**—Residents can set up and manage their own Wi-Fi networks within the community, ensuring personalized and secure Internet access.
- **Solution providers**—Solution providers can utilize MarketApps to offer tailored Wi-Fi solutions, enhancing network performance and user satisfaction in multi-dwelling units and apartment complexes.

Benefits

- **Centralized management**—Property managers can oversee and control Wi-Fi access across multiple units or buildings from cnMaestro.
- **Customization**—Residents can set up personal Wi-Fi networks with customized SSIDs and passwords, enhancing their user experience.

To access MarketApps, navigate to **Network Services > MarketApps** in cnMaestro.

For more information on configuring and viewing MarketApps, refer to the *cnMaestro User Guide*.

CLI configuration

To enable MarketApps using AP CLI, execute the following command:

```
ap(config)# wireless wlan 2
ap(config)# epsk cnMaestro
```

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).

Term	Definition
MIR	See Maximum Information Rate.
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
Proxy Server	Network computer that isolates another from the Internet. The proxy server communicates for the other computer, and sends replies to only the appropriate computer which has an IP address that is not unique or not registered.
PoE	Power over Ethernet.
SLA	Service Level Agreement
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	A virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes are possible. SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.

Appendix

This appendix contains the following topics:

- [Supported RADIUS Attributes](#)
- [Supported DFS channels](#)
- [Priority order for parameters](#)
- [Best practices for wireless clients seamless roaming across APs](#)

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

Table 65 WISPr VSAs

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

[Table 66](#) lists the WISPr VSAs supported on Enterprise Wi-Fi APs with CoA support.

Table 66 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 67](#) lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs.

Table 67 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

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		
154	Cambium-Wi-Fi-Quota-Down-Gigaword	integer64	No	No	Yes	No	No	No	-NA-	Yes
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		

[Table 68](#) lists the Cambium Networks VSAs supported on Enterprise Wi-Fi APs with CoA.

Table 68 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	

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		
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		

Standard RADIUS attributes

[Table 69](#) lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs.

Table 69 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
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-		

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		
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 70](#) lists the standard RADIUS attributes supported on Enterprise Wi-Fi APs with CoA support.

Table 70 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
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-

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		
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 71](#) lists the RADIUS attributes supported in authentication and accounting packets with WPA2-Enterprise security.

Table 71 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

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
42	Acct-Input-Octets	integer	No	No	No	No	Yes	Yes
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

Attribute Value	Attribute Description	Attribute Type	Access-Request	Access-Challenge	Access-Accept	Accounting-Start	Accounting-Interim	Accounting-Stop
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 72](#) lists the supported CoA messages.

Table 72 CoA messages

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



Note

Following are the mandatory parameters to be included in the CoA message:

- When sent through cnMaestro—User-Name, Calling-Station-Id, and Session ID
- When sent directly through the AP—User-Name, Calling-Station-Id, and NAS-Identifier

Supported DFS channels

[Table 73](#) lists the DFS channel support for various platforms in conformance with FCC standards.

Table 73 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)
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes

[Table 74](#) lists the DFS channel support for various platforms in conformance with IC standards.

Table 74 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)
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes

[Table 75](#) lists the DFS channel support for various platforms in conformance with CE standards.

Table 75 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)
XV2-22H	Yes	Yes	Yes
XV2-21X	Yes	Yes	Yes
XV2-23T	Yes	Yes	Yes

Priority order for parameters

This section provides information on the order of priority for the following parameters:

- **Session timeout and inactivity timeout**—Following priority is considered when configuring session timeout and inactivity timeout:
 - a. Configured from the RADIUS server
 - b. Configured from the AP



Note

- Inactivity timeout is triggered when there is no data packets from the client to the AP.
- A five minute static idle time is configured from the driver, which is triggered when there are no wireless packets from the client.

- **VLAN assignment**—Following priority is considered when assigning VLANs to clients:
 - a. RADIUS dynamic VLAN for guest access clients
 - b. RADIUS dynamic VLAN (Filter-ID/RADIUS-ID)
 - c. RADIUS dynamic VLAN
 - d. RADIUS-based ePSK
 - e. RADIUS-based dynamic VLAN Pool
 - f. Local ePSK VLAN setting
 - g. VLAN pool (Static)
 - h. SSID/WLAN profile VLAN
- **User group filter**—Following priority is considered for assigning policy:
 - a. Global policy
 - b. User Group policy
 - c. Device Group policy
 - d. SSID/WLAN policy

Reasons for AP restarting

The AP restarts only when the Software Defined Radios configurations are modified, such as:

- Modify radio band mode from 5 GHz to 6 GHz and vice versa
- Splitting the radio from 8x8 into 4x4 on XV3-8 (on the Radio 2) and XE5-8 APs (on the Radio 4)

Software Defined Radios					
Model	Radio 1	Radio 2	Radio 3	Radio 4	Radio 5
XV3-8	2.4 GHz	5 GHz (Split 4x4)	5 GHz	N/A	N/A
XE3-4/XE3-4TN	2.4 GHz	5 GHz	6 GHz	N/A	N/A
XE5-8	2.4 GHz	5 GHz	6 GHz	5 GHz (Split 4x4)	5 GHz

Best practices for wireless clients seamless roaming across APs



Note

- Inactivity timeout is triggered when there is no data packets from the client to the AP.
- A five minute static idle time is configured from the driver, which is triggered when there are no wireless packets from the client.

This appendix explains the recommended configuration for Cambium Networks APs and external network to facilitate a seamless roaming across the APs for the wireless clients. Additionally, this appendix also lists the recommended network best practices for minimizing broadcast and multicast packets processing.

This appendix contains the following topics:

- [External network recommendation](#)
- [AP WLAN profile configuration recommendations](#)
- [AP group configuration recommendations](#)

External network recommendations

The Cambium APs work in the distributed architecture mode and it is important to facilitate AP-to-AP communication for the wireless clients seamless roaming. The APs uses the Cambium propriety XRP protocol to exchange clients information with the neighboring APs.

Following are the recommendations:

- The intermediate network switches, to which the APs are connected, must not block the following XRP messages:

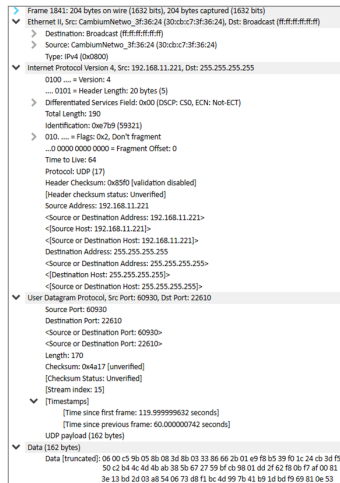
XRP message packet information

- Source MAC—APs ethernet MAC
- Destination MAC—Ethernet broadcast
- Source IP Address—APs exit interface IP address

- Destination IP Address—255.255.255.255 Broadcast IP address
- Protocol—UDP with a random source port and a fixed destination port

A sample pcap capture of the XRP message is displayed in [Figure 106](#).

Figure 106 Sample XRP message



- APs send the XRP messages on the ethernet port's native VLAN.
- All the APs must be part of the same native VLAN.
- Make sure that the APs have the L3 interface for the native VLAN with a valid IP address.

AP WLAN profile configuration recommendations

If the WLAN profile is configured with WPA2 and WPA3 security, it is recommended to enable the following:

- 802.11r fast roaming
- OKC



Note

A few clients use 802.11k and 802.11v protocols for fast roaming. We can enable the same.

Figure 107 Enabling OKC and 802.11r

WLANs > NORMAL BROWSING

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Band Steering

Disable

Steer clients across all Bands.

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

☐ Proxy ND Respond to IPv6 Neighbor Discovery (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

Option82 Circuit ID

BSSID

Option82 Remote ID

APMAC

☐ Tunnel Mode Enable tunnelling of WLAN traffic over configured tunnel

Fast Roaming Protocol

☒ OKC ☒ 802.11r Configure roaming protocol (not applicable when authentication type is Open)

☒ Over-the-DS

Re-association Timeout

20

Number of seconds (1-100)

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

☒ 802.11v Enable 802.11v BSS Transition Management

PMF (802.11w)

Optional

- Enable client isolation with the **Network Wide** option to prevent clients communicating with other clients on the same L2 network.

Figure 108 Enabling Client Isolation

WLANs > Default Enterprise

Configuration Devices

WLAN

AAA Servers

Guest Access

Access Control

Passpoint

ePSK

Basic Settings

SSID

☒ Enable

SSID*

cnPilot

The SSID of this WLAN (up to 32 characters)

Mesh

Off

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 (must contain 8 to 63 ascii or 64 hex digits)

Change your password, do not use default passwords!

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

Network Wide

When selected, it prevents wireless clients connected to the same AP or different APs from communicating with each other which are in the same VLAN. Clients are allowed to communicate to gateway mac address automatically and also mac addresses listed in below MAC address table

Client Isolation MAC List

e.g. xxxxxxxxxx

Add

Import .csv

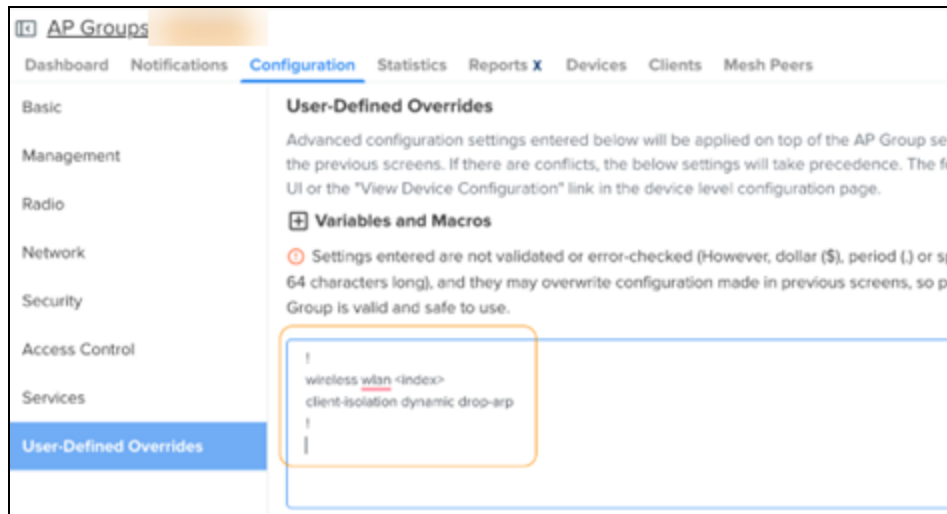
Save



Note

From AP version 6.6.0.2 onwards, the AP drops the ARP packets when the client isolation feature is enabled. To enable this in APs running firmware version lesser than 6.6.0.2, execute the `client-isolation dynamic drop-arp` CLI command from the AP group **User-Defined Overrides** section.

Figure 109 Enabling Client Isolation in User-Defined Overrides



AP group configuration recommendations

- In large public Wi-Fi and campus deployments, it is common to see large number of network discovery protocols, such as mDNS, LLNMR, SSDP and other service discovery packets coming from the wireless clients.

Disable these packets using **Access Control Policy**.

- If IPv6 is not required, disable IPv6 packets from the wireless clients using **Access Control Policy**.
- Use **Air Cleaner Rules** to:
 - prevent unauthorized rogue DHCP server from wireless clients
 - prevent unwanted DHCP client packets from wired network side
 - drop L2 broadcast packets
 - drop IPv4 and IPv6 multicast packets
 - drop ARP discovery packets from one SSID to another SSID interface
 - disable mDNS packets in the default Air Cleaner rules



Note

Allow the mDNS packet to enable bonjour discovery service to work.

- Sample AP group policy with **Air Cleaner Rules**.

Figure 110 Sample AP group policy with Air Cleaner Rules

View Access Control Policy Rules

Air Cleaner Rules

Apply Filter(s)

Name	Status	Action	Direction	Source ...	Source Mask	Destination ...	Destination Mask	Protocol	Source Port	Destination Port
Air-cleaner-Arp.1	Enabled	Deny	In	any	FF:FF:FF:FF:FF:FF	any	FF:FF:FF:FF:FF:FF	ARP	any	any
Air-cleaner-Dhcp.1	Enabled	Deny	Out	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	67
Air-cleaner-Dhcp.2	Enabled	Deny	In	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	68
Air-cleaner-Bcast.1	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	ARP	any	any
Air-cleaner-Bcast.2	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	67
Air-cleaner-Bcast.3	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	68
Air-cleaner-Bcast.4	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	UDP	any	22610
Air-cleaner-Bcast.5	Enabled	Deny	Any	any	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	FF:FF:FF:FF:FF:FF	ANY	any	any
Air-cleaner-mDNS.1	Enabled	Allow	Any	any	FF:FF:FF:FF:FF:FF	01:00:5E:00:00:FB	FF:FF:FF:FF:FF:FF	ANY	any	any
Air-cleaner-Mcast.1	Enabled	Deny	Any	any	FF:FF:FF:FF:FF:FF	multicast	FF:FF:FF:FF:FF:FF	ANY	any	any

MAC Filtering Rules

IP and Application Filtering Rules

Apply Filter(s)

Name	Status	Action	Type	Application / Category	Protocol	Sour...	Source IP Mask	Destination ...	Destination IP Mask
BLOCK DROPBOX DISCOVERY	Enabled	Deny	Layer3-filter	-	UDP	any	any	255.255.255.255	any
BLOCK LLNMR	Enabled	Deny	Layer3-filter	-	UDP	any	any	224.0.0.252	any
BLOCK SSDP	Enabled	Deny	Layer3-filter	-	UDP	any	any	239.255.255.250	any

Sample user-defined rule for blocking IPv6 traffic and allowing the rest of the traffic.

```
!  
  
filter global-filter  
filter precedence 14  
enable  
  
layer3-filter deny proto6 any any any any any any //BLOCK IPv6  
TRAFFIC  
  
exit  
  
filter precedence 15  
enable  
  
layer3-filter permit ip any/any any/any any //ALLOW TRAFFIC  
exit  
  
!
```

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places, and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified Connected Partners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

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



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 © 2025 Cambium Networks, Ltd. All rights reserved.