



USER GUIDE

Enterprise Wi-Fi Access Point

System Release 6.4



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
Chapter 1: About This User Guide	9
Overview of Enterprise Wi-Fi AP products	9
Intended audience	9
Purpose	9
Related documents	9
New hardware platforms	10
Existing hardware platforms	10
Premium feature list	10
Premium feature notice	10
Chapter 2: Quick Start – Device Access	12
Powering up the device	12
PoE switches (802.3af/802.3at/802.3bt)	12
PoE adapter	13
DC power supply	14
Accessing the device	14
Device access using default/fallback IP	15
Device access using zeroconf IP	16
Device access using DHCP IP address	17
LED status	17
Chapter 3: Onboarding the Device	19
Overview	19
Device Onboarding and Provisioning	19
cnMaestro cloud	19
XMS-Cloud	19
Swift	19
Chapter 4: UI Navigation	21
Login screen	21

Home page (dashboard)	22
Monitor	24
Configure	24
Operations	25
Troubleshoot	25
Chapter 5: Configuration - System	26
System	26
PoE out	28
Link Layer Discovery Protocol (LLDP)	28
Power negotiation	30
Management	30
HTTPs Proxy server configuration	33
Time settings	33
Event Logging	35
Chapter 6: Configuration - Radio	36
Overview	36
Configuring Radio parameters	36
Basic	36
Enhanced Roaming	40
BSS coloring	41
Target Wake Time (TWT)	41
Receive sensitivity configuration	41
Multicast-snooping and Multicast-to-Unicast conversion	42
Chapter 7: Configuration - Wireless LAN	44
Overview	44
Configuring WLAN parameters	44
Basic	44
802.11k/v	55
Radius server	55
Guest Access	59

Usage Limits	75
Scheduled Access	76
Access	77
Passpoint	79
Link Aggregation Control Protocol (LACP)	81
Radius attributes	82
enhanced PSK (ePSK)	84
RADIUS based ePSK	84
Chapter 8: Configuration - Network	85
Overview	85
Configuring Network parameters	85
IPv4 network parameters	85
Routes	90
IPv6 network parameters	93
General network parameters	97
Ethernet Ports	97
General network parameters	98
Security	99
DHCP	99
Tunnel	102
PPPoE	105
VLAN Pool	106
Chapter 9: Filter Management	108
Overview	108
Filter list	108
Filters	108
Configuring filter CLI	108
Air Cleaner	112
Application control Premium feature	114
Deep Packet Inspection (DPI)	114

Chapter 10: Configuration - Services	122
Overview	122
Configuring services	122
User Groups Premium feature	122
Location API	124
Speed Test	125
BT location API	126
Bonjour Gateway	127
Link Aggregation Control Protocol (LACP)	129
Real Time Location System (RTLS)	130
Chapter 11: Operations	131
Overview	131
Firmware upgrade	131
System	132
Configuration	133
Chapter 12: Troubleshoot	134
Overview	134
Logging	134
Events	134
Debug Logs	135
Radio Frequency (RF)	135
Wi-Fi Analyzer	135
Packet capture	137
Performance	138
Speedtest on Access Point	138
Connectivity	139
XIRCON tool support	142
XIRCON tool support for Linux 1.0.0.40	142
Chapter 13: Management Access	143
Local authentication	143

Device configuration	143
SSH-Key authentication	143
Device configuration	144
SSH key generation	144
RADIUS authentication	147
Device configuration	147
Chapter 14: Guest Access Portal- INTERNAL	148
Introduction	148
Configurable parameters	149
Access policy	150
Splash page	151
Redirect parameters	151
Success message	152
Timeout	152
Whitelist	153
Configuration examples	153
Access Policy – Clickthrough	154
Chapter 15: Guest Access Portal- EXTERNAL	156
Introduction	156
Configurable parameters	156
Access policy	157
WISPr	158
External portal post through cnMaestro	158
External portal type	158
Redirect parameters	158
Success message	159
Timeout	159
Whitelist	160
Configuration examples	160
Access Policy – Clickthrough	161

Chapter 16: Guest Access – cnMaestro164

Chapter 17: Device Recovery Methods 165

 Factory reset via ‘RESET’ button165

 Boot partition change via power cycle165

Glossary167

Cambium Networks169

Chapter 1: About This User Guide

This chapter describes the following topics:

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

Overview of Enterprise Wi-Fi AP products

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

Intended audience

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

Purpose

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

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

Related documents

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

Table 1: Related documents

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

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

New hardware platforms

System Release 6.4 includes the following new hardware platforms:

Table 2: New hardware platforms

Hardware Platform	Description
XE3-4	4x4:4; 2x2:2; 2x2:2 802.11a/b/g/n/ac wave 2/ax Tri-Radio Indoor Wi-Fi 6e Access Point

Existing hardware platforms

System Release 6.4 includes the following existing hardware platforms:

Table 3: Existing hardware platforms

Hardware Platform	Description
XV3-8	8x8:8, 4x4:4 802.11a/b/g/n/ac wave 2/ax Tri-Radio indoor Access Point
XV2-2	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio indoor Access Point
XV2-2T	2x2:2, 2x2:2 802.11a/b/g/n/ac wave 2/ax Dual-Radio Outdoor Access Point, Omni, PoE out
e410	2x2:2, 802.11a/b/g/n/ac wave 2 indoor Access Point
e510	2x2:2, 802.11a/b/g/n/ac wave 2 outdoor Access Point
e430	2x2:2, 802.11a/b/g/n/ac wave 2 indoor Access Point
e600	2x2:2 for 2.4 GHz and 4x4:4 for 5 GHz, 802.11a/b/g/n/ac wave 2 indoor Access Point
e700	2x2:2 for 2.4 GHz and 4x4:4 for 5 GHz, 802.11a/b/g/n/ac wave 2 indoor Access Point

Premium feature list

Premium feature notice

System Release 6.0 and later releases of Enterprise Wi-Fi Access Point firmware support certain advanced features which are available only through a paid subscription to cnMaestro X or XMS-Cloud management. These features will be identified with the label **Premium feature** in the applicable documentation. With the current System Release 6.3, end users can access these features without a management subscription; however, access to these features is currently on a free trial basis, and only for a limited time. As Cambium Networks releases new versions, we will begin enforcing restrictions on the

use of these premium features only in conjunction with a current cnMaestro X or XMS-Cloud subscription, and at that time, the APs will stop enabling configurations including these premium features if the user does not have a current subscription.

Table 4: Premium feature list

Feature Name	First Release
ePSK scale (more than 300 keys)	System Release 6.3
Stanley AeroScout Location Engine	System Release 6.3
User Groups	System Release 6.2
Advanced Filters	System Release 6.0
Application Control	System Release 6.0

Chapter 2: Quick Start – Device Access

This chapter describes the following topics:

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

Powering up the device

This section includes the following topics:

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

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

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

Enterprise Wi-Fi APs negotiate the power via LLDP mechanism. Please refer below sample connection. AP Eth1 port connecting to Switch PoE PSE Port.

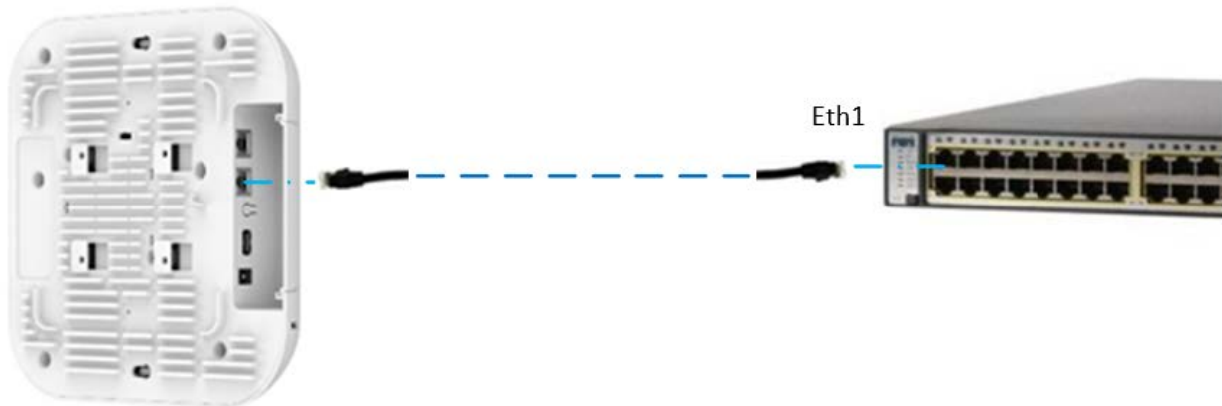


Table 5 provides detailed information on the modules that are enabled based on power negotiated via LLDP.

Table 5: Power management policy

Serial Number	PSE detection mode	Power Available for AP	LLDP Power Negotiation	Modules
1	802.3af	Critical	Yes	<ul style="list-style-type: none"> Wireless modules: Enabled USB port: Disabled BT module: Disabled
2	802.3at	Limited	Yes	<ul style="list-style-type: none"> Wireless modules: Enabled USB port: Disabled BT module: Disabled
3	802.3bt Class-0/1/2/3	Critical	Yes	<ul style="list-style-type: none"> Wireless modules: Enabled USB port: Disabled BT module: Disabled
4	802.3bt Class-4	Limited	Yes	<ul style="list-style-type: none"> Wireless modules: Enabled USB port: Disabled BT module: Disabled
5	802.3bt Class-5	Sufficient	No	<ul style="list-style-type: none"> Wireless modules: Enabled USB port: Enabled BT module: Enabled

PoE adapter

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

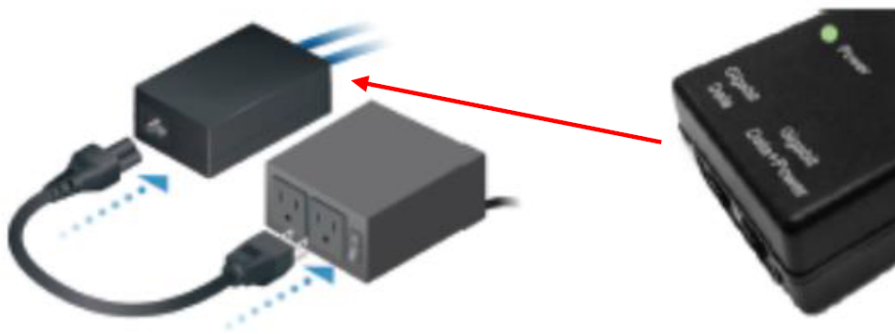
1. Connect the Ethernet cable from Eth1/PoE-IN of the device to the PoE port of 5 Gigabit Data + Power.
2. Connect an Ethernet cable from your LAN or Computer to the 5 Gigabit Data port of the PoE adapter.

Figure 1: Installation of Enterprise Wi-Fi AP to PoE adapter



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

Figure 2: Installation of adapter to power outlet



DC power supply

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

Accessing the device

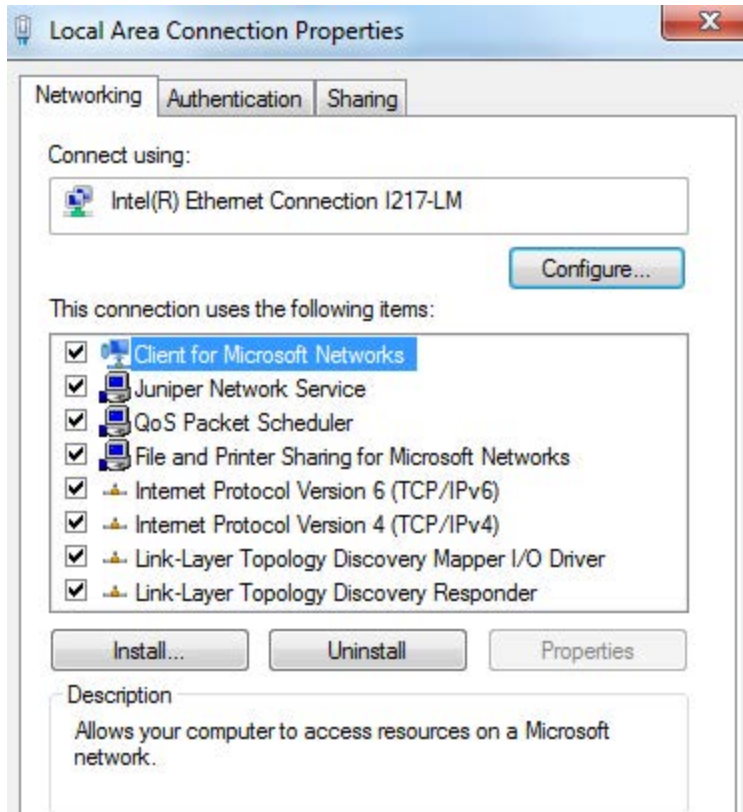
This section includes the following topics:

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

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

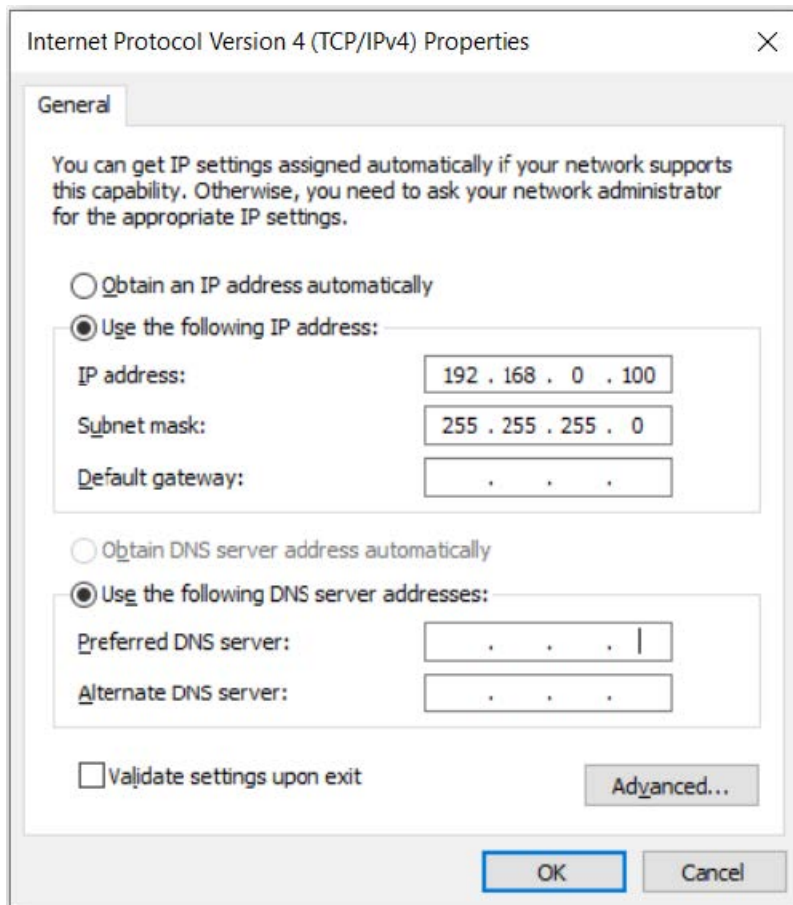
Device access using default/fallback IP

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



2. IP Address Configuration:

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



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

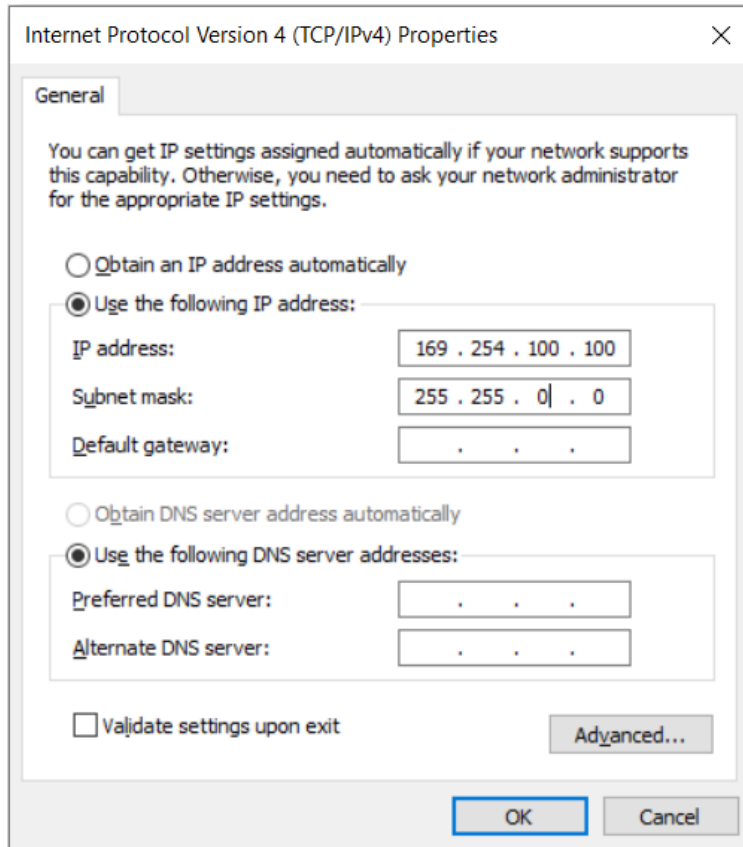
- Username: admin
- Password: admin

Device access using zeroconf IP

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

For example:

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



4. Access the device UI using <http://169.254.170.187> with default credentials as below:
 - Username: admin
 - Password: admin





Device access using DHCP IP address

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

LED status

The Enterprise Wi-Fi AP has single color LED. The power LED will glow Amber as the AP boots up and turn Green once it has booted up successfully. The network/status LED will glow Green if the connection to XMS/cnMaestro controller/manager is down and turns Blue once the AP is connected successfully to XMS/cnMaestro.

Table 6: Enterprise Wi-Fi AP LED status

LED Color	Status Indication
	<ul style="list-style-type: none"> Device is booting up. <div>  <div> Note: If these LEDs remain Amber for more than 5 minutes, indicates that the device failed to boot. </div> </div>
	<ul style="list-style-type: none"> Device is successfully up and accessible. Wi-Fi services are up if configured.
	<ul style="list-style-type: none"> XMS/cnMaestro connection is successful.

Chapter 3: Onboarding the Device

This chapter describes the following topics:

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

Overview

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

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

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

Device Onboarding and Provisioning

Enterprise Wi-Fi APs support the following Onboarding Methods:

cnMaestro cloud

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

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

XMS-Cloud

Overview

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

Device Onboarding

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

Swift

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

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



Chapter 4: UI Navigation

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

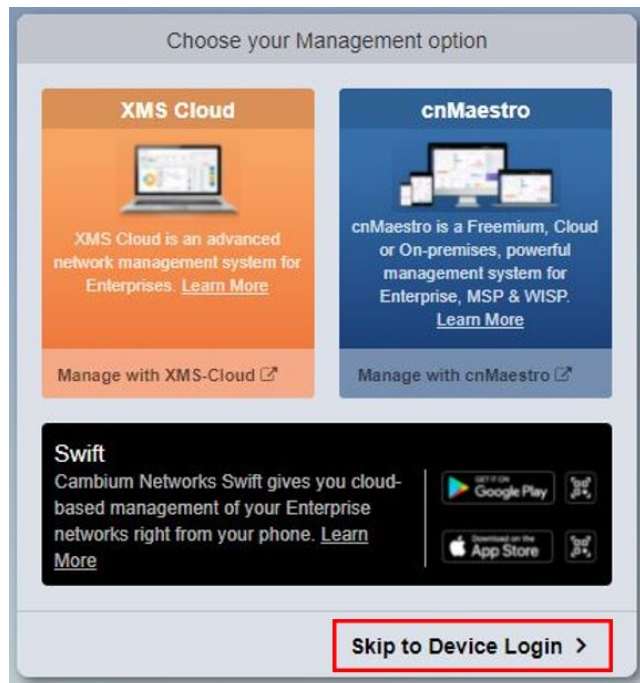
This chapter describes the following topics:

- [Login screen](#)
- [Home page \(dashboard\)](#)

Login screen

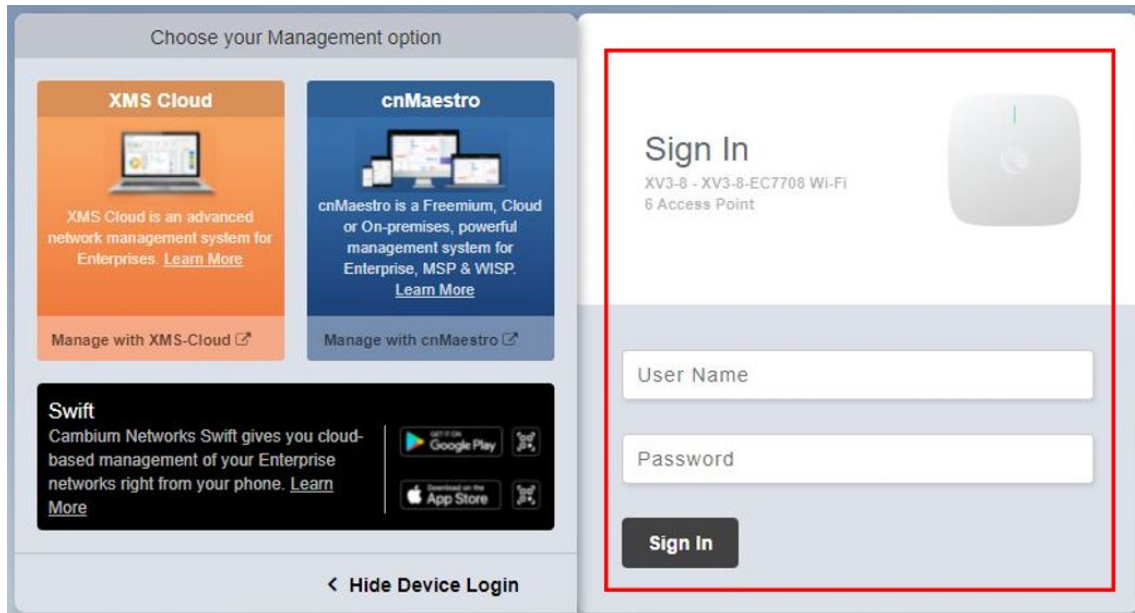
User can select the Management options as **XMS-Cloud** or **cnMaestro** to manage the device as shown in the below [Figure 1](#).

Figure 3: Management option page



If the user needs to login to the device login page, click **Skip to Device Login** and a **Sign In** tab appears as show in the below figure.

Figure 4: Device UI login page



To login to the device UI, enter the following credentials:

- User Name: admin
- Password: admin

Home page (dashboard)

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

Figure 5: Enterprise Wi-Fi AP UI Home page

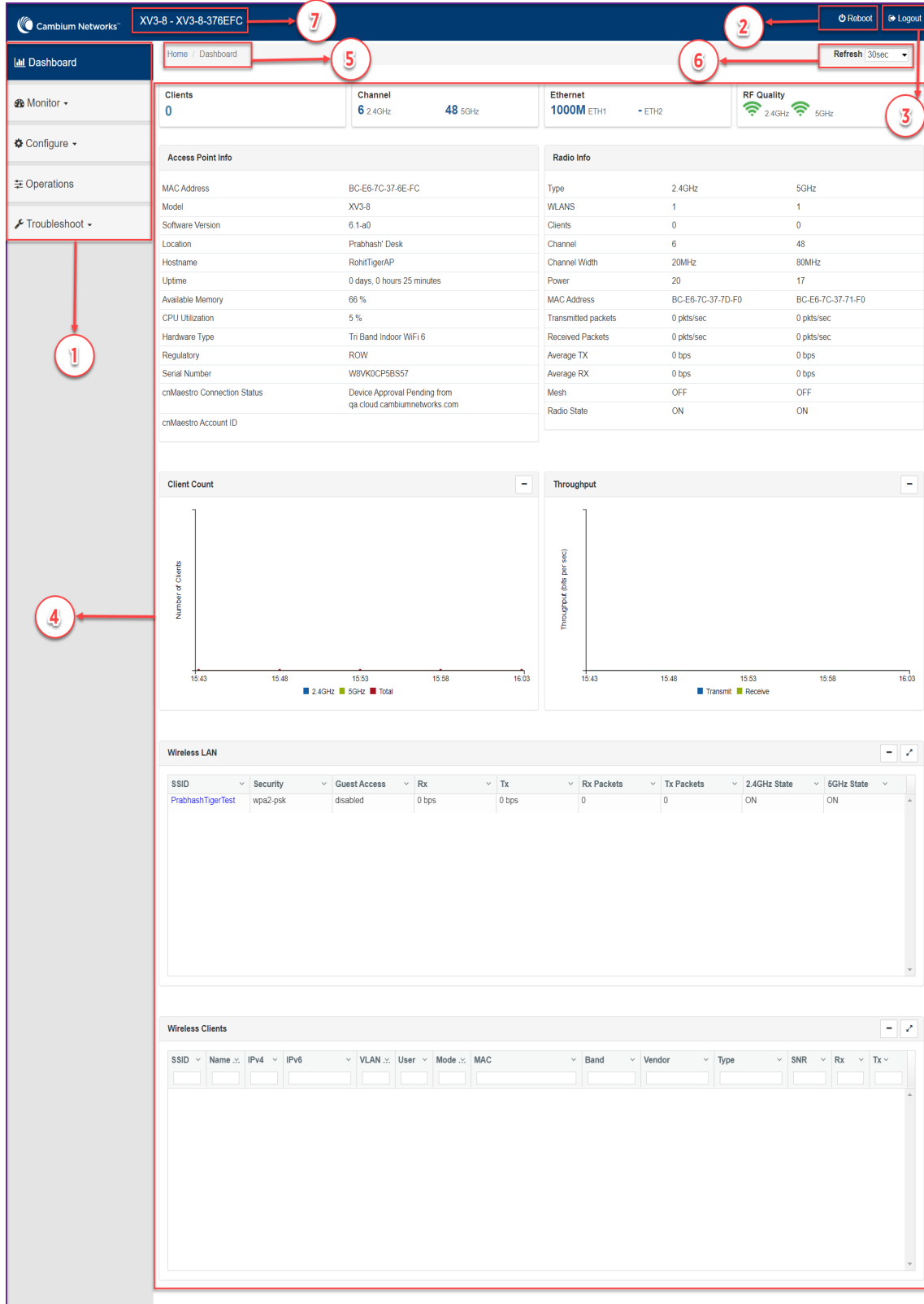




Table 7: Enterprise Wi-Fi AP web interface elements

Number	Element	Description
1	Menu	This section contains multiple tabs that helps the user to configure, monitor and troubleshoot Enterprise Wi-Fi AP device. Menu consists of the following: <ul style="list-style-type: none"> • Dashboard • Monitor • Configure • Operations • Troubleshoot
2	Reboot	Global button to reboot the Enterprise Wi-Fi AP device ().
3	Logout	Global button to logout user from the Enterprise Wi-Fi AP device ().
4	Content	Information in the area of web interface varies based on the tab selected in Menu section. Usually, this area contains details of configuration or statistics or provision to configure Enterprise Wi-Fi AP device.
5	UI path	Provides UI navigation path information to the user.
6	UI refresh interval	Provision to reload updated statistics at regular intervals.
7	Model number	Provides information related to the Enterprise Wi-Fi AP model number and configured hostname.

Monitor

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

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

Configure

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

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

Operations

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

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

Troubleshoot

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

- **Wi-Fi Analyzer:** When this is initialized, device provides information related to air quality.
- **Connectivity:** Provides different modes network reachability of Enterprise Wi-Fi AP device.
- **Packet Capture:** Provides feasibility for the user to capture packets on operational interfaces.
- **Logs:** Feasibility to check logs of different modules of Enterprise Wi-Fi AP devices helps support and the customer to debug an issue.

Chapter 5: Configuration - System

This chapter describes the following topics:

- [System](#)
- [Management](#)
- [Time settings](#)
- [Event Logging](#)

System

Table 8 lists configurable parameters that are available under **Configuration > System** UI tab:

Table 8: Configuration: System parameters

Parameter	Description	Range	Default
Name	Hostname of the device. Configurable maximum length of hostname is 64 characters.	-	Enterprise Wi-Fi AP Model Number- Last 3 Bytes of ESN
Location	The location where the device is placed. The maximum length of location is 64 characters.	-	-
Contact	Contact information for the device.	-	-
Country-Code	To be set by the administrator to the country-of-operation of the device. The allowed operating channels and the transmit power levels on those channels depends on the country of operation. Radios remain disabled unless this is set. The list of countries supported depends on the SKU of the device (FCC, ROW etc.).	-	-
Placement	Enterprise Wi-Fi AP device supports both Indoor and Outdoor deployments. Based on deployment user can configure it as follows: <ul style="list-style-type: none">• Indoor: When selected, only Indoor channels for country code configured will be available and operational.• Outdoor: When selected, only outdoor channels for country code configured will be available and operational.	-	Indoor
Dual 5 GHz radio	Provision to enable Dual 5 GHz radio. This provides the flexibility of splitting 8x8 5 GHz radio into two 4x4 5 GHz radios.	-	Disabled
LED	Select the LED checkbox for the device LEDs to be ON during operation.	-	Enabled

Parameter	Description	Range	Default
LLDP	Provision to advertise device capabilities and information in the L2 network.	-	Enabled
Default Power Policy	Provision to configure current power policy.	-	Sufficient
Power Force Type	Provision to configure power force type.	-	None

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

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

Figure 6: Configuration: System page

System

Name
XV3-8-EC7708
Hostname of the device (max 64 characters)

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

Contact
Contact information for the device (max 64 characters)

Country-Code
India
For appropriate regulatory configuration

Placement
Indoor Outdoor
Configure the AP placement details

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

LED
Whether the device LEDs should be ON during operation

LLDP
Whether the AP should transmit LLDP packets

Default Power Policy
Sufficient
Configure default power policy

Power Force Type
None
Configure power force type

PoE out

Provision to power on standard 802.3af/at devices or Cambium devices. By default, this feature is disabled.

CLI configuration

To Enable:

```
XV2-2T0-3000AA(config)# poe-out
cambium-poe|802.3af
XV2-2T0-3000AA(config)# poe-out
```

To Disable:

```
XV2-2T0-3000AA(config)# no poe-out
cambium-poe|802.3af
XV2-2T0-3000AA(config)# no poe-out
```

PoE out is supported in the following platform:

- XV2-2T

Link Layer Discovery Protocol (LLDP)

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

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

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

CLI configuration

To Enable:

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

To Disable:

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

Request power

To enable/disable power negotiation via LLDP.

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

  request-power      : Enable power negotiation (default:enabled)
  tx-hold            : Set transmit hold multiplier (default:4, used to calculate the time-to-live (tx-interval * tx-hold))
  tx-interval        : Set LLDP packet transmit delay (in Sec, default:30 sec)

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

<ENTER>

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

Transmit hold

It is used to compute the time to live (TTL) value. This is the time for which the receiving device maintains information before expiring it.

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

  request-power      : Enable power negotiation (default:enabled)
  tx-hold            : Set transmit hold multiplier (default:4, used to calculate the time-to-live (tx-interval * tx-hold))
  tx-interval        : Set LLDP packet transmit delay (in Sec, default:30 sec)

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

  Specify transmit hold multiplier value (max 65535)

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

Transmit interval

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

```

XV3-8-EC7708(config)# lldp

request-power      : Enable power negotiation (default:enabled)
tx-hold            : Set transmit hold multiplier (default:4, used to calculate the
time-to-live (tx-interval * tx-hold))
tx-interval        : Set LLDP packet transmit delay (in Sec, default:30 sec)

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

Specify LLDP transmit delay in sec (max 65535)

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

```

Power negotiation

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

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

Management

Table 9 lists configurable fields that are displayed in the **Configuration > System > Management** tab:

Table 9: Configuration: System > Management parameters

Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	-	admin
Telnet	Enables Telnet access to the device CLI.	-	Disabled
SSH	Enables SSH access to the device CLI.	-	Enabled
SSH Key	Provision to login to device using SSH Keys. User needs to add Public Key in this section. If configured, user has to login to AP using Private Keys. This is applicable for both CLI and GUI.	-	Disabled
HTTP	Enables HTTP access to the device UI.	-	Enabled
HTTP Port	Provision to configure HTTP port number to access device UI.	1-65535	80
HTTPS	Enables HTTPS access to the device UI.	-	Enabled
HTTPS Port	Provision to configure HTTPS port number to access device UI.	1-65535	443
RADIUS Mgmt	User has provision to control login to AP using RADIUS	-	Disabled

Parameter	Description	Range	Default
Auth	authentication. If enabled, every credential that are provided by user undergo RADIUS authentication. If success, allowed to login to UI of AP. This is applicable for both CLI and GUI.		
RADIUS Server	Provision to configure RADIUS IPv4 server for Management Authentication.	-	-
RADIUS Secret	Provision to configure RADIUS shared secret for Management authentication.	-	-
cnMaestro			
Cambium Remote Mgmt.	Enables support for Cambium Remote Management of this device.	-	Enabled
Validate Server Certificate	This allows HTTPs connection between cnMaestro and Enterprise Wi-Fi AP device.	-	Enabled
cnMaestro URL	Static provision to onboard devices either using IPv4 URL.	-	-
Cambium ID	Cambium ID used for provisioning cnMaestro (Cambium Remote Management) of this device.	-	-
Onboarding Key	Password used for onboarding the device to cnMaestro.	-	-
SNMP			
Enable	Provision to enable SNMPv2 or SNMPv3 support on device	-	-
SNMPv2c RO community	SNMP v2c read-only community string.	-	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 username for SNMPv3.	-	-
SNMPv3 Password	Enter password for SNMPv3.	-	-
Authentication	choose Authentication type as MD5 or SHA.	-	MD5
Access	Choose Access type as RO or RW.	-	RO
Encryption	Choose ON or OFF.	-	ON

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

1. Enter the admin password of the device in the **Admin Password** textbox.
2. Enable the **Telnet** checkbox to enable telnet access to the device CLI.
3. Enable the **SSH** checkbox to enable SSH access to the device CLI.

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

To configure **cnMaestro**:

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

To configure **SNMP**:

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

Figure 7: Configuration: Management page

The screenshot shows the 'Management' configuration page. It includes sections for:

- Admin Password:** A field with masked characters (*****).
- Telnet:** A checkbox labeled 'Enable Telnet access to the device CLI'.
- SSH:** A checked checkbox labeled 'Enable SSH access to the device CLI'.
- SSH Key:** A text input field.
- HTTP:** A checked checkbox labeled 'Enable HTTP access to the device GUI'.
- HTTP Port:** A text input field with the value '80'.
- HTTPS:** A checked checkbox labeled 'Enable HTTPS access to the device GUI'.
- HTTPS Port:** A text input field with the value '443'.
- RADIUS Mgmt Auth:** An unchecked checkbox labeled 'Enable RADIUS authentication of GUI/CLI sessions'.
- RADIUS Server:** A text input field.
- RADIUS Secret:** A text input field.
- cnMaestro:** A section containing:
 - Remote Management:** A checked checkbox.
 - Validate Server Certificate:** A checked checkbox.
 - cnMaestro URL:** A text input field.
 - Cambium ID:** A text input field.
 - Onboarding Key:** A text input field.
- SNMP:** A section containing:
 - Enable:** A checked checkbox labeled 'Enable/Disable SNMP'.
 - SNMPv2c RO community:** A text input field.
 - SNMPv2c RW community:** A text input field.
 - Trap Receiver IP:** A text input field.
 - SNMPv3 Username:** A text input field.
 - SNMPv3 Password:** A text input field.
 - Authentication:** A dropdown menu with 'MD5' selected.
 - Access:** A dropdown menu with 'Read-Only' selected.
 - Encryption:** A dropdown menu with 'On' selected.

HTTPs Proxy server configuration

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

For zero touch configuration, please refer [DHCP Option 43 - Zero touch onboarding](#).

CLI configuration:

```
XV3-8-EC7708(config)# management proxy
https                               : Enable HTTPS proxy support

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


Time settings

User can configure up to two NTP servers. These are used by the AP to set its internal clock to respective time zones configured on the device. While powering ON the AP, the clock will reset to default and resyncs the time as the Enterprise Wi-Fi AP does not have battery backup. The servers can be specified

as an IPv4 addresses or as a hostname (Eg: pool.ntp.org). If NTP is not configured on device, device synchronizes time with cnMaestro if onboarded.

Table 10 lists the fields that are displayed in the **Configuration > System > Time Settings** section.

Table 10: Configuration: System > Time Settings parameters

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

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

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

Figure 8: Configuration: Time settings page

Time Settings

NTP Server 1

Name or IP address of a Network Time Protocol server

NTP Server 2

Time Zone

Configure Timezone

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

Event Logging

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

Table 11 lists the fields that are displayed in the **Configuration > System > Event Logging** section.

Table 11: Configuration: System > 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

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

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

Figure 9: Configuration: Event Logging page

Event Logging

Syslog Server 1

10.110.211.97

Port

514

Name or IPv4/IPv6 address of syslog server

Syslog Server 2

10.110.219.10

Port

1234

Syslog Severity

Debug (level 7 ▾)

Specify severity of events forwarded to Syslog servers

Save

Cancel

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

Chapter 6: Configuration – Radio

This chapter describes the following topics:

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

Overview

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

Configuring Radio parameters

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

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

Basic

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

Table 12: Configure Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables operation of radio.	-	Enabled
Band	If any radio supports multiple bands then user can select one of the band.	-	-
Channel	User can select the channel from the drop-down list. Channels in drop-down list is populated based on Country selected in Configuration > System UI.	2.4 GHz: 1 - 14 5 GHz: 36 - 173	Auto
Channel Width	User can select operating width of the channel. <ul style="list-style-type: none">• For 2.4 GHz: Only 20MHz channel width is supported.• For 5 GHz:	-	20 MHz for 2.4 GHz and 5 GHz

Parameter	Description	Range	Default
	20 MHz, 40 MHz, 80MHz and 160 MHz channel width is supported.		
Transmit Power	User can configure transmit power of each radio based on coverage and SLA. Unit of transmit power is in dBm and its range is from 4 to 30. Maximum transmit power of Enterprise Wi-Fi AP devices varies based on model number. More details of transmit power supported by each Enterprise Wi-Fi AP device is available at https://www.cambiumnetworks.com/products/wifi/ . Transmit power drop-down box varies as per the country selected in Configuration > System UI. Default value is AUTO, which means radio transmit power is configured to maximum as per the county configured selected in Configuration > System UI.	2.4 GHz: 4 - 30 5 GHz: 4 - 30	Auto
Beacon Interval	User can configure time durations between two consecutive Beacon's. It is termed as Beacon interval.	50ms - 3400ms.	100
Minimum Unicast rate	Provision to adjust the coverage area of Enterprise Wi-Fi AP device. Higher the rate selected, lesser the range. User can configure this value based on SLA in deployment. Drop-down list contains all values that are advertised by Enterprise Wi-Fi AP device which includes legacy, HT and VHT rates.	Standard 802.11b and 802.11g data rates	1Mbps
Candidate Channels	Enterprise Wi-Fi AP provides user to configure selective channels based on their requirement. Options vary based on band of operation and is as follows: <ul style="list-style-type: none"> For 2.4 GHz: <ul style="list-style-type: none"> All Specific For 5 GHz: <ul style="list-style-type: none"> All Specific Prefer Non-DFS Prefer DFS 	2.4 GHz: 1 - 14 5 GHz: 36 - 173	All
Mode	All Enterprise Wi-Fi AP devices are either 802.11ax, 802.11ac Wave 1 or 802.11ac Wave 2 supported. There are few legacy clients which might not work as expected, hence this parameter can be tuned to backward compatibility based on wireless clients.	a) 2.4 GHz: b/g/n/ax. b) 5 GHz: a/n/ac/ ax.	All mode
Short Guard	Standard 802.11 parameter to increase the throughput of	-	Enabled

Parameter	Description	Range	Default
Interval	Enterprise Wi-Fi AP device.		
Off Channel Scan (OCS)**			
Enable	Provision to enable OCS on device to capture neighbour clients and APs.	-	-
Dwell-time	Configure the time period to spend scanning of Wi-Fi devices on a channel.	50-300	50ms
Auto-RF			
Dynamic Power	Provision to enable dynamic power management.	-	-
Mode	Select the required dynamic power modes. Two modes are supported: 1. By-channel 2. By-band	-	By-channel
Minimum Transmit Power	The minimum transmit power that the AP can assign to a radio when adjusting automatic cell sizes	5-15 dBm	8 dBm
Minimum Neighbour Threshold	The minimum number of neighbors to consider for power reduction by autocell logic.	1-10	2
Cellsize Overlap Threshold	Cell overlap that will be allowed when the AP is determining automatic cell sizes.	0-100%	50%

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

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

To configure **Off Channel Scan**:

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

To configure **Auto-RF**:

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

Figure 10: Configure: Radio parameters

Basic

Enhanced Roaming

Radio

Enable

☒

Enable operation of this radio

Band

2.4GHz

▼

Configure the supported bands

Channel

Automatic

▼

Primary operating channel

Channel Width

20MHz

▼

Operating width of the channel

Transmit Power

Auto

▼

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

Beacon Interval

100

▼

Beacon interval in mSec (100 to 3500 in increments of 100)

Minimum Unicast rate

default

▼

Configure the minimum unicast management rate (Mbps)

Multicast data rate

default

▼

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

Airtime Fairness

☐

Enable Airtime Fairness

Candidate Channels

All

▼

Mode

default

▼

Allow 802.11 b/g/n clients to connect

Short Guard Interval

☒

Enable short guard interval

Off Channel Scan

Enable

☐

Enable OCS

Dwell-time

50

▼

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

Auto RF

Dynamic Power

☐

Enable dynamic power management

Mode

☒ By-channel ☐ By-band

Set dynamic power mode by-channel/by-band

Minimum Transmit Power

8

▼

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

Minimum Neighbour Threshold

2

▼

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

Cellsize Overlap Threshold

50%

▼

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

Save

Cancel

Off Channel Scan (OCS)**

In the CLI, to configure Off Channel Scan:

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

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

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

    active          : active off channel scan
    passive         : passive off channel scan
```

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

Table 13: Configuring Off Channel Scan

Parameter	Description	Range	Default
dwell time	Provision to configure Off Channel Scan dwell time. Needs to change 100 or more than 100+ ms for supporting passive scan method.	50-300	50ms
interval	AP Off Channel Scan interval time.	-	6 sec
type	<p>Provision to configure Off Channel Scan types.</p> <ul style="list-style-type: none">activepassive <p>AP radio transmits a probe request and listens for a probe response from an AP.</p> <p>AP radio listens on each channel for beacons sent periodically by an neighbor APs.</p> <p>Users are advised to use passive as scan type.</p>	-	active

Enhanced Roaming

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

Table 14: Configure: Radio Enhanced Roaming parameters

Parameter	Description	Range	Default
Enhanced Roaming			
Enable	Provision to enable enhanced roaming on device.	-	Disabled

Parameter	Description	Range	Default
Roam SNR threshold	Enterprise Wi-Fi AP device triggers de-authentication of wireless station, when the wireless station is seen at configured SNR or below.	1-100	15dB

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

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

Figure 11: Configure: Radio > Enhanced Roaming parameters

The screenshot shows the 'Enhanced Roaming' configuration page. At the top, there are two tabs: 'Basic' and 'Enhanced Roaming', with 'Enhanced Roaming' being the active tab. Below the tabs, there is a section with the following elements:

- An 'Enable' checkbox, which is currently checked.
- A link: 'Enable active disconnection of clients with weak signal'.
- A label 'Roam SNR threshold' followed by a text input field containing the value '15'.
- A descriptive text: 'SNR below which clients will be forced to roam (1-100 dB)'.
- At the bottom of the configuration area, there are two buttons: 'Save' (in blue) and 'Cancel' (in white).

BSS coloring

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

Target Wake Time (TWT)

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



Note

By default, BSS coloring and TWT is enabled.

Receive sensitivity configuration

This feature enables users to configure the receiver sensitivity per radio. The configuration hooks are exposed from both CLI and XMS-Cloud. The cnMaestro does not expose any hooks for configuring receiver configuration. The receiver configuration is the signal power required at the receiver to achieve the targeted or configured bit rate. Every RF receiver comes up with some default receiver sensitivity

which may or may not be sufficient for achieving required RF performance in terms of meeting bit rate, hence reconfiguration of receiver sensitivity is suggested.

Multicast-snooping and Multicast-to-Unicast conversion

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

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

CLI configuration:

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

-----Bridge Snooping Hash Table -- IPv4-----
NUM  GROUP                                FDB                                PORT  AGE
IPv4 Router Ports:      None

-----Bridge Snooping Hash Table -- IPv6-----
NUM  GROUP                                FDB                                PORT  AGE
IPv6 Router Ports:      None
XV3-8-EC7708(config)# service show mcastsnoop br0 acltbl

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

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

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

```

XV3-8-EC7708(config)# wireless radio 1
XV3-8-EC7708(config-radio-1)# multicast-to-unicast
XV3-8-EC7708(config-radio-1)# no multicast-to-unicast
XV3-8-EC7708(config-radio-1)# multicast-to-unicast mode 802.3
XV3-8-EC7708(config-radio-1)# multicast-to-unicast mode amsdu
XV3-8-EC7708(config-radio-1)# multicast-to-unicast exclude-list 224.0.0.1
XV3-8-EC7708(config-radio-1)# no multicast-to-unicast exclude-list 224.0.0.1
XV3-8-EC7708(config-radio-1)# show wireless radios multicast-to-unicast
=====
RADIO      BAND      MC2UC      MC2UC-MODE  EXCLUDE-LIST
=====
radio1     2.4GHz    NO         amsdu
radio2     5GHz      YES        amsdu
XV3-8-EC7708(config-radio-1)#

```

Chapter 7: Configuration - Wireless LAN

This chapter describes the following topics:

- [Overview](#)
- [Configuring WLAN parameters](#)
- [Link Aggregation Control Protocol \(LACP\)](#)
- [Radius attributes](#)
- [enhanced PSK \(ePSK\)](#)
- [RADIUS based ePSK](#)

Overview

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

Configuring WLAN parameters

Configurable parameters under WLAN profile are listed below:

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

Basic

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

Table 15: Configure: WLAN > Basic parameters

Parameters	Description	Range	Default
WLAN > Basic			
Enable	Option to enable a WLAN profile. Once enabled, a Beacon is broadcasted with SSID and respective configured parameters in a WLAN profile.	-	-
Mesh	This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. Four options are	-	OFF (Access)

Parameters	Description	Range	Default
	<p>available under this parameter:</p> <ol style="list-style-type: none"> 1. Base A WLAN profile configured with mesh-base will operate like a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients. 2. Client A WLAN profile configured with mesh-client will scan all available channels on startup, looking for a mesh-based AP to connect. 3. Recovery A WLAN profile configured as mesh-recovery will broadcast pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on mesh-base device. Meshclient will auto scan for mesh-recovery SSID upon failure of mesh link. 4. Off Mesh support disable on WLAN profile. 		Profile Mode)
SSID	SSID is the unique network name that wireless stations scans and associates.	-	-
VLAN	VLAN is configured to segregate wireless station traffic from AP traffic in the network. Wireless stations obtain IP address from the subnet configured in VLAN field of WLAN profile.	1-4094	1
Security	<p>This parameter determines key values that is encrypted based on selected algorithm. Following security methods are supported by Enterprise Wi-Fi AP devices:</p> <ol style="list-style-type: none"> 1. Open This method is preferred when Layer 2 authentication is built in the network. With this configured on Enterprise Wi-Fi AP device, any wireless station will be able to connect. 2. Osen This method is extensively used when Passpoint 2.0 is enabled on Enterprise Wi-Fi AP devices. If Passpoint 2.0 is disabled, this security plays no role in wireless station association. 3. WPA2-Pre-Shared Keys This mode is supported with AES and TKIP encryption. WPA-TKIP can be enabled from the CLI with the "allow-tkip" CLI option. 	-	Open

Parameters	Description	Range	Default
	<p>4. WPA2 Enterprise</p> <p>This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication method.</p> <p>5. WPA2/WPA3 Pre-shared Keys</p> <p>WPA2/WPA3 is a method of securing the network using WPA2/WPA3 with the use of the optional Pre-shared Key (PSK) authentication, that is designed for home users without an enterprise authentication server. To encrypt a network with WPA2/WPA3-PSK, the user to provide the router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. (E.g: Welcome@123).</p> <p>6. WPA3 Pre-shared Keys</p> <p>WPA3 security protocol provides a much more secure and reliable method replacing WPA2 and the older security protocols. WPA3 has further security improvements that make it harder to break into networks by guessing passwords.</p> <p>7. WPA3 Enterprise</p> <p>WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates mixing and matching of security protocols that are defined in 802.11 standard.</p> <p>8. WPA3 Enterprise CNSA</p> <p>WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates mixing and matching of security protocols that are defined in 802.11 standard. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite, and commonly used in high-security Wi-Fi networks in government, defence, Finance and industrial verticals.</p>		
Passphrase	String that is a key value to generate keys based on security method configured.	-	12345678
Radios	<p>Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options available to configure transmit mode of SSID:</p> <ul style="list-style-type: none"> • 2.4 GHz • 5 GHz • 6 GHz 	-	all
VLAN Pooling	This parameter is required when user requires to distribute clients across multiple subnets. Different modes of VLAN	–	Disabled

Parameters	Description	Range	Default
	<p>pooling is supported by Enterprise Wi-Fi AP devices, based on infrastructure available at deployment site. Modes supported are as follows:</p> <ol style="list-style-type: none"> 1. Disabled This feature is disabled for this WLAN. 2. Radius Based User is expected to configure WPA2 Enterprise for this mode to support. During association phase, AP obtains pool name form RADIUS transaction and based on present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IP address from the VLAN selected by Enterprise Wi-Fi AP device. 3. Static For this mode to support, user requires to configure VLAN Pool details available under Configure > Network > VLAN pool. During association phase, AP obtains pool and based on present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4 address from the VLAN selected by Enterprise Wi-Fi AP device. 		
Max Clients	This specifies the maximum number of wireless stations that can be associated to a WLAN profile. This varies based on Enterprise Wi-Fi AP device model number. Refer Table 16 for more details.	1-512 (Refer Table 16)	256
Client Isolation	<p>This feature needs to be enabled when there is a need for restriction of wireless station to station communication across the network or on an AP. Four options are available to configure based on requirement:</p> <ol style="list-style-type: none"> 1. Disable This option when selected disables client isolation feature. i.e. any wireless stations can communicate to other wireless stations. 2. Local This options when selected enables client isolation feature. This option prevents wireless station communications connected to same AP. 3. Network Wide 		

Parameters	Description	Range	Default
	<p>This options when selected enables client isolation feature. It prevents wireless stations communications connected to different AP deployed in same L2 network.</p> <p>Note:</p> <ul style="list-style-type: none"> • Network wide mode is not supported when Redundancy Gateway protocol is used on deployment. • In Redundancy Gateway case, Network wide static can be used providing list of Gateway MAC addresses. <p>4. Network Wide Static</p> <p>This option when configured enables client isolation feature across network. Wireless stations can communicate only to statically added MAC list. Communication to rest other MAC addresses are blocked.</p> <p>Note: When Network Wide and Network Wide Static selected, user has the provision to add the whitelist MAC addresses to allow the communication. A maximum 64 MAC addresses can be added.</p>		
cnMaestro Managed Roaming	Provision to enable centralized management of roaming for wireless clients through cnMaestro.	-	-
Hide SSID	This is the basic security mode of a Wi-Fi device. This parameter when enabled, will not broadcast SSID.	-	Disabled
Session Timeout	This field is specific to non-guest wireless stations. When a wireless station connects, a session timer is triggered. Once session time expires, wireless station must undergo either re-authentication or re-association based on state of wireless station. By default, it is enabled.	60-604800	28800
Inactivity Timeout	Inactivity timer triggers whenever there is no communication between Enterprise Wi-Fi AP device and wireless station associated to Enterprise Wi-Fi AP device. Once the timer reaches the configured Inactivity timeout value, APs sends a de-authentication to that wireless station. By default, it is enabled.	60-28800	1800

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

1. Select the **Enable** checkbox to enable a particular WLAN.
2. Enter the SSID name for this WLAN in the **SSID** textbox.

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

Table 16: WLAN (Max clients) parameters

Number of clients	2.4 GHz	5 GHz	6 GHz	Concurrent
XV3-8	512	512	NA	1024
XV2-2	512	512	NA	1024
XV2-2T	512	512	NA	1024
XE3-4	512	512	512	1536
e410/e430 and e510	256	256	NA	256
e600 and e700	512	512	NA	512

Figure 12: Configure: WLAN > Basic parameter

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

Basic

Enable
☒

Mesh
Off
Mesh Base/Client/Recovery mode

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

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

SSID
1212
The SSID of this WLAN (upto 32 characters)

Security
WPA2 Pre-shared Keys
Set Authentication and encryption type

Passphrase

WPA2 Pre-shared Security passphrase or key

VLAN Pooling
Disable
Configure VLAN pooling

Max Clients
256
Default maximum Client assigned to this WLAN. (1-512)

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

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

Hide SSID
☐ Do not broadcast SSID in beacons

Session Timeout
28800
Session time in seconds (60 to 604800)

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

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

Table 17: Configure: WLAN > Advanced parameters

Parameters	Description	Range	Default																														
WLAN > Advanced																																	
UAPSD	<p>When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming etc. is in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by Enterprise Wi-Fi AP device.</p> <table><tr><th>Priority</th><th>802.1D Priority (= UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr><tr><td rowspan="8"><div>lowest</div><div>↓</div><div>highest</div></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	<div>lowest</div> <div>↓</div> <div>highest</div>	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																													
<div>lowest</div> <div>↓</div> <div>highest</div>	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 of channel usage by AP, so that smart wireless station can decide better AP for connectivity. Station count, Channel utilization and Available admission capacity are the information available in this IE.	–	Disabled
DTIM interval	This parameter plays a key role when power save supported mobile stations are part of infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.	1-255	1
Monitored Host			
Host	This feature is required where there is 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 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	This feature is required when an Administrator requires to monitor the websites accessed by wireless stations connected to WLAN profile.	–	Disabled
Connection Logging Host	When enabled provides information of all TCP connections accessed by a wireless station that is associated to WLAN.	–	Disabled
Band Steering ¹	This feature when enabled, steers wireless stations to connect to 5GHz. There are three modes supported by Enterprise Wi-Fi device. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces wireless station to connect to 5GHz band. <ul style="list-style-type: none"> • Low • Normal • Aggressive 	–	Disabled
Proxy ARP	Provision to avoid ARP flood in wireless network. When enabled, AP responds to ARP requests for the wireless stations connected to that AP. This is for IPv4 infrastructure.	–	Enabled
Insert DHCP Option 82	When enabled, DHCP packets generated from wireless stations that are associated to APs are appended with Option 82 parameters. Option 82 provides provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID: <ul style="list-style-type: none"> • Hostname 	–	Disabled

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom • All 		
Tunnel Mode	This option is enabled when user traffic is tunneled to DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	<p>One of the important aspects to support voice applications on Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 msec to avoid any call drop. This is easily achievable when WPA2-PSK security mechanism is in use. However, in enterprise environments there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with AAA server and hence depending on the location of AAA server the roaming-time will be above 700 msec.</p> <p>Select any one of the following:</p> <ol style="list-style-type: none"> 1. OKC This roaming method is a proprietary solution to bring scalability to the roaming problem. This method avoids the need to authenticate with AAA server every time a client moves to new AP. 2. 802.11r Fast transition (FT) is a 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. Two modes of FT roaming are supported: <ul style="list-style-type: none"> • Over-the-Air 	–	Disabled
RRM (802.11k) ²	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 11k clients.	–	Disabled

Parameters	Description	Range	Default
	Following parameter needs to be enabled: <ul style="list-style-type: none"> • Enable RRM 		
802.11v ³	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF (802.11w)	802.11w, also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames makes wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	–	Optional
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms
Association Comeback Time	This value is included in the Association Response as an Association Comeback Time information element. AP will deny association for the configured interval.	1-20	1 Sec

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

1. Select the **UAPSD** checkbox to enable UAPSD.
2. Select the **QBSS** checkbox to enable QBSS.
3. Enter the value in the **DTIM interval** textbox to configure DTIM interval.
4. Enter IP address or Hostname in **Host** textbox.
5. Enter **Interval time** duration in the textbox.
6. Select number of attempts to check the reachability of monitored host in the **Attempts** drop-down list.
7. Enter the FQDN or IP address of the Server where all the client DNS requests will be logged in the **DNS Logging Host** server along with customized port number in the textbox. If the port number is not entered, AP will take default value as 514.
8. Enter the FQDN or IP address of the Server where all wireless client connectivity events/logs will be displayed in the configured **Connection Logging Host** server along with customized port number in the textbox. If the port number is not entered, AP will take default value as 514.
9. Select **Band Steering** parameter for 5GHz band from the drop-down list.
10. Enable **Proxy ARP** checkbox to avoid ARP flood in wireless network.
11. Enable **Insert DHCP Option 82** checkbox.
12. Select **Option 82 Circuit ID** to enable DHCP Option-82 from the drop-down list.
13. Select **Option 82 Remote ID** to choose the MAC address of the AP from the drop-down list.
14. Select **Tunnel Mode** checkbox to enable tunnelling of WLAN traffic over configured tunnel.

15. Enable the required OKC or 802.11r configure roaming protocol in the **Fast-Roaming Protocol** checkbox.
16. Enable **RRM (802.11k)** checkbox.
17. Enable **802.11v** checkbox.
18. Select **PMF (802.11w)** parameter from the drop-down list.
 - a. Enter **SQ Query Retry Time** in the textbox.
 - b. Enter **Association Comeback Time** in the textbox.
19. Click **Save**.

Figure 13: Configure: WLAN > Advanced parameter

Advanced

UAPSD ☒ Enable UAPSD

QBSS ☒ Enable QBSS load element

DTIM interval Number of beacons (1-255)

Monitored Host

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

Interval Duration in seconds (60-3600)

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

DNS Logging Host Port Syslog server where all client DNS requests will be logged

Connection Logging Host Port Syslog server where all client connection requests will be logged

Band Steering Steer dual-band capable clients towards 5GHz radio

Proxy ARP ☒ Respond to ARP requests automatically on behalf of clients

Proxy ND ☐ Respond to IPv6 ND requests automatically on behalf of clients

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

Insert DHCP Option 82 ☒ Enable DHCP Option 82

Option 82 Circuit ID

Option 82 Remote ID

Tunnel Mode ☐ Enable tunnelling of WLAN traffic over configured tunnel

Fast-Roaming Protocol ☐ OKC ☐ 802.11r Configure roaming protocol

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

802.11v ☐ Enable 802.11v BSS Transition Management

Note¹: Band steering also support client load balancing based on the below CLI configuration:

```
XV3-8-376FDC(config)#
XV3-8-376FDC(config)# wireless wlan 1
XV3-8-376FDC(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
```

802.11k/v

802.11k²

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 neighbor report from the AP using 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 provide the list of neighbors to the client in the neighbor_report_rsp message.

802.11v³

802.11v is deployed on the APs to govern the wireless networking transmission methods. It allows client 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 client is expected to respond back with the best APs in the vicinity to assist the client in roaming. The neighbor information is collected using proprietary methods.

Radius server

[Table 4](#) lists configurable fields that are displayed in the **Configuration > WLAN > > Radius Server** tab:

Table 18: Configure: WLAN > 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. Maximum of three RADIUS server can be configured.	-	Disabled
Accounting Server	Provision to configure Accounting server details such as Hostname/IPv4, Shared Secret, Port Number. Maximum of three RADIUS server can be configured.	-	Disabled
Timeout	Wait time period for response from AAA server.	1-30	3
Attempts	Parameter to configure number of attempts that a device should send AAA request to server if no response is received within configured timeout period.	1-3	1
Accounting Mode	This field is enabled based on customer requirement. Accounting packet is transmitted based on mode selected.	-	Disabled

Parameters	Description	Range	Default
	<ol style="list-style-type: none"> 1. Start-Stop Accounting packets are transmitted by AP to AAA server when a wireless station is connected and then disconnects. 2. Start-Interim-Stop Accounting packets are transmitted by AP to AAA server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects. 3. None Accounting mode will be disabled. 		
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Server Pool Mode	<p>User can configure multiple Authorization and Accounting servers. Based on number of wireless stations, user can choose Failover mode.</p> <ol style="list-style-type: none"> 1. Failover AP selects the RADIUS server which is up and running based on the order of configuration. 	-	Failover
NAS Identifier	This is configurable parameter and is appended in RADIUS request packet.	-	Hostname/ System Name
Dynamic Authorization	This option is required, where there is a CoA requests from AAA/RADIUS server.	-	Disabled
Dynamic VLAN	When enabled, AP honors the VLAN information provided in RADIUS transaction. Wireless station requests IP address from the same VLAN learnt through RADIUS.	-	Enabled
Called Station ID	<p>Following information can be communicated to RADIUS server:</p> <ul style="list-style-type: none"> • 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 	-	AP-MAC: SSID

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> CUSTOM 		

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

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

Figure 14: Configure: WLAN > Radius Server parameter

Basic	Radius Server	Guest Access	Usage Limits	Scheduled Access	Access	Passpoint	Delete
<div>Authentication Server 1</div> <div> <div>Host</div> <div>10.110.211.50</div> </div> <div> <div>Secret</div> <div>*****</div> </div> <div> <div>Port</div> <div>1812</div> </div> <div> <div>Realm</div> <div></div> </div>							
<div>2</div> <div> <div>Host</div> <div></div> </div> <div> <div>Secret</div> <div></div> </div> <div> <div>Port</div> <div>1812</div> </div> <div> <div>Realm</div> <div></div> </div>							
<div>3</div> <div> <div>Host</div> <div></div> </div> <div> <div>Secret</div> <div></div> </div> <div> <div>Port</div> <div>1812</div> </div> <div> <div>Realm</div> <div></div> </div>							
<div>Timeout</div> <div>3</div> <div>Timeout in seconds of each request attempt (1-30)</div>							
<div>Attempts</div> <div>1</div> <div>Number of attempts before giving up (1-3)</div>							
<div>Accounting Server 1</div> <div> <div>Host</div> <div></div> </div> <div> <div>Secret</div> <div></div> </div> <div> <div>Port</div> <div>1813</div> </div>							
<div>2</div> <div> <div>Host</div> <div></div> </div> <div> <div>Secret</div> <div></div> </div> <div> <div>Port</div> <div>1813</div> </div>							
<div>3</div> <div> <div>Host</div> <div></div> </div> <div> <div>Secret</div> <div></div> </div> <div> <div>Port</div> <div>1813</div> </div>							
<div>Timeout</div> <div>3</div> <div>Timeout in seconds of each request attempt (1-30)</div>							
<div>Attempts</div> <div>1</div> <div>Number of attempts before giving up (1-3)</div>							
<div>Accounting Mode</div> <div>None</div> <div>Configure accounting mode</div>							
<div>Accounting Packet</div> <div><input type="checkbox"/> Enable Accounting-On messages</div>							
<div>Sync Accounting Records</div> <div><input type="checkbox"/> Configure accounting records to be synced across neighboring AP's</div>							
<div>Server Pool Mode</div> <div> <input checked="" type="radio"/> Load Balance Load balance requests equally among configured servers <input type="radio"/> Failover Move down server list when earlier servers are unreachable </div>							
<div>NAS Identifier</div> <div>AP-HOSTNAME</div> <div>NAS-Identifier attribute for use in Request packets. Defaults to system name</div>							
<div>Interim Update Interval</div> <div>1800</div> <div>Interval for RADIUS Interim-Accounting updates (10-65535 Seconds)</div>							
<div>Dynamic Authorization</div> <div><input type="checkbox"/> Enable RADIUS dynamic authorization (COA, DM messages)</div>							
<div>Dynamic VLAN</div> <div><input checked="" type="checkbox"/> Enable RADIUS assigned VLANs</div>							
<div>Proxy through cnMaestro</div> <div><input type="checkbox"/> Proxy RADIUS packets through cnMaestro (on-premises) instead of directly to the RADIUS server from the AP</div>							
<div>Called Station ID</div> <div>AP-MAC.SSID</div> <div>Configure AP-MAC.SSID as Called-Station-Id in the RADIUS packet</div>							
<div>Save Cancel</div>							

Guest Access

Internal Access Point

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

Table 19: Configure: WLAN > Guest Access > Internal Access Point parameters

Parameters	Description	Range	Default
WLAN > Guest Access > Internal Access Point			
Enable	Enables the Guest Access feature.	-	Disabled
Access Policy	<p>There are four types of access types provided for the user:</p> <ol style="list-style-type: none">1. Clickthrough This mode allows the users to get access data without any authentication mechanism. User can access internet as soon as he is connected and accepts Terms and Conditions2. RADIUS This mode when selected, user has to provide username and password, which is then redirected to RADIUS server for authentication. If successful, user is provided with data access.3. Local Guest Account User must configure username and password on device, which has to be provided in the redirection page for successful authentication and data access.	-	Clickthrough
Redirect Mode	<p>This option helps the user to configure the HTTP or HTTPS mode of redirection URL.</p> <ol style="list-style-type: none">1. HTTP AP sends a HTTP POSTURL to the associated client, which will be <a href="http://<Pre-defined-URL>">http://<Pre-defined-URL>.2. HTTPS AP sends HTTPS POSTURL to the successful associated client, which will be <a href="https://<Pre-defined-URL>">https://<Pre-defined-URL>.	-	HTTP
Redirect	User can configure a friendly hostname, which is	-	-

Parameters	Description	Range	Default
Hostname	added in DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with IP address in the redirection URL provided to wireless stations.		
Title	User can configure a Title to the splash page. Configured text in this parameter will be displayed in the redirection page. This text is usually Bold.	Up to 255 characters	Welcome To Cambium Powered Hotspot
Contents	User can configure the contents of Splash page using this field. Displays the text configured under the Title section of redirection page.	Up to 255 characters	Enter username and password to get Web Access
Terms	Splash page displays the text configured when user accepts Terms and Agreement.	Up to 255 characters	-
Logo	Displays the logo image updated in URL http (s)://<ipaddress>/logo.png. Either PNG or JPEG format of logo are supported.	-	-
Background Image	Displays the background image updated in URL http (s)://<ipaddress>/backgroundimage.png. Either PNG or JPEG format of logo are supported.	-	-
Success Action	<p>Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL:</p> <ol style="list-style-type: none"> 1. Internal Logout Page After successful login, wireless client is redirected to logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to URL which is configured on device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to URL that is accessed by user before successful captive portal authentication. 	-	Internal Logout page
Redirect user to External URL	<p>Provision to configure re-direction URL after successful login and an additional information of AP and wireless station information can be appended in the URL.</p> <ul style="list-style-type: none"> • Prefix Query Strings in Redirect URL 	-	-

Parameters	Description	Range	Default
	<p>This option is selected by default. Following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> • SSID • AP MAC • NAS ID • AP IP • Client MAC • Redirection URL • User can provide either HTTP or HTTPS URL 		
Redirection user to Original URL	<p>Users will be redirected to URL that is accessed by user before successful captive portal authentication. There is additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below:</p> <ul style="list-style-type: none"> • Prefix Query Strings in Redirect URL <p>This option is selected by default. Following information is appended in the redirection URL:</p> <ul style="list-style-type: none"> • SSID • AP MAC • NAS ID • AP IP • Client MAC 	-	-
Success message	Provision to configure text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	-	-
Redirect	<ul style="list-style-type: none"> • If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPS URLs will be redirected to Guest Access login page. 	-	Enabled
Redirect User Page	IPv4 address configured in this field is used as logout URL for Guest Access sessions. IPv4 address configured should be not reachable to internet.	-	1.1.1.1
Proxy	Proxy port can be configured with which proxy	1 - 65535	-

Parameters	Description	Range	Default
Redirection Port	server is enabled. This allows URL's accessed with proxy port to be redirected to login page.		
Session Timeout	This is the duration of time, client will be allowed to access internet if quota persists, after which AP sends de-authentication. Wireless station has to undergo Guest Access authentication after session timeout.	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to Guest Access login page after any supported type of MAC address authentication fails.	-	Disabled
Extend Interface	Provision to support Guest Access on Ethernet interface.	-	Disabled
Whitelist	Provision to configure either IPv4 or URLs to bypass traffic, therefor user can access those IPs or URLs without Guest Access authentication.	-	-
Captive Portal bypass User Agent	Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.	-	-

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

1. Select **Enable** checkbox to enable the Guest Access feature.
2. Enable **Internal Access Point** checkbox.
3. Enable the required access types from the **Access Policy** checkbox.
4. Enable HTTP or HTTPS from the **Redirect Mode** checkbox.
5. Enter **Redirect Hostname** in the textbox.
6. Enter the title to appear in the splash page in the **Title** textbox.
7. Enter the content to appear in the splash page in the **Contents** textbox.
8. Enter the terms and conditions to appear in the splash page in the **Terms** textbox.
9. Enter the logo to be displayed in the **Logo** textbox.
10. Select the **Background Image** to be displayed on the splash page in the textbox.
11. Enable configured modes of redirection URL in **Success Action** checkbox.
12. Enter **Success message** to appear in the textbox.

13. Enable **Redirect** checkbox for HTTP packets.
14. Enter configuring IP address in the **Redirect User Page** textbox.
15. Enter Port number in **the Proxy Redirection Port** textbox.
16. Enter the session timeout in seconds in the **Session Timeout** textbox.
17. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.
18. Enable **MAC Authentication Fallback** checkbox if guest-access is used only as fallback for clients failing MAC-authentication.
19. Enter the name of the interface that is extended for guest access in **the Extend Interface** textbox.
20. Click **Save**.

To configure Whitelist parameter:

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

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

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

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

Basic
Radius Server
Guest Access
Usage Limits
Scheduled Access
Access
Passpoint

Enable
☐

Portal Mode
☒ Internal Access Point
☐ External Hotspot
☐ cnMaestro

Access Policy
☒ Clickthrough
☐ Radius
☐ LDAP
☐ Local Guest Account

Redirect Mode
☒ HTTP
☐ HTTPS

Redirect Hostname

Title

Contents

Terms

Logo

Background Image

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

Success message

Redirect
☒ HTTP-only

Redirect User Page

Proxy Redirection Port

Session Timeout

Inactivity Timeout

MAC Authentication Fallback
☐

Extend Interface

Save
Cancel

Add Whitelist
Captive Portal bypass User Agent

IP Address or Domain Name
Save

IP Address Domain Name	Action
No white list available	

Items per page

External Hotspot

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

Table 20: Configure: WLAN > Guest Access > External Hotspot parameters

Parameters	Description	Range	Default
WLAN > Guest Access > External Hotspot			
Access Policy	<p>There are four types of access types provided for the end user:</p> <ol style="list-style-type: none">1. Clickthrough This mode allows users to get access data without any authentication mechanism. User can access internet as soon as he is connected and accepts Terms and Conditions.2. RADIUS User has to provide username and password, which is then redirected to RADIUS server for authentication. If successful, user is provided with data access.3. Local Guest Account User has to configure username and password on device, which has to be provided in the redirection page for successful authentication and data access.	–	Clickthrough
LDAP Server baseDN	Provision to configure the point from where the server will search for users.	–	–
LDAP Server adminDN	Provision to configure the Admin Domain which binds with LDAP server for successful search of LDAP/AD server.	–	–
Redirect Mode	<p>Provision to configure the HTTP or HTTPS mode of redirection URL.</p> <ol style="list-style-type: none">1. HTTP AP sends a HTTP POSTURL to the associated client, which will be <a href="http://<Pre-defined-URL>">http://<Pre-defined-URL>.2. HTTPS AP sends HTTPS POSTURL to the successful associated client, which will be <a href="https://<Pre-defined-URL>">https://<Pre-defined-URL>.	–	HTTP

Parameters	Description	Range	Default
Redirect Hostname	User can configure a friendly hostname, which is added in DNS server and is resolvable to Enterprise Wi-Fi AP IP address. This parameter once configured will be replaced with IP address in the redirection URL provided to wireless stations.	-	-
External Page URL	User can configure landing/login page which is posted to wireless stations that are not Guest Access authenticated.	-	-
External Portal Post Through cnMaestro	This is required when HTTPS is only supported by external guest access portal. This option when enabled minimizes certification. Certificate is required to install only in cnMaestro On-Premises.	-	Disabled
External Portal Type	Enterprise Wi-Fi AP products are supported by standard mode configuration. 1. Standard This mode is selected, for all third-party vendors whose Guest Access services is certified and integrated with Enterprise Wi-Fi AP products.	-	Standard
Success Action	Provision to configure redirection URL after successful login to captive portal services. User can configure three modes of redirection URL: 1. Internal Logout Page After successful login, Wireless client is redirected to logout page hosted on AP. 2. Redirect user to External URL Here users will be redirected to URL which is configured on device in Redirection URL configurable parameter. 3. Redirect user to Original URL Here users will be redirected to URL that is accessed by user before successful captive portal authentication.	-	Internal Logout Page
Redirect user to External URL	Provision to configure re-direction URL after successful login and an additional information of AP and wireless station information can be appended in the URL. • Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: ◦ SSID	-	-

Parameters	Description	Range	Default
	<ul style="list-style-type: none"> ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC • Redirection URL User can provide either HTTP or HTTPS URL. 		
Redirection user to Original URL	<p>Users will be redirected to URL that is accessed by user before successful captive portal authentication. There is additional parameter Prefix Query Strings in Redirection URL that is enabled by default and details given below:</p> <ul style="list-style-type: none"> • Prefix Query Strings in Redirect URL This option is selected by default. Following information is appended in the redirection URL: <ul style="list-style-type: none"> ◦ SSID ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC 	–	–
Success message	Provision to configure text to display upon successful Guest Access authentication. This is applicable only when Success Action mode is Internal Logout Page.	–	–
Redirection URL Query String	<p>Following information is appended in the redirection URL, if “Prefix Query Strings in Redirect URL” is enabled.</p> <ul style="list-style-type: none"> • Client IP • RSSI • AP Location 	-	Disabled
Redirect	<ul style="list-style-type: none"> • If enabled, only HTTP URLs will be redirected to Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page. 	–	Enabled
Redirect User Page	IP address configured in this field is used as logout/disconnect/redirect to captive portal URL for Guest Access sessions. IP address configured should not be reachable to internet.	–	1.1.1.1

Parameters	Description	Range	Default
Proxy Redirection Port	Proxy port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.	1 - 65535	–
Session Timeout	This is the duration of time, client will be allowed to access internet if quota persists, after which AP sends de-authentication. Wireless station has to undergo Guest Access authentication after session timeout.	60 - 2592000	28800
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
MAC Authentication Fallback	It is a mechanism in which wireless stations will be redirected to Guest Access login page after any supported type of MAC address authentication failures.	–	Disabled

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

1. Enable the required access types from the **Access Policy** checkbox.
2. Enable HTTP or HTTPS from the **Redirect Mode** checkbox.
3. Enter Redirect Hostname in the textbox.
4. Enter **External Page URL** in the textbox.
5. Enable **External Portal Post Through cnMaestro** checkbox.
6. Select External Portal Type from the drop-down list.
7. Enable configured modes of redirection URL in **Success Action** checkbox.
8. Enter **Success message** to appear in the textbox.
9. Enable the required **Redirection URL Query String** checkbox.
10. Enable **Redirect** checkbox for HTTP packets.
11. Enter configuring IP address in the **Redirect User Page** textbox.
12. Enter Port number in the **Proxy Redirection Port** textbox.
13. Enter the session timeout in seconds in the **Session Timeout** textbox.
14. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.
15. Select the **MAC Authentication Fallback** checkbox if guest-access is used only as fallback for clients failing MAC-authentication.
16. Click **Save**.

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

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

Enable
☐

Portal Mode
☐ Internal Access Point
☒ External Hotspot
☐ cnMaestro
☐ XMS/Easypass

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

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

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

WISPr Clients External Server Login
☐

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

External Portal Post Through cnMaestro
☐

External Portal Type

Standard

External Portal Type Standard/XWF

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

Success message

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

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

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

Proxy Redirection Port
Port number(1 to 65535)

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

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

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

Extend Interface
Configure the interface which is extended for guest access

Save
Cancel

White List
Captive Portal Bypass User Agent

IP Address or Domain Name
Save

IP Address | Domain Name
Action

No white list available

1 / 1
10 items per page

cnMaestro

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

Table 21: Configure: WLAN > Guest Access > cnMaestro parameters

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	–	–
Redirect	<ul style="list-style-type: none">If enabled, only HTTP URLs will be redirected to Guest Access login page.If disabled, both HTTP and HTTPS URLs will be redirected to Guest Access login page.	–	Enabled
Redirect User Page	IP address configured in this field is used as logout URL for Guest Access sessions. IP address configured should be not reachable to internet.	–	1.1.1.1
Proxy Redirection Port	Proxy port can be configured with which proxy server is enabled. This allows URL's accessed with proxy port to be redirected to login page.	1 - 65535	–
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but no data traffic. AP starts timer when there is no data received from a wireless station and disconnects when timer reaches 0.	60 - 2592000	1800
Extend Interface	Provision to support Guest Access on Ethernet interface.	–	Disabled
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	–	–
Captive Portal bypass User Agent	Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.	–	–

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

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

6. Enter the name of the interface that is extended for guest access in the **Extend Interface** textbox.
7. Click **Save**.

To configure the **Whitelist parameter**:

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

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

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

Figure 17: Configure: WLAN > Guest Access > cnMaestro parameter

BasicRadius ServerGuest AccessUsage LimitsScheduled AccessAccessPasspointDelete

Enable☒

Portal Mode

☐ Internal Access Point☐ External Hotspot☒ cnMaestro☐ XMS/Easypass

Guest Portal Name

Eg: cnMaestro-guest-portal

Guest Portal Name which is hosted on cnMaestro

Redirect

☒ HTTP-only Enable redirection for HTTP packets only

Redirect User Page

1.1.1.1

Configure IP address for redirecting user to guest portal splash page

Proxy Redirection Port

Port number(1 to 65535)

Inactivity Timeout

1800

Inactivity time in seconds (60 to 2592000)

MAC Authentication Fallback

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

Extend Interface

Configure the interface which is extended for guest access

SaveCancel

White ListCaptive Portal Bypass User Agent

IP Address or Domain Name

Save

IP Address | Domain Name

Action

No white list available

1

/ 1

10

Items per page

Chapter 7: Configuration - Wireless LAN

72

XMS/EasyPass

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

Table 22: Configure: WLAN > Guest Access > XMS/EasyPass parameters

Parameters	Description	Range	Default
External Page URL	User can configure login page which is posted to wireless stations that are not Guest Access authenticated.	–	–
Secret	Provision to configure the secret to be used during redirection.	–	–
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	–	–
Captive Portal bypass User Agent	Provision to limit the auto-popup to a certain browser as configured based on User-agent of browsers.	–	–

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

1. Enter **External Page** URL in the textbox.
2. Enter **Secret** to be used during redirection in the textbox.
3. Click **Save**.

To configure the Whitelist parameter:

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

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

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

Figure 18: Configure: WLAN > Guest Access > XMS/EasyPass

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

Enable ☐

Portal Mode ☐ Internal Access Point ☐ External Hotspot ☐ cnMaestro ☒ XMS/Easypass

External Page URL
URL of external splash page

Secret
Configure the secret to be used during redirection

Save Cancel

White List Captive Portal Bypass User Agent

IP Address or Domain Name Save

IP Address Domain Name	Action
No white list available	

1 / 1 10 items per page



Note

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



Note

For more information about cnMaestro Guest Access Portal and onboarding, refer cnMaestro [Guest Access portal](#).

Usage Limits

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

Table 23: Configure: WLAN > Usage Limits parameters

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

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

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


Figure 19: Configure: WLAN > Usage Limits parameters

The screenshot shows the 'Usage Limits' configuration page. It features two main sections: 'Rate Limit per Client' and 'Rate Limit per WLAN'. Each section contains input fields for 'Upstream' and 'Downstream' rates, with unit dropdown menus set to 'Kbps'. The values entered in the input fields are '0'. At the bottom of the form are 'Save' and 'Cancel' buttons. The top of the page shows a navigation bar with tabs: 'Basic', 'Radius Server', 'Guest Access', 'Usage Limits' (active), 'Scheduled Access', 'Access', 'Passpoint', and a 'Delete' button.

Scheduled Access

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

Table 24: Configure: WLAN > Scheduled Access parameters

Parameters	Description	Range	Default
Scheduled Access	Provision to configure the availability of Wi-Fi services for a selected time duration. Enterprise Wi-Fi AP has capability of configuring the availability of Wi-Fi services on all days or on specific day (s) of a week. Time format is in Hours. <div>  <p>Note From System Release 6.3 onwards, user can configure up to a maximum of twelve schedule access rules per day on a particular WLAN instead of 1 rule per day.</p> </div>	00:00 Hrs. - 23:59 Hrs.	Disabled

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

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

Figure 20: Configure: WLAN > Scheduled Access parameters

Basic
Radius Server
Guest Access
Usage Limits
Scheduled Access
Access
Passpoint

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

Start Time

End Time

HH:MM format

Start Time

End Time

HH:MM format

Start Time

End Time

HH:MM format

Start Time

End Time

HH:MM format

Start Time

End Time

HH:MM format

Start Time

End Time

HH:MM format

Start Time

End Time

HH:MM format

Save

Cancel

CLI configuration:

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

all           : all
friday        : friday
monday        : monday
saturday      : saturday
sunday        : sunday
thursday      : thursday
tuesday       : tuesday
wednesday     : wednesday
weekday       : weekday
weekend       : weekend

XV3-8-EC7708(config-wlan-1)# scheduled-access all

Time period in HH:MM-HH:MM,HH:MM-HH:MM format
```

Access

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

Table 25: Configure: WLAN > Access parameters

Parameters	Description	Range	Default
DNS-ACL			
Precedence	Provision to configure index of ACL rule. Packets are validated and processed based on Precedence value configured.	-	1
Action	Provision to configure whether to allow or deny traffic.	-	Deny
Domain	Provision to configure domain names and rules are applied based on Action configured.	-	-
MAC Authentication			
MAC Authentication Policy	Enterprise Wi-Fi AP supports multiple methods of MAC authentication. Following are the details of each mode: 1. Permit Wireless station MAC addresses listed will be allowed to associate to AP. 2. Deny When user configures a MAC address, those wireless station shall be denied to associate and the non-listed MAC address will be allowed.	-	Deny

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

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

To configure **DNS ACL**:

1. Select **Precedence** from the drop-down list.
2. Select type of action from **Action** drop-down list.
3. Enter 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 21: Configure: WLAN > Access parameters

Passpoint

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

Table 26: Configure: WLAN > Passpoint parameters

Parameters	Description	Range	Default
Configuration > Hotspot2.0 / Passpoint			
Enable	Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning.	–	Disabled
DGAF	Downstream Group Addressed Forwarding, when enabled the WLAN doesn't transmit any multicast and broadcast packets.	–	Disabled

Parameters	Description	Range	Default
ANQP Domain ID	ANQP domain identifier included when the HS 2.0 indication element is in Beacon and Probe Response frames.	0-65535	0
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: <ul style="list-style-type: none"> • Private • Chargeable Public • Emergency Services • Free Public • Personal Device • Private with Guest • Test • Wildcard 	–	Private
ASRA	Indicates that the network requires a further step for access.	–	Disabled
Internet	The network provides connectivity to the Internet if not specified.	–	Disabled
HESSID	Configures the desired specific HESSID network identifier or the wildcard network identifier.	–	–
Venue Info	Configure venue group and venue type.	–	–
Roaming Consortium	The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP.	–	–
ANQP Elements	Select any one of the following: <ul style="list-style-type: none"> • 3GPP Cellular Network Information • Connection Capability • Domain Name List • Icons • IP Address Type information • NAI Realm List • Network Authentication Type • Operating Class Indication • Operator Friendly Names • OSU Provider List • Venue Name Information • WAN Metrics 	–	–

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

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

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

Figure 22: Configure: WLAN > Passpoint parameters

Configuration

Hotspot2.0 / Passpoint

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

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

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

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

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

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

Internet ☐ *The network provides connectivity to the Internet. Otherwise unspecified*

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

Venue Info *Configure Venue group and Venue type*

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

ANQP Elements (Access Network Query Protocol)

ANQP

Summary

Hotspot2.0 / Passpoint

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

Link Aggregation Control Protocol (LACP)

LACP provides ability to group multiple physical port as a logical port. The logical port is referred as port-channel and is supported only on XV3-8 devices.

Configuration:

Adding ethernet to port channels:

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

Port channel configuration:

```
XV3-8-EC7708(config)# interface portchannel 1
XV3-8-EC7708(config-portchannel-1)#

advertise      : Ethernet link speed advertisement
channel-group  : Ethernet member channel group
clear          : Clear command
duplex         : Ethernet link duplex
speed         : Ethernet link speed
switchport     : Configure switch port
tunnel-mode    : Enable tunnelling of wired traffic over configured tunnel

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

Syntax:

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

Radius attributes

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

Table 27: Radius attributes parameters

Type	Attribute Name	Attribute Number	Purpose
Standard	Acct-Interim-Interval	85	Specifies interval between accounting interim updates
Standard	Acct-Session-Id	44	Session identification (RFC 5176)
Standard	Calling-Station-Id	31	Session identification (RFC 5176)

Type	Attribute Name	Attribute Number	Purpose
Standard	Class	25	Accounting classification
Standard	Event-Timestamp	55	Replay protection (RFC 5176)
Standard	Filter-ID	11	<ul style="list-style-type: none"> 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 session is terminated
Standard	Tunnel-Type	64	Dynamic VLAN assignment (1 of 3 required), should be set to VLAN (Integer = 13)
Standard	Tunnel-Medium-Type	65	Dynamic VLAN assignment (2 of 3 required), should be set to 802 (Integer = 6)
Standard	Tunnel-Private-Group-ID	81	Dynamic VLAN assignment (3 of 3 required), should be set to the VLAN ID or name
Standard	User-Name	1	<ul style="list-style-type: none"> Station username update Session identification (RFC 5176)
Microsoft Vendor-Specific	MS-MPPE-Send-Key	16	Session key distribution
Microsoft Vendor-Specific	MS-MPPE-Recv-Key	17	Session key distribution
Cambium Vendor-Specific	Cambium-Vlan-Pool-Id	157	Radius based VLAN pool
Nas Port ID	NAS-Port-Id	87	NAS identification (RFC 5176)

enhanced PSK (ePSK)

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

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



Note:

eSPK scale is a [Premium feature](#) where user can configure more than 300 ePSK (1024) per WLAN and it is controlled by cnMaestro X.

RADIUS based ePSK

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 client session. This requires custom development on the RADIUS server.

Configuration CLI:

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

RADIUS                : Configure RADIUS based ePSK
username              : Configure Username

XV3-8-EC7708(config-wlan-1)# epsk RADIUS
XV3-8-EC7708(config-wlan-1)# save
[Config Save OK]
```

Chapter 8: Configuration - Network

This chapter describes the following topics

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

Overview

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

Configuring Network parameters

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

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

IPv4 network parameters

VLAN

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

Table 28: Configure: Network > VLAN > IPv4 parameters

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

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

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

To configure VLAN IPv4:

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

Figure 23: Configure: Network > VLAN > IPv4 parameters

The screenshot shows the 'VLAN' configuration page. At the top, there are tabs for 'VLAN', 'Routes', 'Ethernet Ports', 'Security', 'DHCP', 'Tunnel', 'PPPoE', and 'VLAN Pool'. The 'VLAN' tab is active. Below the tabs, there's a section for 'VLAN' with a dropdown menu set to 'VLAN 1' and buttons for 'Delete this interface' and 'Add new L3 Interface'. The 'IPv4' configuration section is highlighted with a red border. It contains the following fields and options:

- Address:** A dropdown menu set to 'DHCP'.
- NAT:** A checkbox labeled 'When NAT is enabled, IP addresses under this SVI are hidden'.
- Zeroconf IP:** A checkbox labeled 'Support 169.254.x.x local IP address'.
- DHCP Relay Agent:** A text input field with the value 'xxx.xxx.xxx.xxx' and a note 'Enables relay agent and assign DHCP server to it'.
- DHCP Option 82 Circuit ID:** A dropdown menu set to 'None'.
- DHCP Option 82 Remote ID:** A dropdown menu set to 'None'.
- Request Option All:** A checkbox labeled 'Enable dhcp request option all on this interface'.

Below the 'IPv4' section, there are tabs for 'IPv6' and 'General'.

DHCP Client Options

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

Table 29: DHCP Options

Options	Description	Usage	Reference CLI
Option 1	The subnet mask option specifies the client's subnet mask as per RFC 950.	Based on state of "Request Option All", device chooses subnet mask from respective VLAN interface.	show ip route
Option 3	This option specifies a list of IP addresses for routers on the client's subnet.	Based on state of "Request Option All", device chooses route learnt from respective VLAN interface. Only first route is honored	show ip route
Option 6	The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers SHOULD be listed in order of preference.	Based on state of "Request Option All", device chooses subnet mask from respective VLAN interface. Top two DNS servers are honored by Enterprise Wi-Fi AP device.	show ip name-server
Option 15	This option specifies the domain name that client should use when resolving hostnames via the Domain Name System.	More details are provided in Option 15.	show ip dhcp-client info

Options	Description	Usage	Reference CLI
Option 26	This option specifies MTU size in a network.	More details are provided in Configuration - Network.	show ip dhcp-client info
Option 28	This option specifies the broadcast address that client should use	Broadcast address learnt for all VLAN interfaces are used respectively as per standards	show ip dhcp-client-info
Option 43	This option is used to help the AP in obtaining cnMaestro IP address from the DHCP server while DHCP request to get an IP address is sent to the DHCP server.	More details are provided in Option 43 (cnMaestro On-Premises 2.4.0 User Guide).	show ip dhcp-client info
Option 51	This option is used in a client request to allow the client to request a lease time for the IP address. In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.	Enterprise Wi-Fi AP renew leases for all VLAN interfaces configured based on lease time that has been learned from DHCP server.	show ip dhcp-client info
Option 54	DHCP clients use the contents of the 'server identifier' field as the destination address for any DHCP messages unicast to the DHCP server.	Enterprise Wi-Fi AP learns DHCP server IP for all VLAN interfaces configured.	show ip dhcp-client info
Option 60	This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.	For Enterprise Wi-Fi AP device, value is updated as Cambium-Wi-Fi-AP.	show ip dhcp-client info

DHCP Option 43 - Zero touch onboarding

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

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

DHCP Option 43 format

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

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

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

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

**Note**

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

Routing and DNS

Table 30: Configure: Network > VLAN > Routing & DNS > IPv4 parameters

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

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

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

Figure 24: Routing & DNS > IPv4 parameters

Routing & DNS

IPv4

Default Gateway

IP address of default gateway

DNS Server 1

Primary Domain Name Server

DNS Server 2

Secondary Domain Name Server

Domain Name

Domain name

DNS Proxy

☐

DNS Proxy

IPv6

Save

Cancel

Routes

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

Table 31: Configure: Network > Routes> IPv4 parameters

Parameters	Description	Range	Default
Gateway Source Precedence	Provision to prioritize default gateway and DNS servers when Enterprise Wi-Fi AP device has learnt from multiple ways. Default order is Static and DHCP.	–	Static
Add Multiple Route Entries	User has provision to configure static Routes. Parameters that are required to configure static Routes are as follows: <ul style="list-style-type: none">• Destination IP• Mask• Gateway	–	–
Port Forwarding	This feature is required when wireless stations are behind NAT. User can access the services hosted on wireless stations using this feature. Following configurable parameters are required to gain the access of services hosted on wireless stations which are behind: <ul style="list-style-type: none">• Port• IP Address• Type	–	–

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

To configure Gateway Source Precedence:

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

To configure Add Multiple Route Entries:

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

To configure Port Forwarding:

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

Figure 25: Routes > IPv4 parameters

VLAN Routes Ethernet Ports Security DHCP Tunnel PPPoE VLAN Pool

Gateway Source Precedence

IPv4
STATIC
DHCP
PPPoE
Save

IPv6
STATIC
AUTO-CONFIG/DHCP
Save

Add Multiple Route Entries - IPv4

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

Destination IP	Mask	Gateway	Action
No routes available			

1 10 Items per page

Add Multiple Route Entries - IPv6

Destination IP/prefix: Gateway: Save

Destination IP	Gateway	Action
No routes available		

1 10 Items per page

Port Forwarding

Port: IP Address: Type: TCP Save

Port	IP Address	Protocol	Action
No rules available			

1 10 Items per page

IPv6 network parameters

VLAN

Table 32: Configure: Network > VLAN > IPv6 parameters

Parameters	Description	Range	Default
Address	Provision to configure mode of IPv6 address configuration for an interface selected. Five modes are supported: <ul style="list-style-type: none">• Disabled• AutoConfig• Static• Stateless DHCPv6• Stateful DHCpv6	–	AutoConfig
Request Option All	This configuration decides the interface on which AP will learn the following: <ul style="list-style-type: none">• IPv6 default gateway• DHCP client options like Option 52 and Option 24 (Controller discovery like controller host name / IPv6 address)• DNS Servers• Domain Name	–	Enabled on VLAN1

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

To configure **VLAN IPv6**:

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

Figure 26: Configure: Network > VLAN > IPv6 parameters

The screenshot shows the 'VLAN' configuration page. At the top, there are tabs for 'VLAN', 'Routes', 'Ethernet Ports', 'Security', 'DHCP', 'Tunnel', 'PPPoE', 'VLAN Pool', and 'WWAN'. The 'VLAN' tab is active. Below the tabs, there's a section for 'VLAN' with a dropdown menu set to 'VLAN 1' and a 'Delete this interface' button. To the right is a button 'Add new L3 Interface'. Below this, there are two expandable sections: 'IPv4' and 'IPv6'. The 'IPv6' section is expanded and highlighted with a red box. It contains a dropdown menu for 'Address' set to 'AutoConfig', a checkbox for 'Request Option All' which is checked, and a note: 'Use IPv6 Gateway, DNS, DHCPv6 options received on this interface'. Below the 'IPv6' section is a 'General' section.

Routing & DNS

Table 33: Configure: Network > VLAN > Routing & DNS > IPv6 parameters

Parameters	Description	Range	Default
Default Gateway	Provision to configure default gateway. If this is provided, Enterprise Wi-Fi AP device installs this gateway as this is the highest priority.	–	–
DNS Server	Provision to configure Static DNS server on Enterprise Wi-Fi AP device. Maximum of two DNS servers can be configured.	–	–
Domain Name	Provision to configure Domain Name. If this is provided, Enterprise Wi-Fi AP device installs this Domain Name as this is highest priority.	–	–
IPv6 Preference	When enabled, IPv6 is preferred over IPv4 bases on DNS response.	–	Disabled

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

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

Figure 27: Routing & DNS > IPv6 parameters

Routing & DNS

IPv4

IPv6

Default Gateway *IP address of default gateway*

DNS Server 1 *Primary Domain Name Server*

DNS Server 2 *Secondary Domain Name Server*

Domain Name *Domain name*

IPv6 Preference ☐ *Prefer IPv6 address over IPv4 for addresses resolved via DNS*

Save **Cancel**

Routes

Table 34: Configure: Network > Routes > IPv6 parameters

Parameters	Description	Range	Default
Gateway Source Precedence	Provision to prioritize default gateway and DNS servers when Enterprise Wi-Fi AP device has learnt from multiple ways. Default order is Static and AUTO-CONFIG/DHCP.	–	Static
Add Multiple Route Entries	User has provision to configure static Routes. Parameters that are required to configure static Routes are as follows: <ul style="list-style-type: none"> Destination IP/prefix Gateway 	–	–

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

To configure **Gateway Source Precedence**:

1. Select **STATIC** or **AUTO-CONFIG/DHCP** from the **Gateway Source Precedence** checkbox.
2. Click **Save**.

To configure **Add Multiple Route Entries**:

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

Figure 28: Figure 39 Routes > IPv6 parameters

VLAN

Routes

Ethernet Ports

Security

DHCP

Tunnel

PPPoE

VLAN Pool

WWAN

Gateway Source Precedence

IPv4

STATIC
DHCP
PPPoE

Save

IPv6

STATIC
AUTO-CONFIG/DHCP

Save

Add Multiple Route Entries - IPv4

Destination IP

Mask

Gateway

Save

Destination IP

Mask

Gateway

Action

No routes available

1 10 items per page

Add Multiple Route Entries - IPv6

Destination IP/prefix

Gateway

Save

Destination IP

Gateway

Action

No routes available

1 10 items per page

Port Forwarding

Port

IP Address

Type

Save

Port

IP Address

Protocol

Action

No rules available

1 10 items per page

General network parameters

Table 35: Configure: Network > VLAN > General parameters

Parameters	Description	Range	Default
Management Access	Provision to restrict the access of device in all modes CLI (Telnet, SSH), GUI (HTTP, HTTPS) and SNMP. User can configure restriction of device access as follows: <ul style="list-style-type: none"> Block Allow from Wired Allow from both wired and wireless 	–	Allow from both Wired and Wireless

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

Figure 29: Configure: Network > VLAN > General parameters

The screenshot shows the 'VLAN' configuration page with tabs for VLAN, Routes, Ethernet Ports, Security, DHCP, Tunnel, PPPoE, VLAN Pool, and WWAN. The 'VLAN' tab is active, showing 'Edit VLAN 1' and a 'Delete this interface' button. Below are sections for IPv4, IPv6, and General. The 'General' section is highlighted with a red box, showing 'Management Access' set to 'Allow from both Wired & Wireless' with a dropdown arrow. A note states 'CLI/GUI/SNMP access via this interface'.

Ethernet Ports

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

Table 36: Configure: Network > Ethernet Ports parameters

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

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

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

Figure 30: Configure: Network > Ethernet Ports parameters

The screenshot shows the 'Ethernet Ports' configuration interface. At the top, there are tabs for 'VLAN', 'Routes', 'Ethernet Ports', 'Security', 'DHCP', 'Tunnel', 'PPPoE', 'VLAN Pool', and 'WWAN'. The 'Ethernet Ports' tab is active. Below it, there are sub-tabs for 'Eth1' and 'Eth2'. The 'Eth1' sub-tab is selected. In the center, there is a configuration box for 'ETH1'. It contains a dropdown menu currently showing 'Access Single VLAN'. Below this, there is a label 'Access Mode' followed by a text input field containing 'VLAN'. Underneath the text input field, the number '1' is entered. At the bottom right of the configuration box, there are 'Save' and 'Cancel' buttons.

General network parameters

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

Table 37: Configure: Network > VLAN > General parameters

Parameters	Description	Range	Default
Management Access	Provision to restrict the access of device in all modes CLI (Telnet, SSH), GUI (HTTP, HTTPs) and SNMP. User can configure restriction of device access as follows: <ul style="list-style-type: none"> • Block • Allow from Wired • Allow from both wired and wireless 	–	Allow from both Wired and Wireless

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

Figure 31: Configure: Network > VLAN > General parameters

Security

Below table lists the fields that are displayed in the **Configuration > Network > Security** tab:

Table 38: Configure: Network > Security parameters

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

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

DHCP

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

Table 39: Configure: Network > DHCP parameters

Parameters	Description	Range	Default
Edit	Provision to select DHCP Pool if multiple Pools are defined on Enterprise Wi-Fi AP device.	–	–
Address Range	User can configure start and end addresses for a DHCP Pool selected from the drop-down box.	–	–
Default Router	Provision to configure next hop for a DHCP pool selected from drop-down box.	–	–
Domain Name	Provision to configure domain name for a DHCP pool selected from drop-down box.	–	–
DNS Address	Provision to configure DNS server for a DHCP pool selected from drop-down box.	–	–
Network	Provision to configure Network ID for a DHCP pool selected from drop-down box.	–	–
Lease	Provision to configure lease for a DHCP pool selected from drop-down box.	–	–
Add Bind List			
	For every DHCP pool configured, user can bind MAC and IP from the address pool defined, so that wireless station gets same IP address every time they connect. Following parameters are required to bind IP address: <ul style="list-style-type: none"> • MAC Address • IP Address 	–	–

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

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

To configure Add Bind List:

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

Figure 32: Configure: Network > DHCP parameters

VLANRoutesEthernet PortsSecurity**DHCP**TunnelPPPoEVLAN Pool

Edit

Create Pool

Address Range

Start

End

IP address range to be assigned to clients

Default Router

Default router IP

Domain Name

Domain Name

DNS Address

Primary

Secondary

Domain name for the client

Network

IP

Mask

Subnet number and mask of the DHCP address pool

Lease

1

Hours

Minutes

Lease time (days:hours:minutes)

Save

Cancel

Add Bind List

MAC Address

IP Address

Save

XX:XX:XX:XX:XX:XX

XXX.XXX.XXX.XXX

MAC Address

IP Address

Action

No bind list available

1

10

items per page

Chapter 8: Configuration - Network

101

Tunnel

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

Table 40: Configure: Network > Tunnel parameters

Parameters	Description	Range	Default
Tunnel Encapsulation	Provision to enable tunnel type. Following tunnel types are supported by Enterprise Wi-Fi AP devices: <ul style="list-style-type: none">• L2TP• L2GRE• OFF	–	OFF
L2TP			
Remote Host	Configure L2TP end point. IPv4 address or Primary hostname of endpoint is supported.	–	–
Authentication Info	Provision to configure credentials required for L2TP authentication.	–	–
Auth Type	Provision to select the PPP authentication method. Following are the options available: <ul style="list-style-type: none">• DEFAULT• CHAP• MS-CHAP• MS-CHAPv2• PAP	–	DEFAULT
Secondary Remote Host	Configure secondary L2TP end point. IPv4 address or Secondary hostname of endpoint is supported.	–	–
Secondary Authentication Info	Provision to configure credentials required for secondary L2TP authentication.	–	–
Secondary Auth Type	Provision to select the secondary PPP authentication method. Following are the options available: <ul style="list-style-type: none">• DEFAULT• CHAP• MS-CHAP• MS-CHAPv2• PAP	–	DEFAULT

Parameters	Description	Range	Default
TCP MSS	Provision to configure TCP Maximum Segment Size.	422- 1410	1400
PMTU Discovery	Provision to enable to discover PMTU in network.	–	Enabled
Disconnect Wireless Clients	Provision to disconnect Wireless Client when state of L2TP tunnel is down.	–	Enabled
L2GRE			
Primary Remote Host	Configure L2GRE end point. IPv4 address or Primary hostname of endpoint is supported.	–	–
Secondary Remote Host	Configure L2GRE end point. IPv4 address or Secondary hostname of endpoint is supported. The tunnel operates in failover mode. After determining the peer is down (no Rx packet received from PEER), AP sends periodic ICMP packet to verify the reachability to the peer before failing over to secondary peer. So ensure ICMP reachability to the tunnel PEER.	–	–
DSCP	User can configure priority of GRE packets.	–	0
TCP MSS	Provision to configure TCP MSS value.	472-1460	1402
PMTU Discovery	Provision to enable to discover PMTU in network.	–	–
MTU	Maximum Transmission Unit.	850-1460	1460
GRE in UDP	GRE protocol designed to establish tunnel between any third-party vendor which complies RFC 8086.	–	Disabled
Disconnect Wireless Clients	Provision to disconnect Wireless Client when state of L2TP tunnel is down.	–	Enabled
Tunnel Reachability	Periodic interval for verifying the RX packet from GRE peer.	30-240	240
Tunnel Retry Attempts	Number of retries before Fail-Over to secondary peer.	2-10	5

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

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

To configure **L2TP**:

2. Enter IP address or domain name in the **Remote Host** textbox.
3. Enter credentials required for L2TP authentication in the **Authentication Info** textbox.
4. Select authentication type from the **Auth Type** drop-down list.
5. Enter IP address or domain name in the **Secondary Remote Host** textbox.

6. Enter credentials required for secondary L2TP authentication in the **Secondary Authentication Info** textbox.
7. Select authentication type from the **Secondary Auth Type** drop-down list.
8. Enter TCP Maximum Segment Size in the **TCP MSS** textbox.
9. Enable **PMTU Discovery** checkbox.
10. Enable **Disconnect Wireless Clients** checkbox.
11. Click **Save**.

To configure **L2GRE**:

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

Figure 33: *Configure: Network > Tunnel parameters*

VLAN
Routes
Ethernet Ports
Security
DHCP
Tunnel
PPPoE
VLAN Pool
WWAN

Tunnel Encapsulation
L2TP

Remote Host
0.0.0.0
IP address or domain

Authentication Info
admin
Max 64 characters

Auth Type
DEFAULT
MS-CHAPv2, MS-CHAP, CHAP, PAP

Secondary

Secondary Remote Host
0.0.0.0
IP address or domain

Secondary Authentication Info
admin
Max 64 characters

Secondary Auth Type
DEFAULT
MS-CHAPv2, MS-CHAP, CHAP, PAP

TCP MSS
1400
TCP Maximum Segment Size (422-1410 bytes)

PMTU Discovery
Path MTU Discovery

Disconnect Wireless Clients
Disconnect Wireless Client when state of L2TP tunnel is down

Primary Remote Host
10.110.211.39
IP address or domain

Secondary Remote Host
0.0.0.0
IP address or domain

The tunnel operates in failover mode. After determining the peer is down (no rx packet received from PEER), AP sends periodic ICMP packet to verify the reachability to peer before failing over to secondary peer. So please ensure ICMP reachability to the tunnel peer

DSCP
0
Differentiated Service Code Point

TCP MSS
1402
TCP Maximum Segment Size (472-1460 bytes)

PMTU Discovery
Path MTU Discovery

MTU
1460
Configure MTU for L2GRE tunnel (850-1460 bytes)

GRE
GRE in UDP
Enable GRE in UDP encapsulation (RFC 8086)

Disconnect Wireless Clients
Disconnect Wireless Client when state of L2TP tunnel is down

Tunnel Reachability
240
Periodic interval for verifying the RX packet from GRE peer (30-240)

Tunnel Retry Attempts
5
Number of Retries before Fail-Over to Secondary peer (2-10 seconds)

Save
Cancel

PPPoE

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

Table 41: Configure: Network > PPPoE parameters

Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disabled
VLAN	User can configure VLAN ID where PPPoE client should	–	–

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

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

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

Figure 34: Configure: Network > PPPoE parameters

The screenshot shows the 'PPPoE' configuration tab in a network management interface. The 'Enable' checkbox is unchecked. The 'VLAN' field contains the value '1'. The 'Service Name' field is empty. The 'Authentication Info' field contains 'admin' and a password field with six dots. The 'MTU' field contains '1430'. The 'TCP-MSS Clamping' checkbox is checked. The 'Management Access' checkbox is unchecked. At the bottom are 'Save' and 'Cancel' buttons.

VLAN Pool

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

Table 42: Configure: Network > VLAN Pool Parameters

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

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

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

Figure 35: Configure Network > VLAN Pool parameters

The screenshot displays the 'VLAN Pool' configuration page. At the top, there is a navigation bar with tabs: VLAN, Routes, Ethernet Ports, Security, DHCP, Tunnel, PPPoE, **VLAN Pool**, and WWAN. The main content area has two text input fields: 'VLAN Pool Name' and 'VLAN ID List'. Below these fields is a table with the following structure:

VLAN Pool Name	VLAN ID List	Act...
pool1	1,20	[icon]

At the bottom of the table, there is a pagination control showing '1 - 1 of 1 items' and '10 items per page'. Below the table are 'Save' and 'Cancel' buttons.

Chapter 9: Filter Management

This chapter describes the following topics:

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

Overview

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

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

Filter list

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

Filters

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

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

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

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

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

Configuring filter CLI

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

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

```
XV3-8-EC7708(config)# filter
filter-list      : Configure filter list
global-filter    : Configure Global filter parameters
```

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

```
XV3-8-EC7708(config-global-filter)#
air-cleaner      : Configure Preset air cleaner filters
application-control : Enable application control
clear            : Clear command
disable          : Disable filter list
filter           : Configure filter rules in precedence order
stateful         : Enable stateful filtering

apply            : Apply configuration that has just been set
exit             : Exit from filter list configuration
no              : Delete/disable filter list parameters
save             : Save configuration to Flash so it persists across reboots
show            : Show command
```

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

3. Each filter list includes below options:

```
clear            : Clear command
disable          : Disable filter list
filter           : Configure filter rules in precedence order
name             : Name of filter list

apply            : Apply configuration that has just been set
exit             : Exit from filter list configuration
no              : Delete/disable filter list parameters
save             : Save configuration to Flash so it persists across reboots
show            : Show command
```



Note

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

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

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

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

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

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

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



Note

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

5. Layer 3 filter has the below provisions.

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

deny               : Drop packet matching the rule
permit             : Allow packet matching the rule
set-dscp           : Set DSCP value to packet matching the rule
set-qos            : Set QoS value (0-3) to packet matching the rule
```

- **QoS [Premium feature](#)**: Set packets QoS level (0 to 3). Level 0 has the lowest priority; level 3 has the highest priority
- **DSCP [Premium feature](#)**: Differentiated Services Code Point or DiffServ (DSCP). DSCP level (0 to 63). Level 0 has the lowest priority and level 63 has the highest priority.
- **Rate limit [Premium feature](#)**: Filters support rate limiting per station or all stations and support Kbps/Mbps/pps.
- **Schedule [Premium feature](#)**: Filter support scheduling the activation of the layer3 /application control rules based on the day and local time selected.
- **Disable**: Each filter and filter list can be turned on/off.



Note:

Stateful filtering, Application Control, QoS, DSCP, Schedule and Rate limit are [Premium features](#).

6. Each layer 3 rule category has below types

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

ip                 : IPV4 address based rule
ip6                : IPV6 address based rule
proto              : Protocol based rule
proto6             : IPv6 Protocol based rule
```

7. For proto or port number-based rule, select proto.

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

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



Note

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

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

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

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

9. Layer 2 filter has below options:

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

deny          : Drop packet matching the rule
permit        : Allow packet matching the rule
```

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

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

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

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

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

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

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

Example:

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

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

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

layer2-filter permit proto (tcp|udp|arp|icmp|igmp|srp|sctp|any) (SOURCE-MAC/IPv4/IPv6{/{mask|prefix-length}}|any) (SOURCE-PORT|any) (DESTINATION-MAC/IPv4/IPv6{/{mask|prefix-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. In order to attach filter list into WLAN profile, filter-list < filter-list ID>.

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

14. To show filter statistics:

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

Filter ID | global
```

Air Cleaner

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

Configuration CLI:


```
XV3-8-EC7708(config)# filter global-filter
XV3-8-EC7708(config-global-filter)# air-cleaner

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

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

```
XV3-8-EC7708(config-global-filter)# air-cleaner all
XV3-8-EC7708(config-global-filter)# show config filter
!
!
filter global-filter
  stateful
  application-control
  air-cleaner all
  filter precedence 1
    layer2-filter deny proto arp any any in //Air-cleaner-Arp.1
    wlan-to-wlan
    exit
  filter precedence 2
    layer2-filter deny proto udp any any FF:FF:FF:FF:FF:FF 67 out //Air-cleaner-Dhcp.1
    exit
  filter precedence 3
    layer2-filter deny proto udp any any FF:FF:FF:FF:FF:FF 68 in //Air-cleaner-Dhcp.2
    exit
  filter precedence 4
    layer2-filter permit proto arp any FF:FF:FF:FF:FF:FF any //Air-cleaner-Bcast.1
    exit
  filter precedence 5
    layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 67 any //Air-cleaner-Bcast.2
    exit
  filter precedence 6
    layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 68 any //Air-cleaner-Bcast.3
    exit
  filter precedence 7
    layer2-filter permit proto udp any any FF:FF:FF:FF:FF:FF 22610 any //Air-cleaner-Bcast.4
    exit
  filter precedence 8
    layer2-filter deny mac any FF:FF:FF:FF:FF:FF any //Air-cleaner-Bcast.5
    exit
  filter precedence 9
    layer2-filter permit mac any 01:00:5E:00:00:FB any //Air-cleaner-mDNS.1
    exit
  filter precedence 10
    layer2-filter deny mac any multicast any //Air-cleaner-Mcast.1
    exit
```



Note

In Mesh link configuration, the Air Cleaner rules needs customisation 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 the Application Control Filters section in the user guide

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

Deep Packet Inspection (DPI)

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

Application control policy

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

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

Risk and Productivity

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

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

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

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

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

Selection criteria

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

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

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

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

```
XV3-8-441BCC(config)# show application-statistics by-category
Application Category Statistics for All Applications
```

Application category	Productivity Index & Risk		TX Packets	TX Bytes	RX Packets	RX Bytes
Networking	3	1	3031	1832377	1975	376598
Social-Networking	3	1	1306	1530897	820	82227
Streaming-Media	1	4	97	26497	102	12452
Web-Services	3	1	8346	10285674	2270	304266

```
XV3-8-441BCC(config)#
```

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

```
XV3-8-441BCC(config)# show application-statistics by-application ssid 1
Applications Count = 24
Application Statistics for wlan index 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	383	404708	211	20118
Mozilla	3	1	104	66692	88	10991
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	0	0	28	5600
SSL	3	3	226	136435	176	22509
TCP	3	1	2665	1661913	1966	403878
Twitter	3	4	79	53301	68	7532
Wikipedia	3	3	19	3126	28	3873
YouTube	1	4	110	32096	112	15632

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

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

```
XV3-8-441BCC(config)# show application-statistics by-application station D4-6A-6A-E7-D0-15
Applications Count = 24
Application Statistics for station D4-6A-6A-E7-D0-15
=====
```

Protocol or Application	Productivity Index & 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 list of stations present along with station count per VLAN.

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

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

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

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

VLAN	STA_COUNT
1	1

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

```
XV3-8-441BCC(config)# show application-statistics by-application vlan 1
Applications Count = 24
Application Statistics for VLAN 1
```

Protocol or 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

- By Time frame: This gives information about the application seen in last the duration (E.g. 1 day).
 - For low risk number the productivity is high and vice versa. (E.g. For GitHub (Shown in below figure) the risk index number is 1 and the productive index is 4, this means the application is low risk and more productive).

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

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

DPI CLI configuration

User can enable Application Control globally by using below commands:

Enable DPI support

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

Disable DPI support

```
XV3-8-441BCC(config)# filter global-filter
XV3-8-441BCC(config-global-filter)# no application-control
XV3-8-441BCC(config-global-filter)#
```

Global application policy

Per application policy

```
XV3-8-441BCC(config)# filter global-filter
XV3-8-441BCC(config-global-filter)# filter precedence 1
XV3-8-441BCC(config-global-filter-precedence-1)# application-control

050plus          : 050Plus
12306cn          : 12306.cn
123movie         : 123movies
126com           : 126.com
17173            : 17173.com
1fichier         : 1fichier
2345com          : 2345.com
247inc           : [24]7 Inc.
247media         : 24/7 Media
2channel         : 2channel
33across         : 33Across
360antiv         : 360 AntiVirus
39net            : 39.net
3comtsmx         : 3COM-TSMUX
3pc              : 3PC
4399com          : 4399.com
4chan            : 4chan
4shared          : 4Shared
51com            : 51.com
56com            : 56.com
58com            : 58.com.cn
914cg            : 914CG
9gag             : 9GAG
about            : about.com
abschn           : ABS-CBN
acas             : ACA Services
accweath         : accuweather.com

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

deny            : Block this application
permit          : Allow this Application
set-dscp        : set dscp priority
set-qos         : set qos priority

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

permit          : Allow this Application
```


Set per category policy

```
XV3-8-441BCC(config-global-filter-precedence-1)# category-control

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

XV3-8-441BCC(config-global-filter-precedence-1)# category-control games permit
XV3-8-441BCC(config-global-filter-precedence-1)#
```

SSID application policy

```
XV3-8-441BCC(config)# filter filter-list 1
XV3-8-441BCC(config-filter-list-1)# filter precedence 1
XV3-8-441BCC(config-list-1-filter-precedence-1)# application-control facebook deny
XV3-8-441BCC(config-list-1-filter-precedence-1)#
XV3-8-441BCC(config)# wireless wlan 1
XV3-8-441BCC(config-wlan-1)# filter-list 1
XV3-8-441BCC(config-wlan-1)#
```

Show configuration

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

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

Chapter 10: Configuration - Services

This chapter describes the following topics:

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

Overview

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

Configuring services

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

- [User Groups](#)
- [Location API](#)
- [Speed Test](#)
- [BT Location API](#)
- [Bonjour Gateway](#)
- [Link Aggregation Control Protocol \(LACP\)](#)
- [Real Time Location System \(RTLS\)](#)

User Groups [Premium feature](#)

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

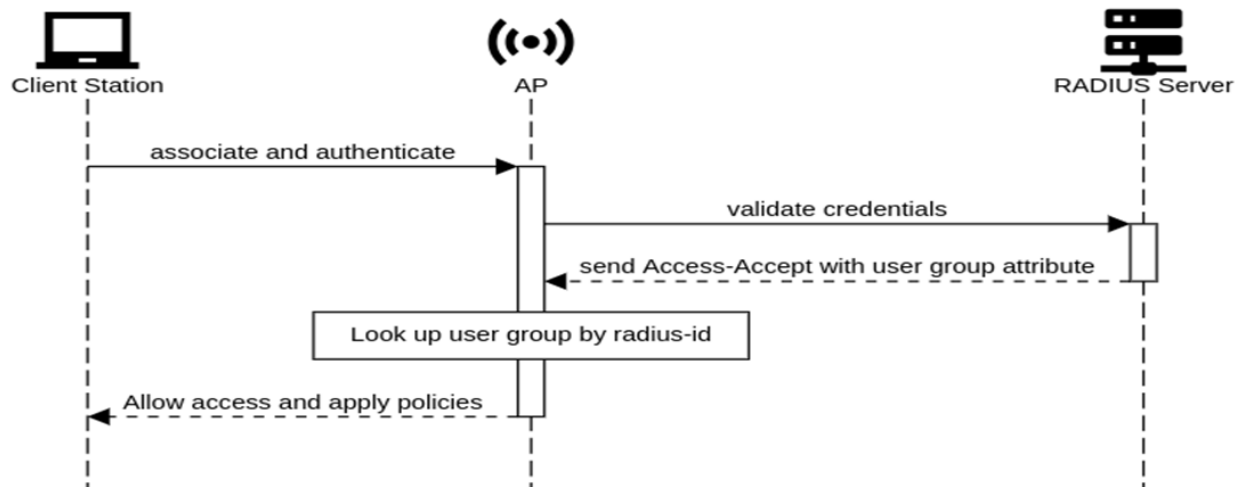
To simplify wireless administration and streamline changes, a feature called User Groups is provided that allows the wireless administrator to apply a set of wireless policies to a user based on a single RADIUS attribute. This eliminates the need for administrative rights on the RADIUS server and simplifies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

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

The User Group feature is natively supported by XMS Cloud.

Figure 36: User Groups interaction

User Groups Interaction



CLI Configuration:

```

XV3-8-EC7708(config)# group

Specify user group number <1-16>

XV3-8-EC7708(config)# group 1
XV3-8-EC7708(config-group-1)#

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

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

XV3-8-EC7708(config-group-1)#
  
```

Example:

```

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

User group properties and actions

A user group supports the following properties and actions:

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

User group policies

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

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

Location API

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

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

Table 43: Configure: Services > Location API parameters

Parameters	Description	Range	Default
Enable	Provision to enable/disable Location API services.	-	-
Server	Provision to configure HTTP/HTTPs server to send report with the port number.	0-65535	-
Interval	Provision to configure custom frequency of information to be shared to server.	2-3600	-
MAC Anonymization	Avoid populating locally administrated MAC addresses in Location API client list.	-	-

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

1. Select the **Enable** checkbox to enable Location API.
2. Enter the HTTP/HTTPs server and port number in the **Server** textbox.

3. Enter the interval for Location API in the **Interval** textbox.
4. Enable **MAC Anonymization** checkbox.
5. Click **Save**.

Figure 37: Configure: Services > Location API parameters

Location API

Enable ☐

Server

Eg: [http://<domain>.com:80](#)

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

Interval

Configure Location API interval (2-3600) seconds

MAC Anonymization ☐

Ignore Anonymized MACs ⓘ



Note

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

Speed Test

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

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

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

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

Table 44 lists the fields that are displayed in the **Configuration > Services > Speed Test** tab:

Table 44: Configure: Services > Speed Test parameters

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

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

Figure 38: Configure: Services > Speed Test parameters

Speed Test

Wi-Fiperf

☐ Enable Wi-Fiperf Endpoint ⓘ

BT location API

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

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

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

Table 45: BT Location API parameters

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

Sending report

After enabling BLE Scanning on AP it will start processing:

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

In the CLI

To configure the BT Location-API:

```
XV3-8-EC7708(config)# location-bt-api

ignore-anonymized-bt-mac : Ignore MAC addresses that are anonymized
interval                  : Configure reporting interval in secs
server                    : HTTP/HTTPS server to send report to with the port number
```

To disable the BT Location-API:

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

BT Location API data elements

Table 46: BT Location API data elements

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

HTTP POST body format:

```
{
  u'ap_mac': '00-04-56-A5-5A-EC',
  'version': '2.2',
  'ap_name': 'E600-A55AEC',
  'ble_discoverd_clients': {Array of 0-250 devices}
}
```

Bluetooth API Data Format

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

Bonjour Gateway

Bonjour enables 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 extend the scope of bonjour service beyond the local network by forwarding bonjour Multicast DNS (mDNS) packet across different VLANs, to make bonjour services/devices available between the different wireless/local networks.

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

Table 47: Configure: Services > Bonjour Gateway parameters

Parameters	Description	Range	Default
Enable	Provision to enable/disable Bonjour Gateway services.	-	-
Service Name	Provision for user defined bonjour rule name	-	-
Proto	Select the required mDNS protocol	-	-

Parameters	Description	Range	Default
From VLAN	VLAN in which mDNS/Bonjour service is running	-	-
To VLAN	VLAN in which clients are listening	-	-

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

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

Figure 39: Configure: Services > Bonjour parameter

to configure in CLI:

1. Enable Bonjour Gateway on AP.

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

1. To configure Bonjour rule.

```
XV3-8-EC7708(config)# bonjour-fw rules
    bonjour-fw rules <sname> <proto> <vidfrom> <vidto>
```


2. To control mDNS repeated packet to WAN side.

```
XV3-8-EC7708(config)# bonjour-fw bonjour-forward-to-wan  
  
all          : Forward all bonjour mdns packets queries and response repeated with vlan to WAN side  
queries      : Forward bonjour mdns Query packets repeated with vlan to WAN side  
responses    : Forward bonjour mdns Response packets repeated with vlan to WAN side
```



Note

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

Link Aggregation Control Protocol (LACP)

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

LACP provides the following benefits:

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

Configuration:

To Add ethernet to port channels:

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

Port channel configuration:

```
XV3-8-EC7708(config)# interface portchannel 1
XV3-8-EC7708(config-portchannel-1)#

advertise      : Ethernet link speed advertisement
channel-group  : Ethernet member channel group
clear          : Clear command
duplex         : Ethernet link duplex
speed          : Ethernet link speed
switchport     : Configure switch port
tunnel-mode    : Enable tunnelling of wired traffic over configured tunnel

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

Syntax:

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

Real Time Location System (RTLS)

Stanley AeroScout Location Engine [Premium feature](#)

The Location Engine delivers an 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 provides network access. AeroScout utilizes a location engine to determine the position of Wi-Fi tags.

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

CLI Configuration:

```
XV3-8-EC7708(config)# rtls aeroscout

ble-tag        : Enable Aeroscout BLE Tag
server         : Configure Aeroscout Server IP or FQDN
server-port    : Configure Aeroscout Server Port (Default port:12092)
wifi-tag       : Enable Aeroscout WiFi Tag
```

Chapter 11: Operations

This chapter describes the following topics:

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

Overview

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

Firmware upgrade

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



Note

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



Warning

Platform: e410, e510, e430, e600 and e700

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

Table 48 lists the fields that are displayed in the **Operations > Firmware** update tab:

Table 48: Configure: Operations > Firmware update parameters

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

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

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

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

Figure 40: Configure: Operations > Firmware update parameters

Firmware update

Choose File

No file chosen

Upgrade Firmware

Upgrade Status :

System

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

Table 49 lists the fields that are displayed in the **Operations > System** tab:

Table 49: Configure: Operations > System parameters

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

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

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

Figure 41: Configure: Operations > System parameters

System

Reboot

Download Tech Support

Disconnect All Clients

Flash LEDs

10

Flash LED (1-120) seconds

Factory Default

Configuration

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

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

Figure 42: Configure: Operations > Configuration parameters

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

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

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

Figure 43: Configure: Operations > Configuration parameters

Configuration

Export

Import

Chapter 12: Troubleshoot

Overview

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

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

Logging

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

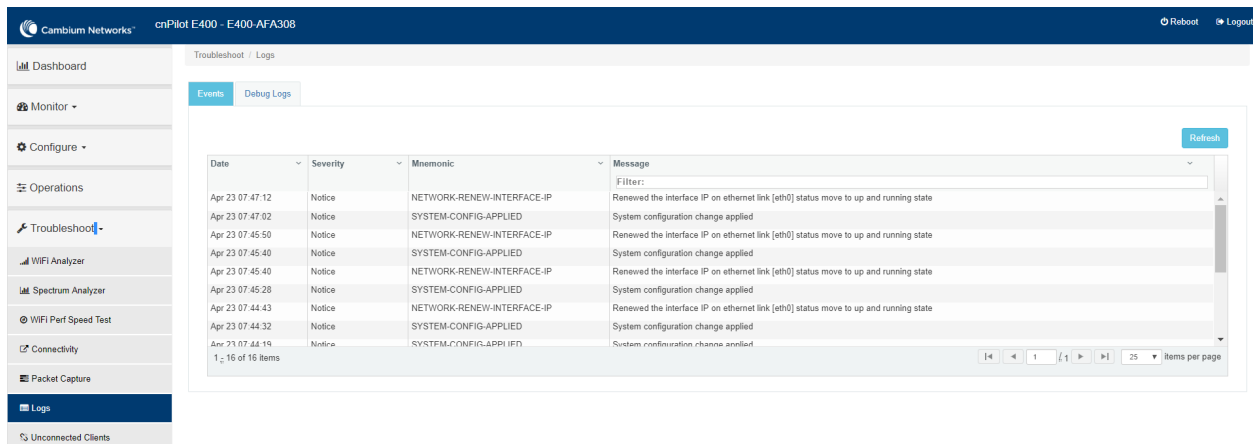
Events

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

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

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

Figure 44: *Troubleshoot > Logs > Events*

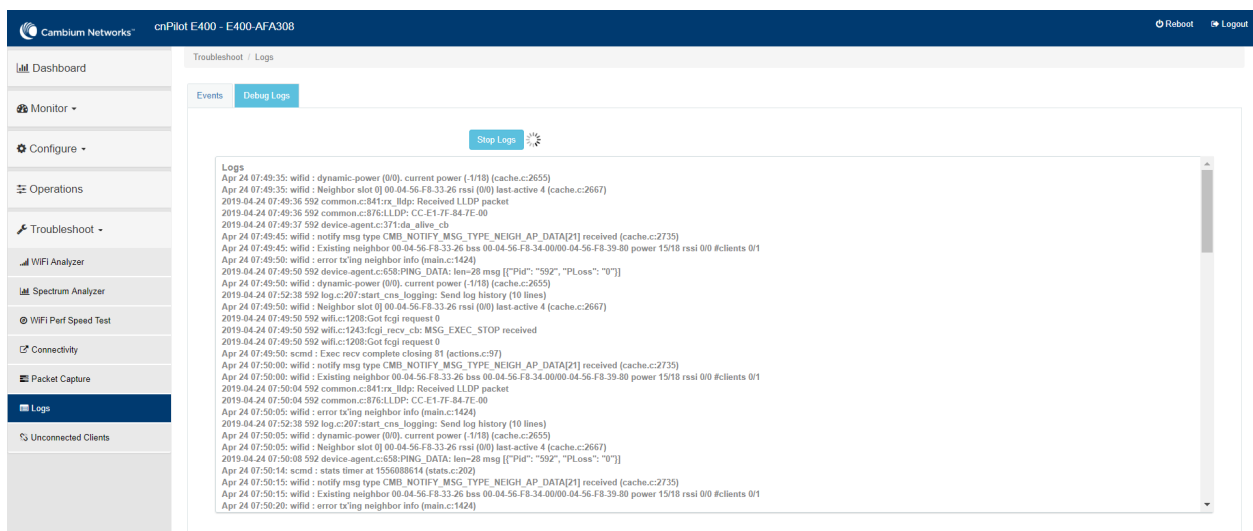


Debug Logs

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

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

Figure 45: *Troubleshoot > Logs > Debug Logs*



Radio Frequency (RF)

Wi-Fi Analyzer

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

- Interference

This tool shares more information of each channel as below:

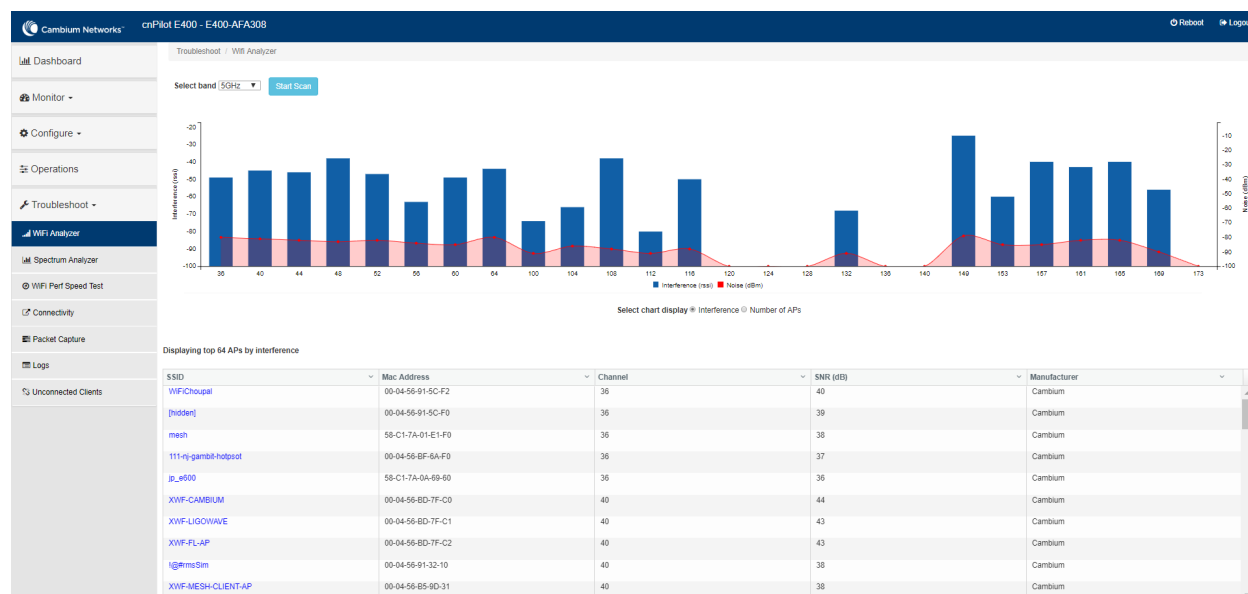
- Noise
 - Interference measured in RSSI
 - List of top 64 neighbor APs
- Number of APs

This tool shares more information of each channel as below:

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

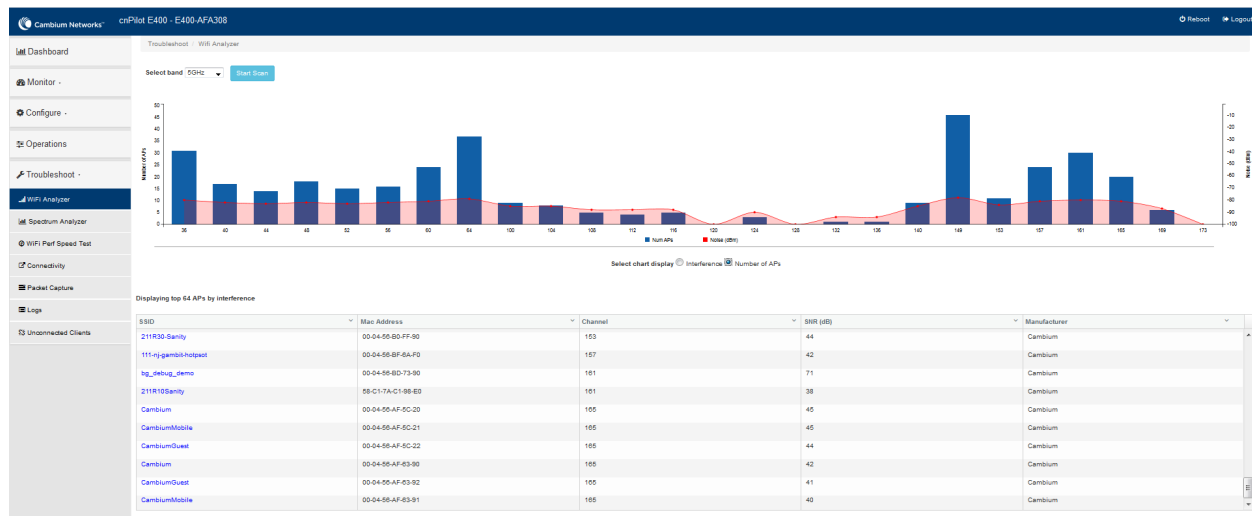
Channel analyzer is available at **Troubleshoot > Wi-Fi Analyzer > Interference Mode.**

Figure 46: *Troubleshoot > Wi-Fi Analyzer > Interference Mode*



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

Figure 47: Troubleshoot > Wi-Fi Analyzer > Number of APs Mode



Packet capture

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

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

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

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

Figure 48: Troubleshoot > Packet Capture page

Troubleshoot / Packet Capture

Interface :

Ethernet

1

Source IP & Destination IP:

Source IP

Destination IP

Source MAC & Destination MAC:

Source MAC

Destination MAC

Direction :

Both

Count :

Ex : 100

0 to 65535 (default 0 indicates unlimited)

Duration :

Ex : 120 Secs

1 to 600 (Default 120) seconds

Snaplen

Ex : 0

0 to 1500 (Default 0 indicates full packet length)

File Size

Ex : 10

1 to 50 (Default is 10 MB on 11ax APs)

Filename

PCAP File Name

1 to 256 characters

Filter

Ex : icmp[icmptype] == 8

Start Capture

Packet Capture Result

#	Interface	Status	Count	Duration	Size	Channel	Filename	Filter	StartTime	EndTime	Action
1	eth1	running	143	14/120	21KB/10MB	NA	XV3-8-EC7708-eth1.pcap		27-08-2021 18:01:26		

Performance

Speedtest on Access Point

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

Configuration:

Syntax:

```
XV3-8-EC7708(config)# speedtest etsi
    <server url> <download MB> <upload MB>

XV3-8-EC7708(config)# speedtest etsi
```

Example:

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

Connectivity

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

- Ping
- DNS Lookup
- Traceroute

Table 50: Troubleshoot: Connectivity

Parameters	Description	Range	Default
Ping			
IP Address or Hostname	Provide IPv4 address or Hostname to validate the reachability of the destined Host.	-	-
Number of Packets	Provide number of request packets that are required to be transmitted to validate the reachability of destined Host.	1-10	3
Buffer Size	Configure ICMP packet size.	1-65507	56
Ping Result	Displays the ICMP results.	-	-
DNS Lookup			
Host Name	Provide Hostname whose IP must be resolved.	-	-
DNS Test Result	Displays the IP's that are associated with configured Hostname.	-	-
Traceroute			
IP Address or Hostname	Provide IPv4 address or Hostname to validate the reachability of the destined Host.	-	-
Fragmentation	Provision to allow or deny fragment packets.	-	Off
Trace Method	Provision to configure payload mechanism to check the reachability of destined IPv4/Hostname.	-	ICMP Echo
Display TTL	Provision to customize TTL display.	-	On
Verbose	Provision to display the output of traceroute.	-	On
Traceroute Result	Displays the output of traceroute command.	-	-

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

To configure **Ping**:

1. Select **Test type** from the drop-down list.
2. Enter IP address or **Hostname** in the textbox.
3. Enter the **Number of Packets** in the textbox.

4. Select **Buffer Size** value from the drop-down list.
5. Click **Start Ping**.

To configure **DNS Lookup**:

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

To configure Traceroute:

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

Figure 49: Troubleshoot > Connectivity > Ping

The screenshot displays the 'Ping' configuration window within the 'Troubleshoot / Connectivity' section. The 'Test Type' dropdown is set to 'Ping' and is highlighted with a red rectangle. Below it, the 'IP Address or Hostname' field contains 'www.google.com'. The 'Number of Packets' is set to '3' (with a range of 'Min = 1, Max = 10') and the 'Buffer Size' is set to '56' (with a range of 'Min = 1, Max = 65507'). A blue 'Start Ping' button is located below these fields. The results section, titled 'Ping Result', shows the following output:

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

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

Figure 50: Troubleshoot > Connectivity > DNS Lookup

Troubleshoot / Connectivity

Test Type :

DNS Lookup ▼

Host Name:

DNS Test

DNS Test Result

Name:www.google.com Address:2404:6800:4007:800::2004 Name:www.google.com Address:216.58.197.68

Figure 51: Troubleshoot: Connectivity > Traceroute

Troubleshoot / Connectivity

Test Type :

Traceroute ▼


IP Address or Hostname :

Fragmentation : ☒ Off ☐ On

Trace Method : ☐ ICMP Echo ☒ UDP

Display TTL : ☐ Off ☒ On

Verbose : ☐ Off ☒ On

Stop Traceroute 

Traceroute Result

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

XIRCON tool support

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

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

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

Chapter 13: Management Access

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

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

Local authentication

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

Device configuration

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

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

Figure 52: Configure/update default password of admin user

The screenshot displays the configuration page for a Cambium Networks cnPilot E400 - E400-AFA308 device. The left sidebar contains navigation links: Dashboard, Monitor, Configure, System (selected), Radio, WLAN, Network, Services, Operations, and Troubleshoot. The main content area is divided into two sections: System and Management.

System Section:

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

Management Section:

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

SSH-Key authentication

SSH keys are also used to connect remote machines securely. They are based on the SSH cryptographic network protocol, which is responsible for the encryption of the information stream between two machines. Ultimately, using SSH keys user can connect to remote devices without even entering a password and much more securely too. SSH works based on “public-key cryptography”. For simplicity, let us consider that SSH keys come in pairs. There is a private key, that is safely stored to the home

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

Device configuration

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

1. Enable **SSH** checkbox.
2. Provide Public key generated from steps described in SSH key generation section.

Figure 53: System > Management

The screenshot shows the configuration interface for a Cambium Networks device (cnPilot E400 - E400-AFA308). The left sidebar contains navigation options: Dashboard, Monitor, Configure, System (selected), Radio, WLAN, Network, Services, Operations, and Troubleshoot. The main content area is divided into two sections: System and Management.

System Section:

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

Management Section:

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

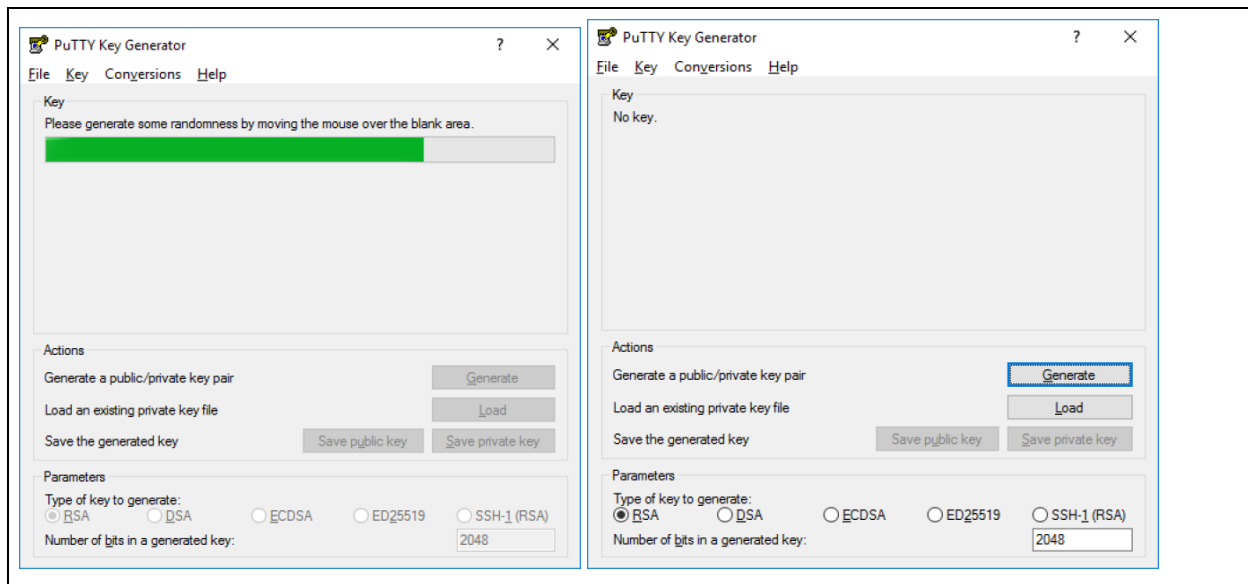
SSH key generation

Windows

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

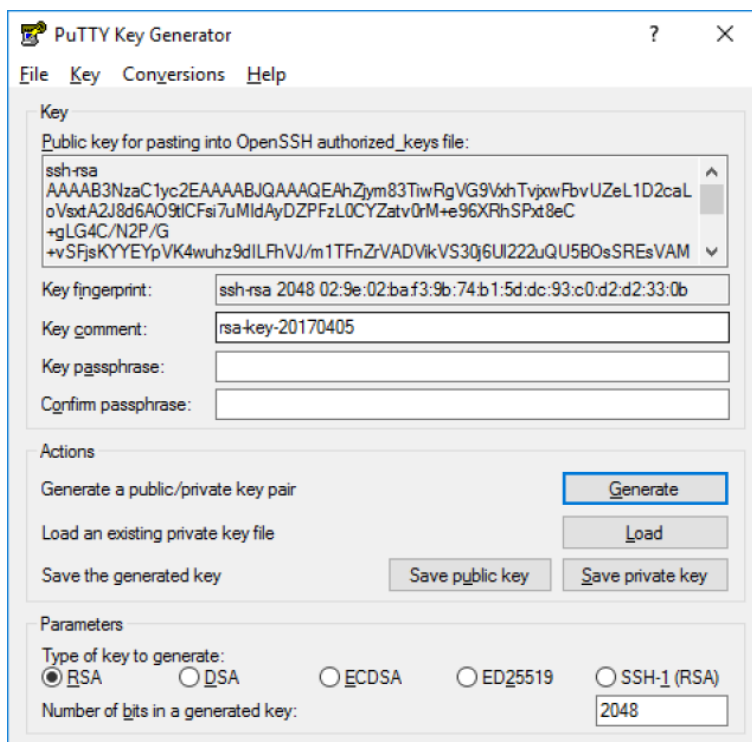
1. Generate a key pair in PUTTY Key Generator ([Chapter 13](#)) and save private and public key as shown in [Figure 55](#).

Figure 54: Generating public/private Key



2. Save the Public key and Private key once key pair is generated as shown in Figure 55.

Figure 55: Public and Private Key



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

Linux

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

1. Generate key pair executing below command on Linux console as shown in [Figure 56](#).

[Figure 56: 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:
SHA256:0qt4vJduO4uvsdpdPtPkNzQ9uorlH7ydwE9fiEXOh0Kao pk@ubuntu
The key's randomart image is:
+---[RSA 2048]-----+
|
|             ..|
|          .+.o|
|       . . . =.*|
|      . S.. = o|
|      .oo*... o|
|      . +E.. . .|
|     oo*X. + + |
|     ooBXOO. = .|
+-----[SHA256]-----+
pk@ubuntu:~$
```

2. The Public key is now located in PATH mentioned in [Figure 56](#).
- PATH = “Enter the file to which to save the key”
3. The private key (identification) is now saved in PATH as mentioned in [Figure 57](#).
- PATH = “Your identification has saved in <>”

[Figure 57: Private Key saved path](#)

```
pk@ubuntu:~$ cat /home/pk/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaClyc2EAAAADAQABAAQDfZq+gc13qG8DlckyFU2JqyW5pI9q8P0MrVtrM9Vu5
P85lkbIiCtsTmPm6Ewrfq/nhWwsn6k4p20pTZ/laX/Ww9BWf4jjw8nOqNY95zlJUD9mV48gqrOY8qbXv
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 Device configuration section.
5. Login to device using Private key generated above with username as “admin”.

RADIUS authentication

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

Device configuration

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

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

Figure 58: System > Management: RADIUS Server and RADIUS Secret parameters

The screenshot shows the configuration interface for a Cambium Networks cnPilot E400 device. The left sidebar contains navigation options: Dashboard, Monitor, Configure, System (selected), Radio, WLAN, Network, Services, Operations, and Troubleshoot. The main content area is divided into two tabs: System and Management.

System Tab:

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

Management Tab:

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

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

Figure 59: UI Login page

The screenshot shows the UI Login page. It has a blue header with the word "Login". Below the header, there is a red-bordered box containing a user icon and the username "bob". Below that is a password field with a lock icon and masked characters. At the bottom is a blue "Sign In" button.

Chapter 14: Guest Access Portal- INTERNAL

Introduction

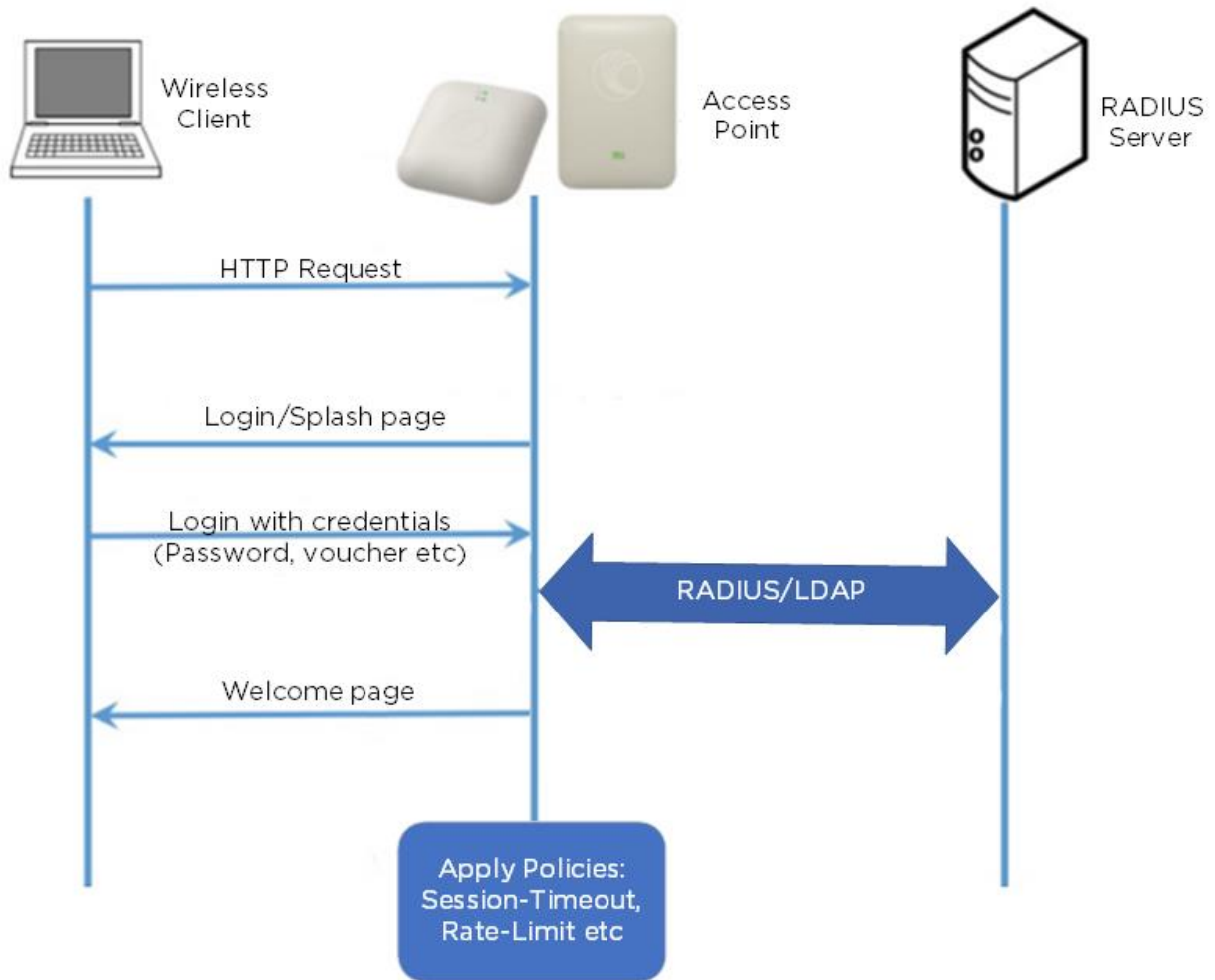
Guest Access Portal services offers a simple way to provide secure access to internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browsers session to a captive portal login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

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

- **Internal Access:** Captive Portal server is hosted on access point and is local to access point.
- **External Access:** Enterprise Wi-Fi AP is integrated with multiple third-party Captive Portal services vendor. Based on the vendor, device needs to be configured. More details on this Guest Access Portal method is described in [Chapter 15](#).
- **cnMaestro:** Captive Portal services are hosted on cnMaestro where various features like Social login, Voucher login, SMS login and Paid login is supported. More details on this Guest Access Portal method is described in [Chapter 16](#).
- **EasyPass:** EasyPass Access Services enable you to easily provide secure and controlled access to users and visitors on your Wi-Fi network.

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

Figure 60: Topology



Configurable parameters

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

Figure 61: Configure: WLAN > Guest Access > Internal Access Point parameter

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

Access policy

- Click through

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

Splash page

Title

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

Contents

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

Terms and conditions

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

Logo

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

Background image

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

Redirect parameters

Redirect hostname

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

Success action

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

- Internal logout Page

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

- Redirect users to external URL

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

- Redirect users to Original URL

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

[Figure 62: Success action](#)

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

Redirect

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

Figure 63: Redirect

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

Redirect Mode

There are two redirect modes available:

- **HTTP Mode**
When enabled, AP sends a HTTP POSTURL to the client.
- **HTTP(s) Mode**
When enabled, AP sends HTTPS POST URL to the client

Success message

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

Figure 64: Success Message

Success message

Timeout

Session

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

Figure 65: Configure: WLAN > Guest Access > Session timeout

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

Inactivity

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

Figure 66: Configure: WLAN > Guest Access > Inactivity timeout

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

Whitelist

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

Configuration examples

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

Access Policy – Clickthrough

Configuration

BasicRadius ServerGuest AccessUsage LimitsScheduled AccessAccessPasspointDelete

Enable☐

Portal Mode☒ Internal Access Point ☐ External Hotspot ☐ cnMaestro ☐ XMS/Easypass

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

Redirect Mode☒ HTTP Use HTTP URLs for redirection
☐ HTTPS Use HTTPS URLs for redirection

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

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

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

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

Logo
Eg: http://domain.com/logo.png
Logo to be displayed on the splash page

Background Image
Eg: http://domain.com/backgroundImage.jpg
Background image to be displayed on the splash page

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

Success message

Redirect☒ HTTP-only Enable redirection for HTTP packets only

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

Proxy Redirection Port
Port number(1 to 65535)

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

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

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

Extend Interface
Configure the interface which is extended for guest access

SaveCancel

White ListCaptive Portal Bypass User Agent

IP Address or Domain Name Save

IP Address | Domain NameAction

No white list available

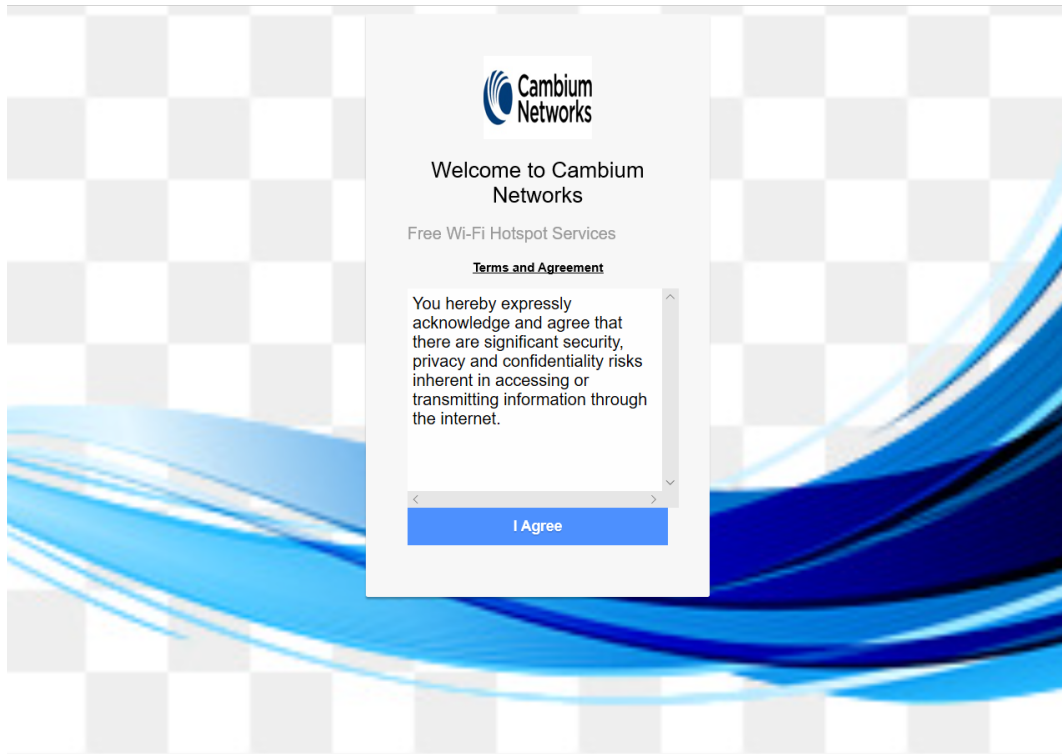
11

10 items per page

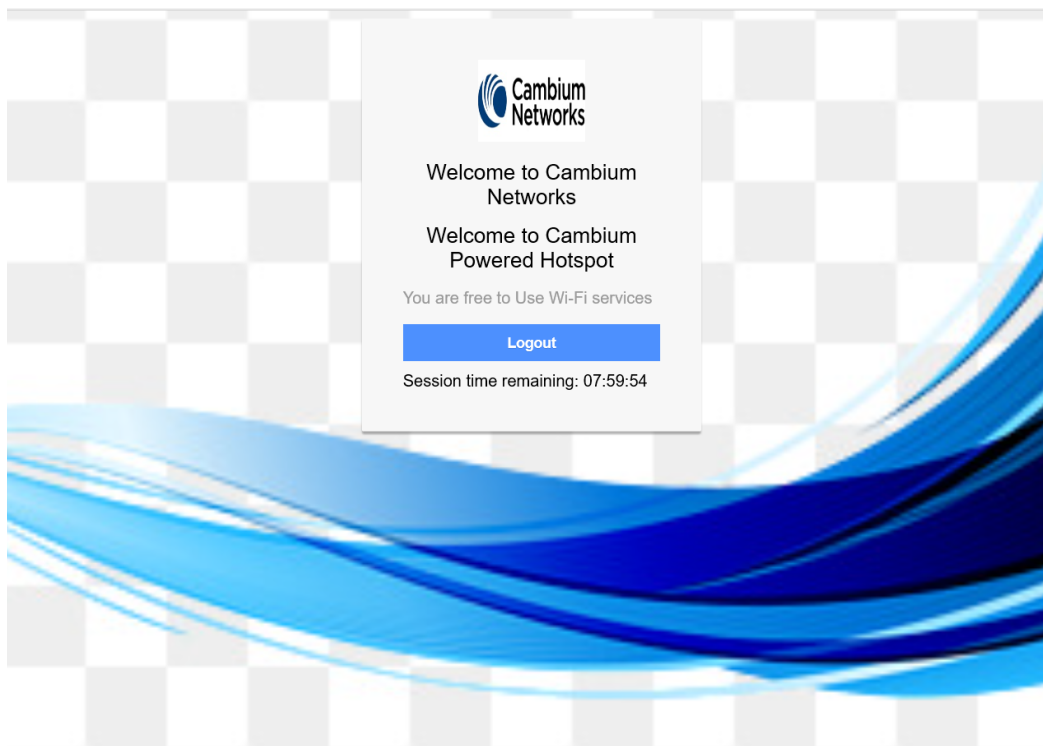
Chapter 14: Guest Access Portal- INTERNAL

154

Authentication – redirected splash page



Successful login – redirected splash page



Chapter 15: Guest Access Portal-EXTERNAL

Introduction

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

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

Configurable parameters

Figure 67 displays multiple configurable parameters supported for External Guest Access hosted on AP.

Figure 67: Configure: WLAN > Guest Access > External Access Point parameter

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

Enable
☒

Portal Mode
☐ Internal Access Point
☒ External Hotspot
☐ cnMaestro
☐ XMS/Easypass

Access Policy
☒ Clickthrough
☐ Radius
☐ LDAP
☐ Local Guest Account

Redirect Mode
☒ HTTP
☐ HTTPS

Redirect Hostname

WISPr Clients External Server Login
☐

External Page URL

External Portal Post Through cnMaestro
☐

External Portal Type
Standard

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

Success message

Redirection URL Query String
☐ Client IP
☐ RSSI
☐ AP Location

Redirect
☒ HTTP-only

Redirect User Page

Proxy Redirection Port

Session Timeout

Inactivity Timeout

MAC Authentication Fallback
☐

Extend Interface

Save
Cancel

White List
Captive Portal Bypass User Agent

IP Address or Domain Name
Save

IP Address | Domain Name
Action

No white list available

1
10
Items per page

Access policy

Click through:

Chapter 15: Guest Access Portal- EXTERNAL

157

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

WISPr

WISPr clients external server login

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

External portal post through cnMaestro

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



Note

This feature is supported only for cnMaestro On-Premises.

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. User can configure three modes of redirection URL:

- Internal logout Page

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

- Redirect users to external URL

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

- Redirect users to Original URL

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

Figure 68: Success action

Success Action

☒ Internal Logout Page ☐ Redirect user to External URL ☐ Redirect user to Original URL

Redirect

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

Figure 69: Redirect

Redirect <input checked="" type="checkbox"/> HTTP-only <i>Enable redirection for HTTP packets only</i>

Redirect mode

There are two redirect modes available:

- HTTP Mode
When enabled, AP sends a HTTP POSTURL to the client.
- HTTP(s) Mode
When enabled, AP sends HTTPS POST URL to the client

Success message

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

Figure 70: Success Message

Success message <input type="text"/>

Timeout

Session

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

Figure 71: Configure: WLAN > Guest Access > Session timeout

Session Timeout <input type="text" value="28800"/> <i>Session time in seconds (60 to 2592000)</i>
--

Inactivity

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

Figure 72: Configure: WLAN > Guest Access > Inactivity timeout

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

Whitelist

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

Configuration examples

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

Access Policy – Clickthrough

Configuration

BasicRadius ServerGuest AccessUsage LimitsScheduled AccessAccessPasspointDelete

Enable☐

Portal Mode☐ Internal Access Point☒ External Hotspot☐ cnMaestro☐ XMS/Easypass

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

Redirect Mode☒ HTTP Use HTTP URLs for redirection
☐ HTTPS Use HTTPS URLs for redirection

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

WISPr Clients External Server Login☐

External Page URL
URL of external splash page

External Portal Post Through cnMaestro☐

External Portal Type External Portal Type Standard/XWF

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

Success message

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

Redirect☒ HTTP-only Enable redirection for HTTP packets only

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

Proxy Redirection Port
Port number(1 to 65535)

Session Timeout Session time in seconds (60 to 2592000)

Inactivity Timeout Inactivity time in seconds (60 to 2592000)

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

Extend Interface
Configure the interface which is extended for guest access

SaveCancel

White ListCaptive Portal Bypass User Agent

IP Address or Domain Name Save

IP Address | Domain Name

Action

No white list available

1

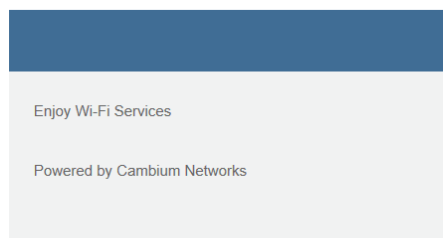
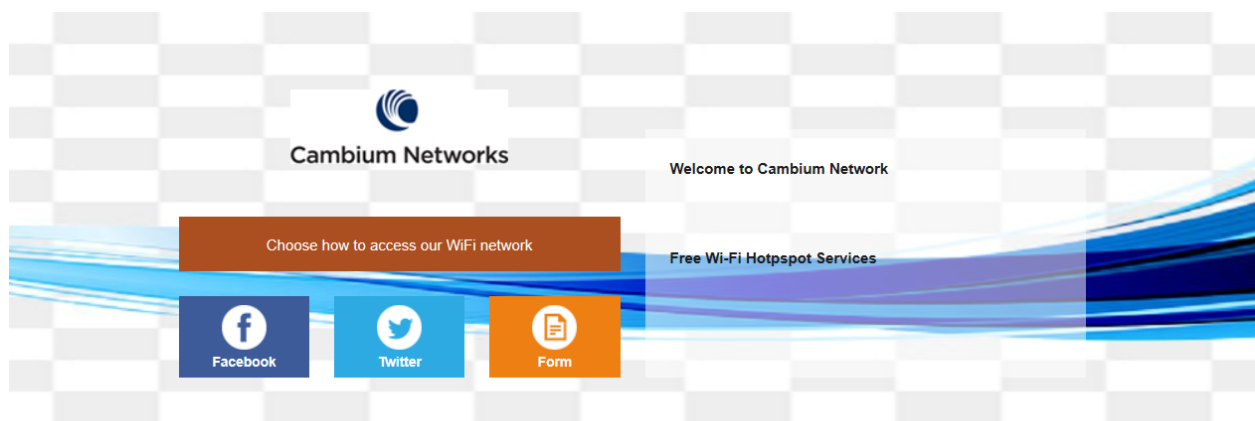
10

Items per page

Chapter 15: Guest Access Portal- EXTERNAL

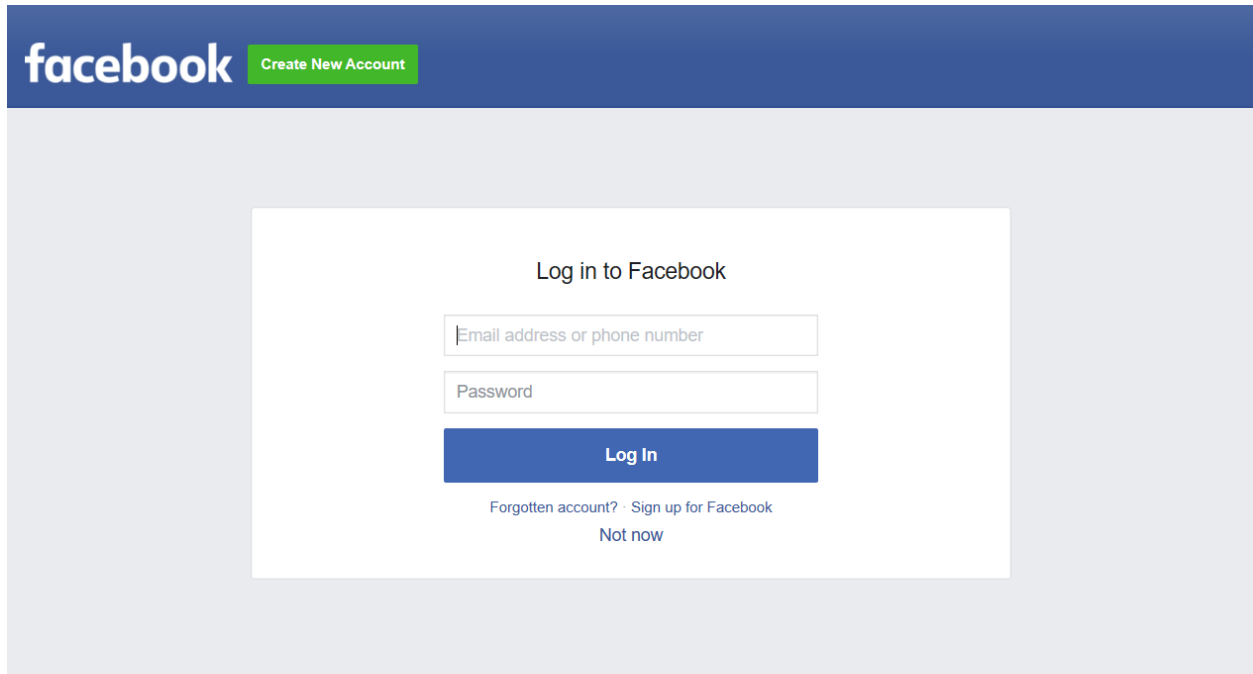
161

Authentication – redirected splash page




British English ▼

Successful Login – redirected splash page



The image shows the Facebook login splash page. At the top, there is a dark blue header with the Facebook logo on the left and a green button labeled "Create New Account" on the right. Below the header, the main content area is light gray. In the center, there is a white rectangular box containing the login form. The form has the title "Log in to Facebook" at the top. Below the title are two input fields: "Email address or phone number" and "Password". Below these fields is a blue button labeled "Log In". At the bottom of the form, there are two links: "Forgotten account? · Sign up for Facebook" and "Not now".

English (UK) ಕನ್ನಡ اردو मराठी తెలుగు हिन्दी தமிழ் മലയാളം বাংলা ગુજરાતી ਪੰਜਾਬੀ 

Chapter 16: Guest Access – cnMaestro

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

- For On-Premises, go to <https://support.cambiumnetworks.com/files/cnmaestro/> and download latest *cnMaestro On-Premises User Guide*.
- For cnMaestro Cloud, go to [cnMaestro Cloud User Guide](#).

Chapter 17: Device Recovery Methods

Factory reset via 'RESET' button

Table 51: Factory reset via RESET button

Access Point	Procedure	LED Indication
XV3-8	Press and hold Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2	Press and hold Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2T	Press and hold Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE3-4	Press and hold Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
e410	Press and hold Reset button for 25 seconds	LED will be OFF and turned onto Amber
e510	Press and hold Reset button for 20 seconds	Both LEDs will be OFF and turned onto Amber
e430	Press and hold Reset button for 25 seconds	LED will be OFF and turned onto Amber
e600	Press and hold Reset button for 20 seconds	LED will be OFF and turned onto Amber
e700	Press and hold Reset button for 25 seconds	Both LEDs will be OFF and turned onto Amber

Boot partition change via power cycle

Table 52: Boot partition change via power cycle

Access Point	Procedure
XV3-8	Follow power ON and off for 9 times with interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2	Follow power ON and off for 9 times with interval of 120 Sec (ON) and 5 Sec (OFF)
XV2-2T	Follow power ON and off for 9 times with interval of 120 Sec (ON) and 5 Sec (OFF)
XE3-4	Follow power ON and off for 9 times with interval of 120 Sec (ON) and 5 Sec (OFF)
e410	Follow power ON and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF)
e510	Follow power ON and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF)
e430	Follow power ON and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF)

Access Point	Procedure
e600	Follow power ON and off for 9 times with interval of 7 Sec (ON) and 5 Sec (OFF)
e700	Follow power ON and off for 9 times with interval of 15 Sec (ON) and 5 Sec (OFF)

Glossary

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

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

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 ConnectedPartners to deliver purposebuilt 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
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
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 © 2021 Cambium Networks, Ltd. All rights reserved.