Cambium Networks™

USER GUIDE

Enterprise Wi-Fi Access Point

System Release 6.4.1

Reservation of Rights

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

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

Contents

About This User Guide

This section describes the following topics:

Overview of Enterprise Wi-Fi AP products

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

Intended audience

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

Purpose

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

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

Related documents

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

Table 1: Related documents

Document Name	Location
Enterprise Wi-Fi AP product details	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/

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

New hardware platforms

System Release 6.4.1 includes the following new hardware platform:

Table 2: New hardware platform

Hardware Platform	Description
XV2-2T1	Outdoor Wi-Fi 6 Access point, 2x2 Sector antenna Dual band 802.11ax 2x2, BLE, 2.5GbE

Existing hardware platforms

System Release 6.4 includes the following existing hardware platforms:

Table 3: Existing hardware platforms

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

System Release 6.0 and later releases of Enterprise Wi-Fi AP 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	Release Details
RADIUS-based ePSK	System Release 6.4
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 (Stateful filtering, QoS, DSCP, Schedule, and Rate limit)	System Release 6.0
Application Control	System Release 6.0

Chapter 1: Quick Start – Device Access

This chapter describes the following topics:

Powering up the device

This section includes the following topics:

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

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

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

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

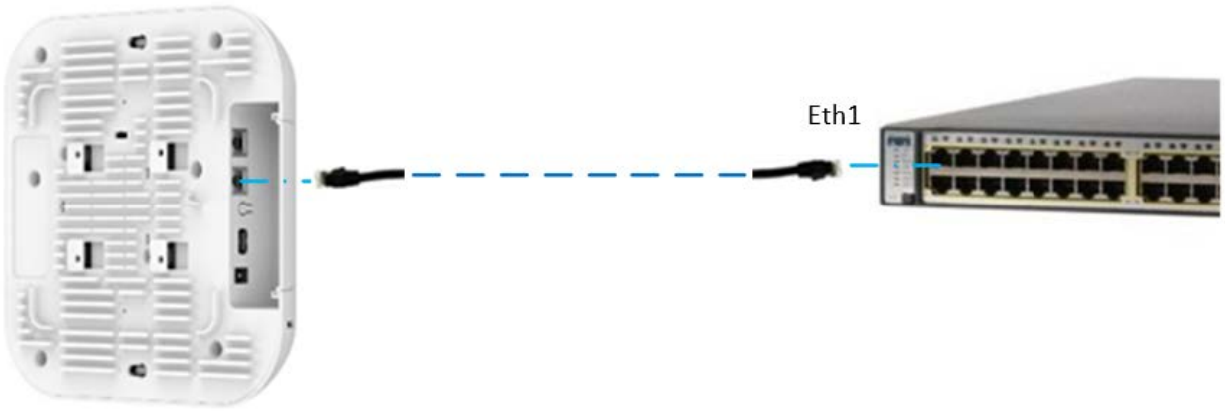


Table 5 provides detailed information on the AP modules that are enabled based on power negotiated via LLDP.

Table 5: Power management policy

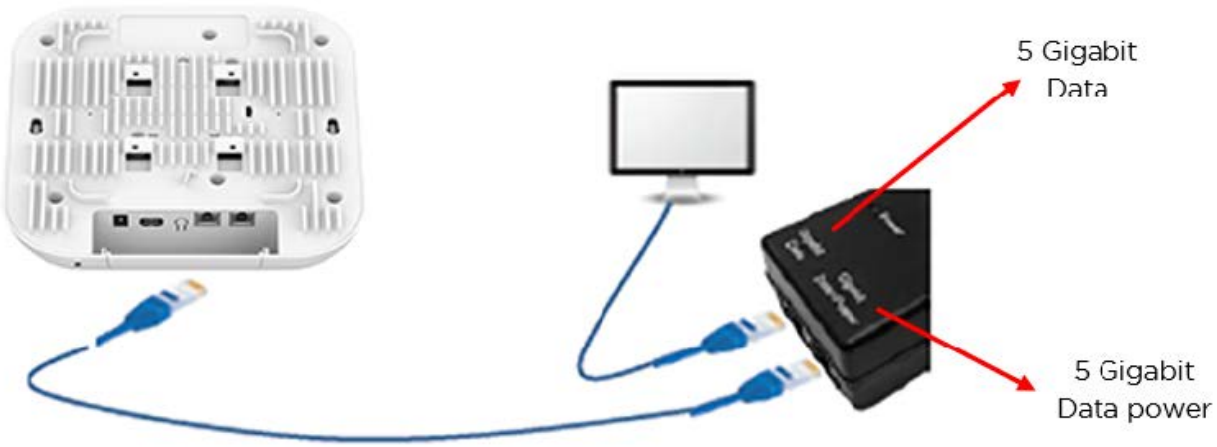
Serial Number	PSE detection mode	Power Available for AP	LLDP Power Negotiation	Modules
1	802.3af	Critical	Yes	• Wireless modules: Enabled • USB port: Disabled • BT module: Disabled
2	802.3at	Limited	Yes	• Wireless modules: Enabled • USB port: Disabled • BT module: Disabled
3	802.3bt Class-0/1/2/3	Critical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

PoE adapter

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

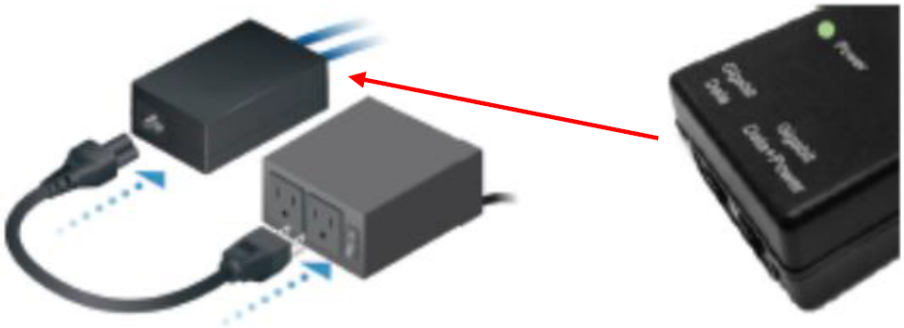
1. Connect the Ethernet cable from Eth1/PoE-IN of the device to the PoE port of 5 Gigabit Data + Power.
2. Connect an Ethernet cable from your LAN or Computer to the 5 Gigabit Data port of the PoE adapter.

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



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

Figure 3: *Installation of adapter to power outlet*



DC Power supply

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

Accessing the device

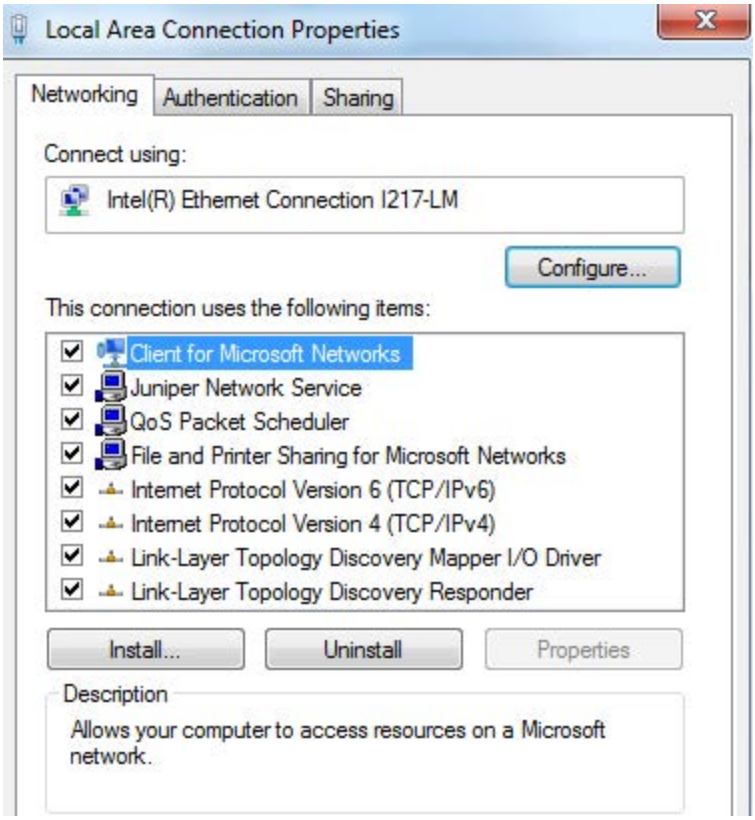
This section includes the following topics:

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

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

Device access using default/fallback IP

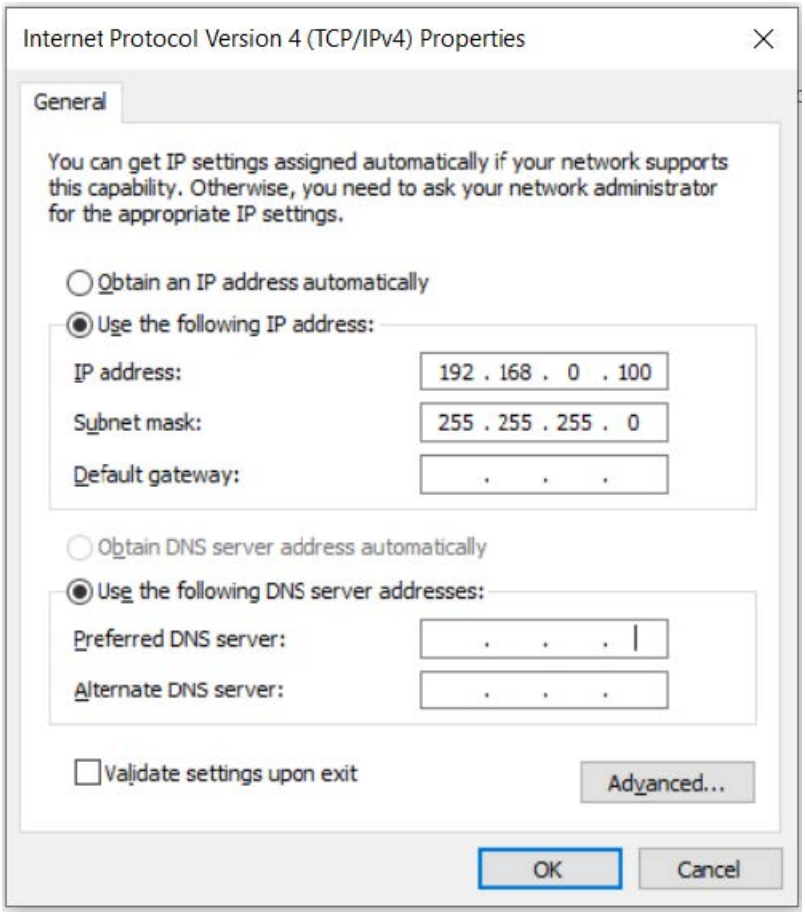
1. Select properties for the Ethernet port:
    a. For Windows 7: **Control Panel > Network and Internet > Network Connections > Local Area Connection**
    b. For Windows 10: **Control Panel > Network and Internet > Network and Sharing Center > Local Area**



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

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

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

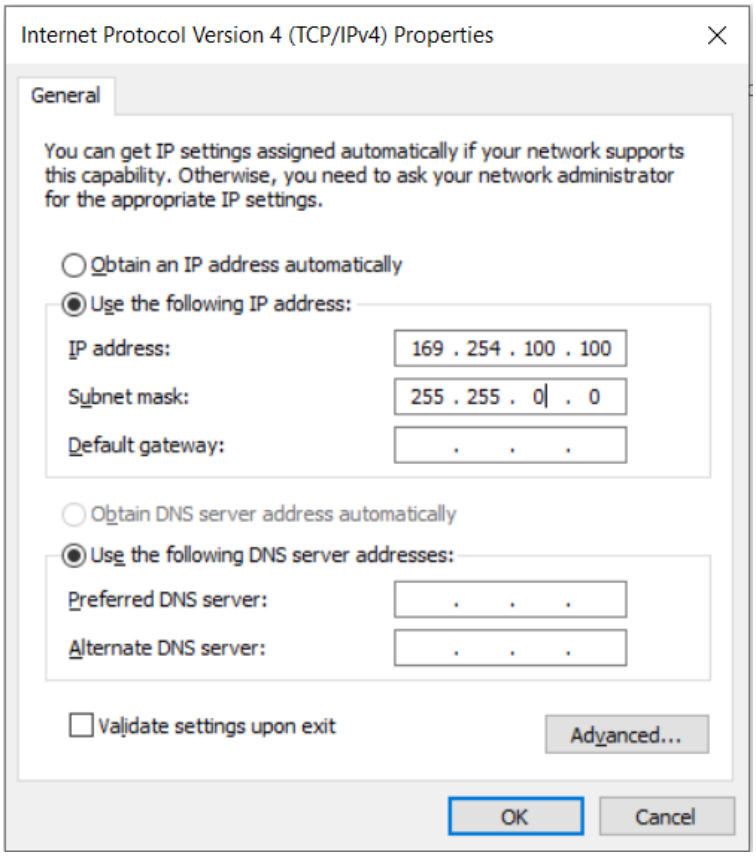


4. In the Use the following IP address section, ensure that an appropriate IP address and a subnet address are provided.
5. Click OK.
6. Ensure that your PC is set up to communicate with the required range of IP addresses.
7. Open a web browser and type the URL - http://192.168.0.11 - to access the device UI. The Sign In page appears.
8. Type an appropriate username and password.
    a. Default username: admin
    b. Default password: admin
9. Click **Sign In**.

Device access using zeroconf IP

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

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



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

- Username: admin
- Password: admin

Device access using DHCP IP address

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

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

LED Status

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

Table 6: Enterprise Wi-Fi AP LED status

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

Chapter 2: Onboarding the Device

This chapter describes the following topics:

Overview

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

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

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

Device onboarding and provisioning

Enterprise Wi-Fi APs support the following onboarding methods:

cnMaestro cloud

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

For onboarding devices to cnMaestro cloud, refer to cnMaestro Onboarding Devices.

XMS-Cloud

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

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

Swift

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

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

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


Download on the
App Store


GET IT ON
Google Play

Chapter 3: Using the UI

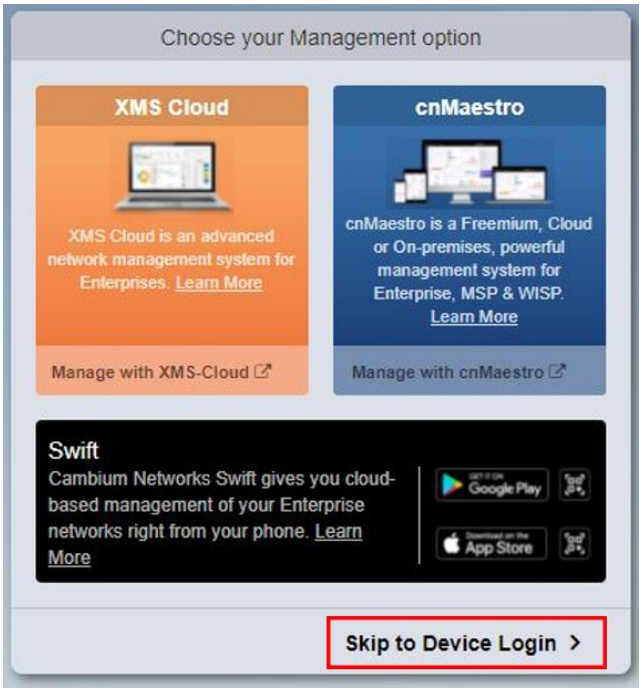
You can manage Enterprise Wi-Fi AP devices using the on-device User Interface (UI), which is accessible from any network device such as computer, mobile, and tabs. This chapter explains how to access the UI of the Enterprise Wi-Fi AP device.

This chapter describes the following topics:

Logging into the UI

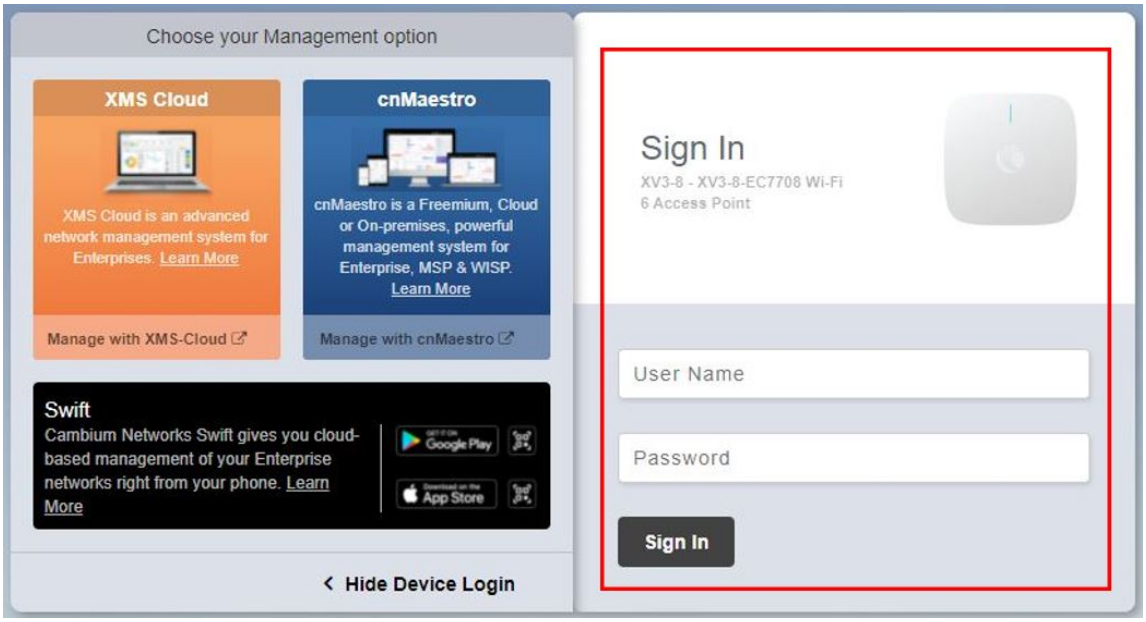
User can select the Management options as **XMS-Cloud** or **cnMaestro** to manage the device, as shown in Figure 1.

Figure 4: *The Management option page*



If the user needs to login to the device login page, click **Skip to Device Login.** The **Sign In** tab appears, as shown in Figure 2.

Figure 5: *The device UI login page*



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

- User Name: admin
- Password: admin

Viewing the Home page (dashboard)

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

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

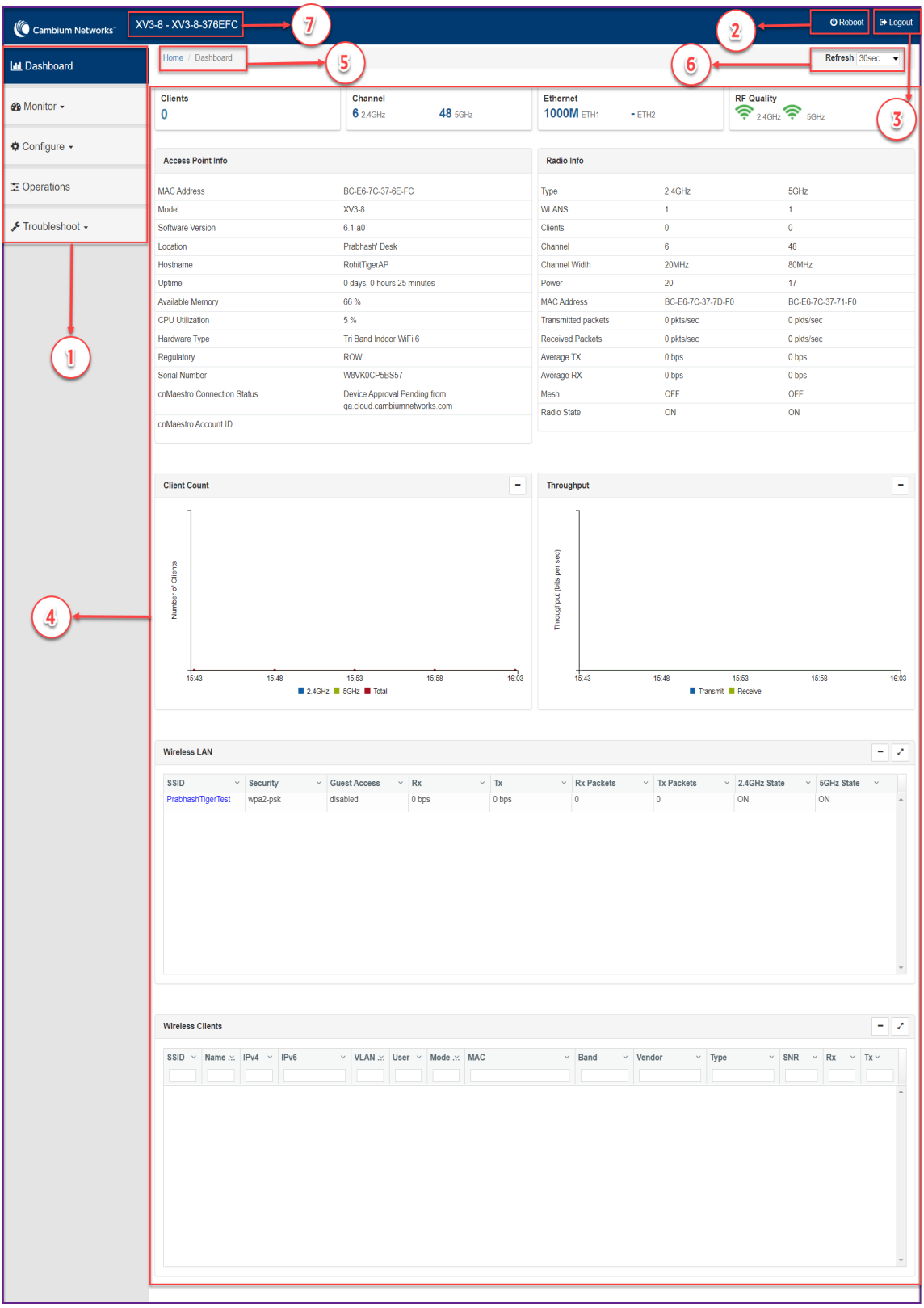


Table 7: Elements in the Enterprise Wi-Fi AP dashboard page

Number	Element	Description
1	Menu	This section contains multiple tabs that help the user to configure, monitor, and troubleshoot the Enterprise Wi-Fi AP device. The menu consists of the following setting options: • 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 the web interface varies based on the tab selected in the Menu section. Usually, this area contains details of configuration or statistics or provision to configure Enterprise Wi-Fi AP device.
5	UI path	Provides UI navigation path information to the user.
6	UI refresh interval	Provision to reload updated statistics at regular intervals.
7	Model number	Provides information related to the Enterprise Wi-Fi AP model number and configured hostname.

Monitor

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

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

Configure

This section allows users to configure Enterprise Wi-Fi AP devices based on deployment requirements. The Configure tab contains multiple sections, as follows:

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

Operations

This section allows users to perform maintenance tasks of devices such as the following:

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

Troubleshoot

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

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

Chapter 4: Configuring the System

This chapter describes the following topics:

System

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

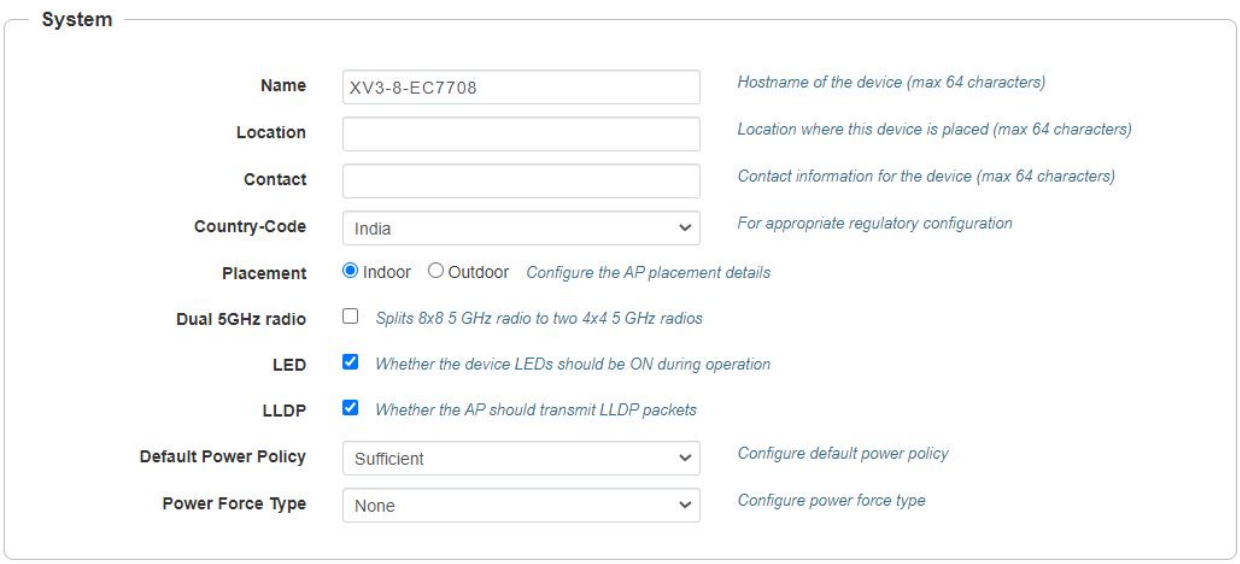
Table 8: System parameters

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

Figure 1 shows the System UI page.

Figure 7: *The System page*



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

Power over Ethernet (PoE) Output port

PoE provisions to power on an RJ45 standard IEEE802.3af/at devices or Cambium Networks devices. By default, this feature is disabled.

The feature is supported by following AP products:

- XV3-8
- XV2-2T

By default, this feature is disabled on supported APs. The PoE output port is managed by CLI `poe-out`.

CLI Configuration

Consider the following tasks to configure the CLI:

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
```

Link Layer Discovery Protocol (LLDP)

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

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

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

Power negotiation

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

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

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

CLI Configuration

Consider the following tasks to configure the CLI:

To enable:

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

To list LLDP configuration:

`show lldp configuration`

`show lldp interfaces`

Request power

To enable/disable power negotiation via LLDP:

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

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



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

  <ENTER>



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

Transmit hold

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

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

  request-power         : Enable power negotiation (default:enabled)
  tx-hold               : Set transmit hold multiplier (default:4, used to calculate th
e 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 th
e 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
```

Management

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

Table 9: Management parameters

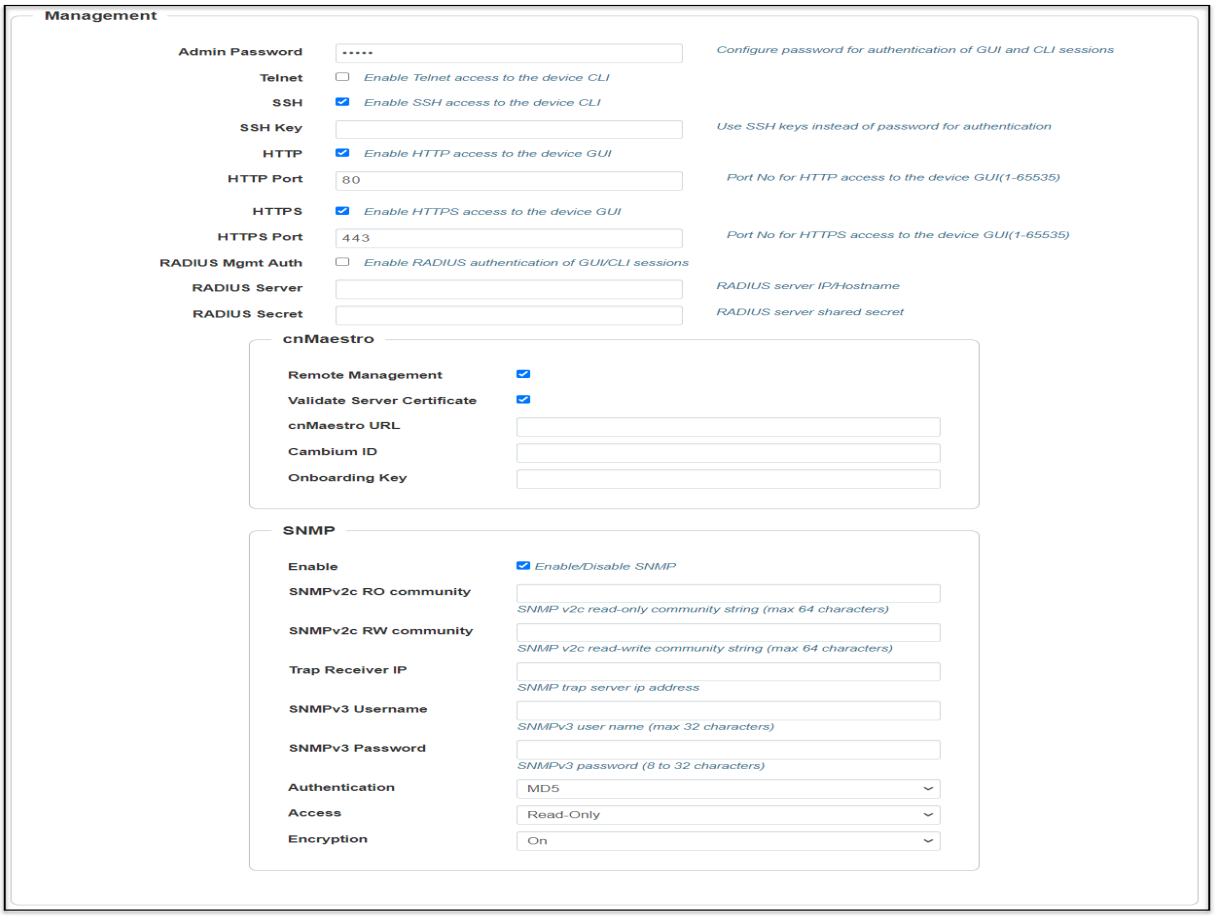
Parameter	Description	Range	Default
Admin Password	Password for authentication of UI and CLI sessions.	-	admin
Telnet	Enables Telnet access to the device CLI.	-	Disabled

Parameter	Description	Range	Default
SSH	Enables SSH access to the device CLI.	-	Enabled
SSH Key	Provision to login to device using SSH Keys. The user needs to add Public Key in this section. If configured, the user has to login to AP using Private Keys. This is applicable for both CLI and GUI.	-	Disabled
HTTP	Enables HTTP access to the device UI.	-	Enabled
HTTP Port	Provision to configure HTTP port number to access device UI.	1-65535	80
HTTPS	Enables HTTPS access to the device UI.	-	Enabled
HTTPS Port	Provision to configure HTTPS port number to access device UI.	1-65535	443
RADIUS Mgmt Auth	User has provision to control login to AP using RADIUS authentication. If enabled, every credential that is provided by the user undergo RADIUS authentication. If successful, allowed to login to UI of the device. This is applicable for both CLI and GUI.	-	Disabled
RADIUS Server	Provision to configure RADIUS IPv4 server for Management Authentication.	-	-
RADIUS Secret	Provision to configure RADIUS shared secret for Management authentication.	-	-
cnMaestro			
Cambium Remote Mgmt.	Enables support for Cambium Remote Management of this device.	-	Enabled
Validate Server Certificate	This allows HTTPs connection between cnMaestro and Enterprise Wi-Fi AP device.	-	Enabled
cnMaestro URL	Static provision to onboard devices either using IPv4 URL.	-	-
Cambium ID	Cambium ID is used for provisioning cnMaestro (Cambium Remote Management) of this device.	-	-
Onboarding Key	Password used for onboarding the device to cnMaestro.	-	-
SNMP			
Enable	Provision to enable SNMPv2 or SNMPv3 support on the device	-	-
SNMPv2c RO community	SNMP v2c read-only community string.	-	public
SNMPv2c RW community	SNMP v2c read-write community string.	-	private
Trap Receiver IP	Provision to configure SNMP trap receiver IPv4 server.	-	-

Parameter	Description	Range	Default
SNMPv3 Username	Enter the username for SNMPv3.	-	-
SNMPv3 Password	Enter the password for SNMPv3.	-	-
Authentication	Provision to choose the authentication type as MD5 or SHA.	-	MD5
Access	Provision to choose Access type as RO or RW.	-	RO
Encryption	Choose ON or OFF.	-	ON

Figure 2 shows the Management page.

Figure 8: *The Management page*



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

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

If certificate-based login is required, enter SSH Key in the textbox else select

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

To configure **cnMaestro**:

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

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 supports SNMP only v1 and v2c Traps) in the textbox.
5. Enter the SNMP V3 username in the **SNMPv3 Username** textbox.
6. Enter the SNMP V3 password in the **SNMPv3 Password** textbox.
7. Select MD5 or SHA from the **Authentication** 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**.

HTTPS Proxy server configuration

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

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

CLI Configuration:

```
XV3-8-EC7708(config)# management proxy

  https                 : Enable HTTPS proxy support


XV3-8-EC7708(config)# management proxy https

  host                  : Configure HTTPS proxy host
  password              : Configure HTTPS proxy password
  port                  : Configure HTTPS proxy port
  username              : Configure HTTPS proxy username
```

Time settings

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

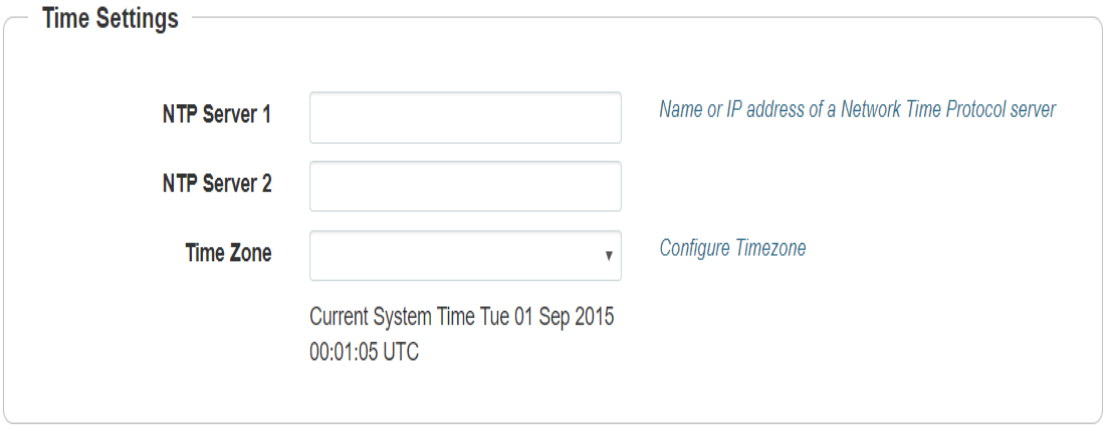
Table 10 lists the fields that are displayed in the **Configuration > System > Time Settings** section.

Table 10: Time Setting 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	The time zone can be set according to the location where the AP is installed. Selecting the appropriate time zone from the drop-down list, ensures that the device clock is synced with the wall clock time. **Note** Accurate time on the AP is critical for features such as WLAN Scheduled Access, and Syslogs.	-	-

Figure 3 shows the Time setting page.

Figure 9: *Time setting page*



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**.

Event logging

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

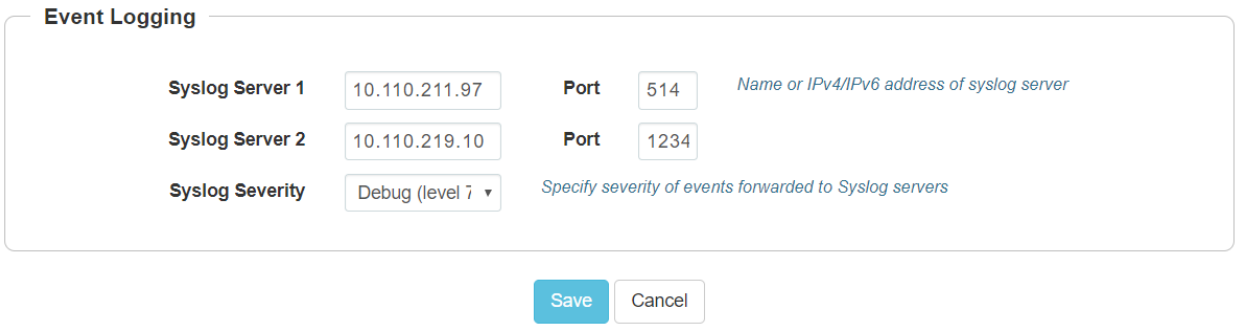
Table 11 lists the fields that are displayed in the **Configuration > System > Event Logging** section.

Table 11: Event logging parameters

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

Figure 4 shows the Event logging page.

Figure 10: *Event logging page*



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

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

Chapter 5: Configuring the Radio

This chapter describes the following topics:

Overview

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

Configuring Radio parameters

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

Basic

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

Table 12: Configure Radio parameters

Parameter	Description	Range	Default
Radio			
Enable	Enables the operation of radio.	-	Enabled
Band	If any radio supports multiple bands then the user can select one of the bands.	-	-
Channel	The user can select the channel from the drop-down list. Channels in the drop-down list are populated based on the Country selected in **Configuration > System** UI.	**2.4 GHz:** 1 - 14 **5 GHz:** 36 - 173	Auto
Channel Width	The user can select the following channel widths for the operation: • For 2.4 GHz: Only 20 MHz channel width is supported.	-	20 MHz for 2.4 GHz and 5 GHz

Parameter	Description	Range	Default
	• For 5 GHz: 20 MHz, 40 MHz, 80 MHz, and 160 MHz channel width are supported.		
Transmit Power	The user can configure transmit power of each radio based on coverage and SLA. Unit of transmit power is in dBm and its range is from 4 to 30. The maximum transmit power of Enterprise Wi-Fi AP devices varies based on model number. More details of transmit power supported by each Enterprise Wi-Fi AP device are available at https://www.cambiumnetworks.com/products/wifi/. Transmit power drop-down box varies as per the country selected in Configuration > System UI. The default value is AUTO, which means radio transmit power is configured to the maximum as per the county configured selected in the **Configuration > System** UI.	**2.4 GHz:** 4 - 30 **5 GHz:** 4 - 30	Auto
Beacon Interval	The user can configure time duration between two consecutive Beacons. It is termed as Beacon interval.	50ms - 3400ms.	100
Minimum Unicast rate	Provision to adjust the coverage area of Enterprise Wi-Fi AP device. Higher the rate selected, the lesser the range. The user can configure this value based on SLA in deployment. The drop-down list contains all values that are advertised by Enterprise Wi-Fi AP devices which include legacy, HT, and VHT rates.	Standard 802.11b and 802.11g data rates	1Mbps

Candidate Channels	Enterprise Wi-Fi AP provides the user to configure selective channels based on their requirement. Options vary based on a band of operation and are as follows:
	• **For 2.4 GHz:**
	  • All
	  • Specific
	• **For 5 GHz:**
	  • 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

Parameter	Description	Range	Default
Short Guard Interval	Standard 802.11 parameter to increase the throughput of Enterprise Wi-Fi AP device.	-	Enabled
Off Channel Scan (OCS)			
Enable	Provision to enable OCS on a device to capture neighbor clients and APs.	-	-
Dwell-time	Configure the time period to spend scanning of Wi-Fi devices on a channel.	50-300	50ms
Auto-RF			
Dynamic Power	Provision to enable dynamic power management.	-	-
Mode	Select the required dynamic power modes. Two modes are supported: 1. By-channel 2. By-band	-	By-channel
Minimum Transmit Power	The minimum transmit power that the AP can assign to radio when adjusting automatic cell sizes	5-15 dBm	8 dBm
Minimum Neighbour Threshold	The minimum number of neighbors to consider for power reduction by automatic cell logic.	1-10	2
Cellsize Overlap Threshold	Cell overlap will be allowed when the AP is determining automatic cell sizes.	0-100%	50%

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

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

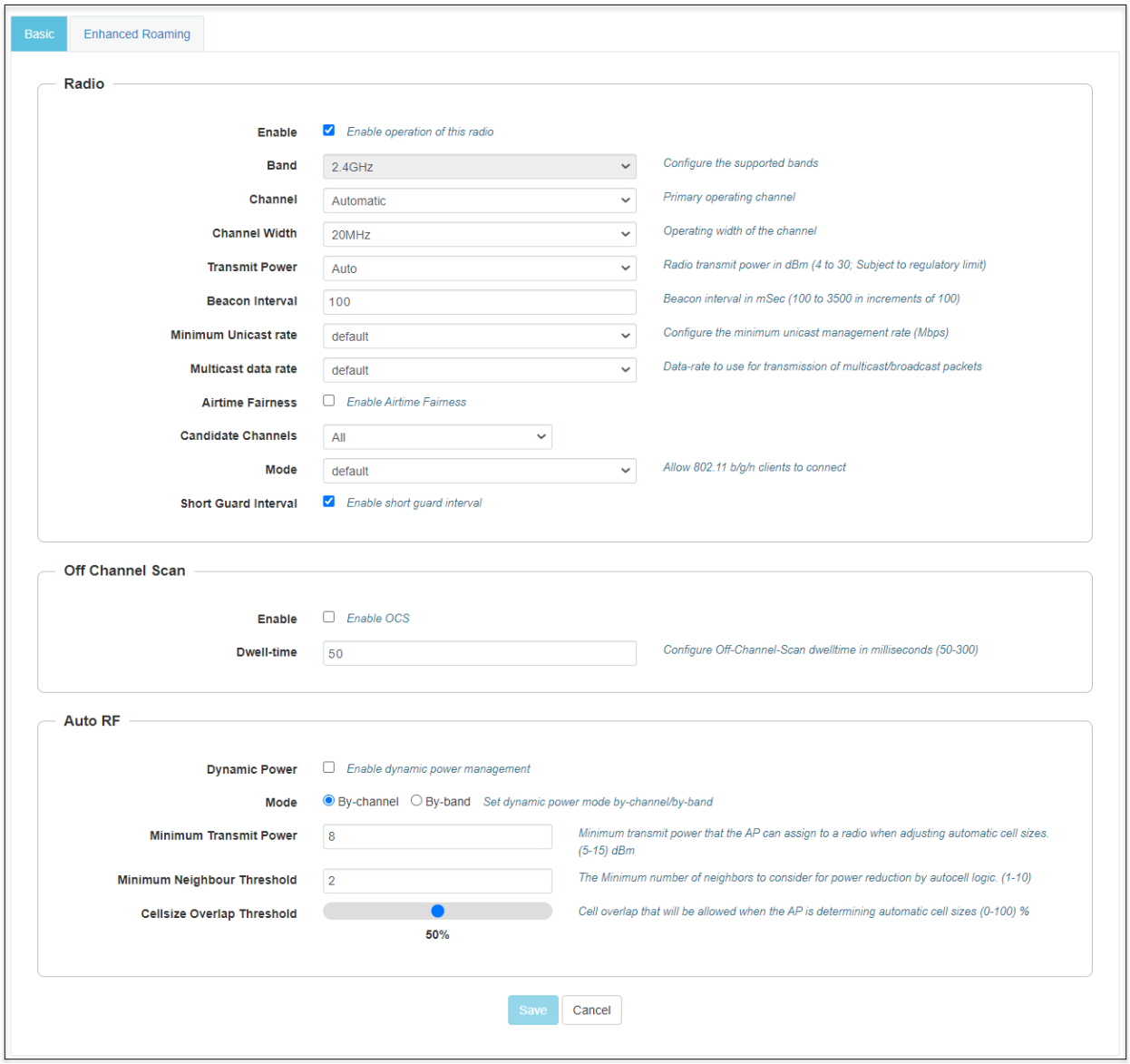
To configure **Off Channel Scan**:

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

To configure **Auto-RF**:

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

Figure 11: *Radio parameters in the Basic page*



Off Channel Scan (OCS)

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

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

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



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

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

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

Table 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	Provision to configure Off Channel Scan types. • active AP Radio transmits a probe request and listens for a probe response from an AP. • passive AP Radio listens on each channel for beacons sent periodically by neighbor APs. Users are advised to use passive as scan type.	-	active

Enhanced Roaming

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

Table 14: Configure: Radio Enhanced Roaming parameters

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

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

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

Figure 12: *The Enhanced Roaming parameters*

BSS Coloring

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

Target Wake Time (TWT)

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

Note

By default, BSS coloring and TWT are enabled.

Receive sensitivity configuration

This feature enables users to configure the receiver sensitivity per radio. The configuration hooks are exposed from both CLI and XMS-Cloud. The cnMaestro does not expose any hooks for configuring receiver configuration. The receiver configuration is the signal power required at the receiver to achieve the targeted or configured bit rate. Every RF receiver comes up with some default receiver sensitivity which may or may not be sufficient for achieving required RF performance in terms of meeting bit rate, hence reconfiguration of receiver sensitivity is suggested.

Multicast-snooping and Multicast-to-Unicast conversion

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

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

CLI Configuration:

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


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

IPv4 Router Ports:      None


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

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

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

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

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

```
XV3-8-EC7708(config)# wireless radio 1
XV3-8-EC7708(config-radio-1)# multicast-to-unicast
XV3-8-EC7708(config-radio-1)# 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 6: Configuring the Wireless LAN

This chapter describes the following topics:

Overview

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

Configuring the WLAN parameters

Configurable parameters under the WLAN profile are listed below:

Basic

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

Table 15: Basic parameters

Parameters	Description	Range	Default
WLAN > Basic			
Enable	An option to enable a WLAN profile. Once enabled, a Beacon is broadcasted with SSID and respective configured parameters in a WLAN profile.	-	-

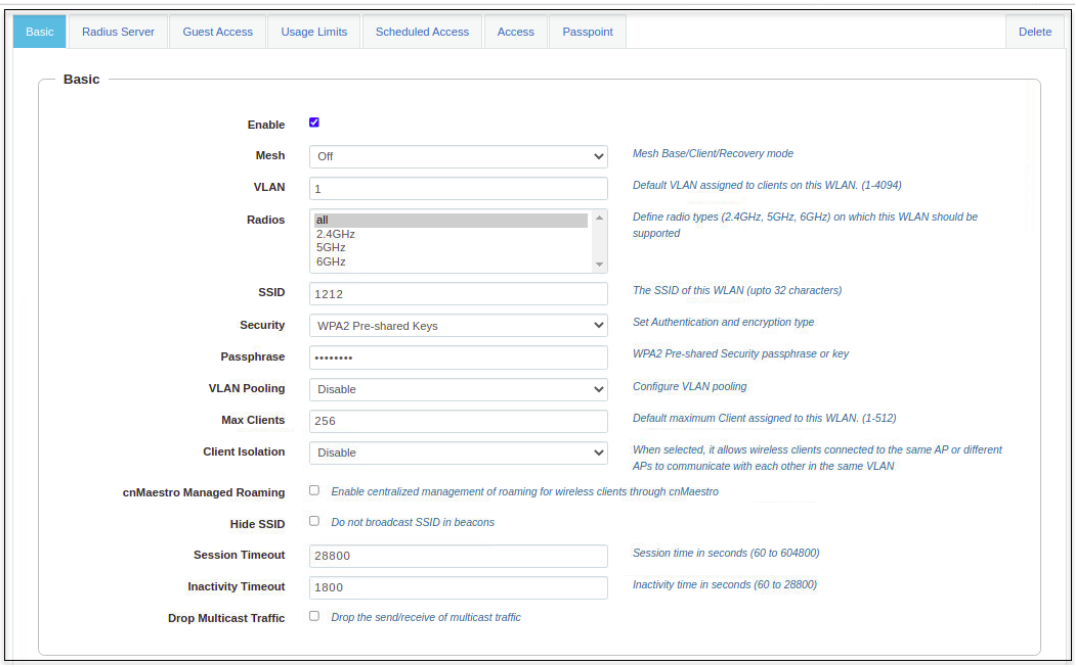
Parameters	Description	Range	Default
Mesh	This parameter is required when a WDS connection is established with Enterprise Wi-Fi devices. This parameter supports the following four options: 1. **Base** A WLAN profile configured with a mesh-base will operate as a normal AP. Its radio will beacon on startup so its SSID can be seen by radios configured as mesh-clients. 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 a pre-configured SSID upon detection of mesh link failure after a successful connection. This needs to be exclusively configured on a mesh-base device. Meshclient will auto scan for mesh-recovery SSID upon failure of mesh link. 4. **Off** Mesh support disabled on WLAN profile.	-	OFF (Access Profile Mode)
SSID	SSID is the unique network name that wireless stations scan and associate.	-	-
VLAN	VLAN is configured to segregate wireless station traffic from AP traffic in the network. Wireless stations obtain an IP address from the subnet configured in the VLAN field of the WLAN profile.	1-4094	1
Security	This parameter determines key values that are encrypted based on the selected algorithm. Following security methods are supported by Enterprise Wi-Fi AP devices: 1. **Open** This method is preferred when Layer 2 authentication is built into the network. With this configured on an 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.	-	Open

Parameters	Description	Range	Default
	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. 4. **WPA2 Enterprise** This security type uses 802.1x authentication to associate wireless stations. This is a centralized system of authentication methods. 5. **WPA2/WPA3 Pre-shared Keys** WPA3 comes with a transition mode where WPA2-only capable clients can connect to SSID. WPA2-only capable clients connect using the older PSK method while WPA3 capable clients connect using a more secure Simultaneous Authentication of Equals (SAE) method. 6. **WPA3 Pre-shared Keys** WPA3 replaces the Pre-Shared Key (PSK) exchange with SAE of Equals, which is more secure and provides forward-secrecy as well as resistance to offline dictionary attack. 7. **WPA3 Enterprise** WPA3 also introduces Enterprise AES CCMP encryption. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. 8. **WPA3 Enterprise CNSA** WPA3 also introduces a 192-bit cryptographic security suite. This level of security provides consistent cryptography and eliminates the mixing and matching of security protocols that are defined in the 802.11 standards. This security suite is aligned with the recommendations from the Commercial National Security Algorithm (CNSA) Suite and is commonly used in high-security Wi-Fi networks in government, defense, Finance, and industrial verticals.		
Passphrase	The string that is a key value to generate keys based on the security method configured.	-	12345678
Radios	Each SSID can be configured to be transmitted as per the deployment requirement. For a regular access profile, options are available to configure transmit mode of SSID: • 2.4 GHz • 5 GHz • 6 GHz	-	all

Parameters	Description	Range	Default
VLAN Pooling	This parameter is required when a user requires to distribute clients across multiple subnets. Different modes of VLAN pooling is supported by Enterprise Wi-Fi AP devices, based on infrastructure available at the deployment site. Modes supported are as follows: 1. Disabled This feature is disabled for this WLAN. 2. Radius Based The user is expected to configure WPA2 Enterprise for this mode to support. During the association phase, AP obtains pool name from RADIUS transaction and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IP address from the VLAN selected by Enterprise Wi-Fi AP device. 3. Static For this mode to support, the user requires to configure VLAN Pool details available under **Configure > Network > VLAN pool**. During the association phase, AP obtains pool, and based on the present distribution of wireless station across VLANs, AP selects appropriate VLAN and wireless station requests an IPv4 address from the VLAN selected by the Enterprise Wi-Fi AP device.	–	Disabled
Max Clients	This specifies the maximum number of wireless stations that can be associated with a WLAN profile. This varies based on the Enterprise Wi-Fi AP device model number. Refer to Table 16 for more details.	1-512 (Refer Table 16)	256
Client Isolation	This feature needs to be enabled when there is a need for restriction of wireless station to station communication across the network or on an AP. Four options are available to configure based on requirement: 1. **Disable** This option when selected disables the client isolation feature. i.e. any wireless station can communicate to other wireless stations. 2. **Local**		

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

Figure 13: *Basic parameter*



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

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

Table 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

Table 17: Advanced parameters

<table>
<tr><th>Parameters</th><th>Description</th><th>Range</th><th>Default</th></tr>
<tr><td colspan="4">WLAN > Advanced</td></tr>
<tr><td>UAPSD</td><td>When enabled, Enterprise Wi-Fi AP devices support WMM Power Save / UAPSD. This is required where applications such as VOIP Calls, Live Video streaming are in use. This feature helps to prioritize traffic. Below is the default traffic priority followed by the Enterprise Wi-Fi AP device.
<table>
<tr><th>Priority</th><th>802.1D Priority (= UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr>
<tr><td rowspan="8">lowest
↓
highest</td><td>1</td><td>BK</td><td rowspan="2">AC_BK</td><td rowspan="2">Background</td></tr>
<tr><td>2</td><td>-</td></tr>
<tr><td>0</td><td>BE</td><td rowspan="2">AC_BE</td><td rowspan="2">Best Effort</td></tr>
<tr><td>3</td><td>EE</td></tr>
<tr><td>4</td><td>CL</td><td rowspan="2">AC_VI</td><td rowspan="2">Video</td></tr>
<tr><td>5</td><td>VI</td></tr>
<tr><td>6</td><td>VO</td><td rowspan="2">AC_VO</td><td rowspan="2">Voice</td></tr>
<tr><td>7</td><td>NC</td></tr>
</table></td><td>–</td><td>Disabled</td></tr>
<tr><td>QBSS</td><td>When enabled, appends QBSS IE in Management frames. This IE provides information on channel usage by AP, so that smart wireless stations can decide better AP for connectivity. Station count, Channel utilization, and Available admission capacity are the information available in this IE.</td><td>–</td><td>Disabled</td></tr>
<tr><td>DTIM interval</td><td>This parameter plays a key role when power save supported mobile stations are part of the infrastructure. This field when enabled controls the transmission of Broadcast and Multicast frames.</td><td>1-255</td><td>1</td></tr>
<tr><td colspan="4">Monitored Host</td></tr>
</table>

Parameters	Description	Range	Default
Host	This feature is required where there is an interrupted backbone network. Enterprise Wi-Fi AP device monitors the reachability of hostname/IP configured in this parameter and modifies the state of WLAN.	-	Disabled
Interval	The frequency of monitoring the network health based on the status of the keep-alive mechanism w.r.t configured monitored host.	60-3600 sec	300
Attempts	The number of packets in the keep-alive mechanism to determine the status.	1-20	1
DNS Logging Host	By enabling this feature, the Administrator can monitor the websites accessed by wireless stations connected to WLAN profile.	–	Disabled
Connection Logging Host	When enabled provides information of all TCP connections accessed by a wireless station that is associated with WLAN.	–	Disabled
Band Steering	This feature when enabled steers wireless stations to connect to 5GHz. There are three modes supported by Enterprise Wi-Fi devices. The mode can be selected based on either deployment or wireless station type. Below is the order of modes, which forces the wireless station to connect to the 5 GHz band. • Low • Normal • Aggressive	–	Disabled
Proxy ARP	Provision to avoid ARP flood in a wireless network. When enabled, AP responds to ARP requests for the wireless stations connected to that AP. This is for IPv4 infrastructure.	–	Enabled
Insert DHCP Option 82	When enabled, DHCP packets generated from wireless stations that are associated with APs are appended with Option 82 parameters. Option 82 provides a provision to append Circuit ID and Remote ID. Following parameters can be selected in both Circuit ID and Remote ID: • Hostname • AP MAC • BSSID • SSID • VLAN ID • SITEID • Custom	–	Disabled

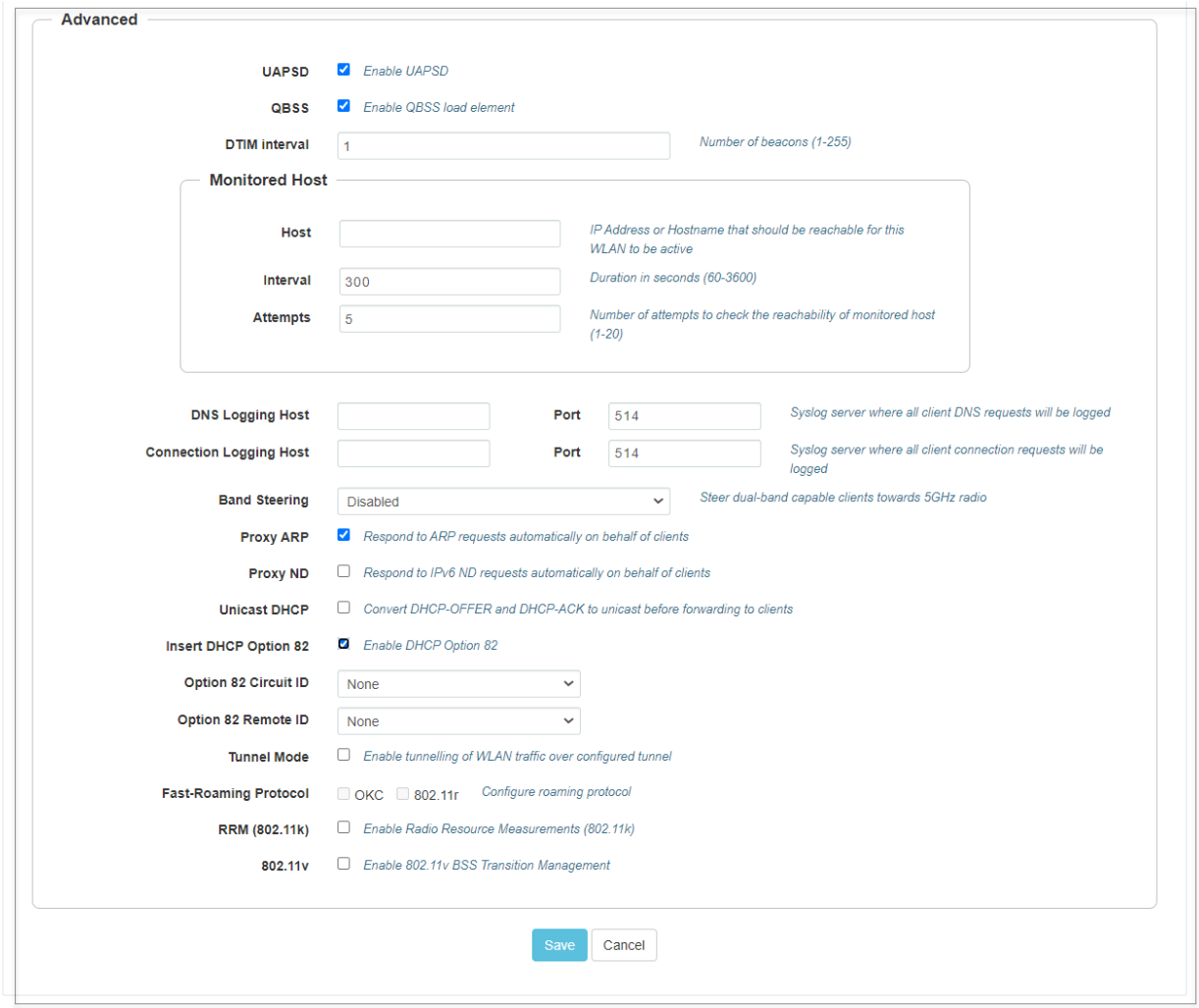
Parameters	Description	Range	Default
	• All		
Tunnel Mode	This option is enabled when user traffic is tunneled to the DMZ network either using L2TP or L2GRE.	–	Disabled
Fast-Roaming Protocol	One of the important aspects to support voice applications on a Wi-Fi network (apart from QoS) is how quickly a client can move its connection from one AP to another. This should be less than 150 msec to avoid any call drop. This is easily achievable when the WPA2-PSK security mechanism is in use. However, in enterprise environments, there is a need for more robust security (the one provided by WPA2-Enterprise). With WPA2-Enterprise, the client exchanges multiple frames with the AAA server, and hence depending on the location of the AAA server the roaming time will be above 700 msec. Select any one of the following: 1. **OKC** This roaming method is a Cambium Networks proprietary solution to share the client authentication information with other Cambium Networks APs on the same network by sending encrypted information on wire on SSID VLAN. This information sharing does not require cnMaestro so even in cases where AP is not connected to cloud, the roaming will be seamless. 2. **802.11r** Fast transition (FT) is an IEEE standard to permit continuous connectivity aboard wireless devices in motion, with fast and secure client transitions from one Basic Service Set (abbreviated BSS, and also known as a base station or more colloquially, an access point) to another performed in a nearly seamless manner. The terms handoff and roaming are often used, although 802.11 transition is not a true handoff/roaming process in the cellular sense, where the process is coordinated by the base station and is generally uninterrupted.	–	Disabled
RRM (802.11k)	AP sends the SSID name of the neighbor APs (SSID configured on multiple APs) to 11k clients. The following parameter needs to be enabled: • Enable RRM	–	Disabled
802.11v	Provision to enable 802.11v BSS Transition Management.	–	Disabled
PMF (802.11w)	802.11w also termed as Protected Management Frames (PMF) Service, defines encryption for management frames. Unencrypted management frames make wireless connection vulnerable to DoS attacks as well as they cannot protect important information exchanged using management frames from eavesdroppers.	–	Optional

Parameters	Description	Range	Default
SA Query Retry Time	The legitimate 802.11w client must respond with a Security Association (SA) Query Response frame within a pre-defined amount of time (milliseconds) called the SA Query Retry time.	100-500	100ms
Association Comeback Time	This value is included in the Association Response as an Association Comeback Time information element. AP will deny association for the configured interval.	1-20	1 Sec

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

1. Select the **UAPSD** checkbox to enable UAPSD.
2. Select the **QBSS** checkbox to enable QBSS.
3. Enter the value in the **DTIM interval** textbox to configure the DTIM interval.
4. Enter IP address or Hostname in **Host** textbox.
5. Enter **Interval time** duration in the textbox.
6. Select number of attempts to check the reachability of the monitored host in the **Attempts** drop-down list.
7. Enter the FQDN or IP address of the server where all the client DNS requests will be logged in the **DNS Logging Host** server along with a customized port number in the textbox. If the port number is not entered, AP will take the default value as 514.
8. Enter the FQDN or IP address of the server where all wireless client connectivity events/logs will be displayed in the configured **Connection Logging Host** server along with a customized port number in the textbox. If the port number is not entered, AP will take the default value as 514.
9. Select **Band Steering** parameter for 5GHz band from the drop-down list.
10. Enable **Proxy ARP** checkbox to avoid ARP flood in a wireless network.
11. Enable **Insert DHCP Option 82** checkbox.
12. Select **Option 82 Circuit ID** to enable DHCP Option-82 from the drop-down list.
13. Select **Option 82 Remote ID** to choose the MAC address of the AP from the drop-down list.
14. Select **Tunnel Mode** checkbox to enable tunneling of WLAN traffic over the configured tunnel.
15. Enable the required OKC or 802.11r configure roaming protocol in the **Fast-Roaming Protocol** checkbox.
16. Enable **RRM (802.11k)** checkbox.
17. Enable **802.11v** checkbox.
18. Select **PMF (802.11w)** parameter from the drop-down list.
    a. Enter **SQ Query Retry Time** in the textbox.
    b. Enter **Association Comeback Time** in the textbox.
19. Click **Save**.

Figure 14: *Advanced parameter*



Band steering also supports 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

802.11k

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

The client can request a neighbor report from the AP using the neighbor_report_req management message. The client may request neighbors with **matching** SSID or request for all neighbors in the vicinity.

The AP collects the neighbor information using proprietary methods and provides the list of neighbors to the client in the neighbor_report_rsp message.

802.11v

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

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

Radius server

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

Table 18: Radius Server parameters

Parameters	Description	Range	Default
Authentication Server	Provision to configure RADIUS Authentication server details such as Hostname/IPv4, Shared Secret, Port Number and Realm. A maximum of three RADIUS servers can be configured.	-	Disabled
Accounting Server	Provision to configure Accounting server details such as Hostname/IPv4, Shared Secret, Port Number. A maximum of three RADIUS servers can be configured.	-	Disabled
Timeout	This field indicates wait time period for a response from the AAA server.	1-30	3
Attempts	Parameter to configure many attempts that a device should send AAA request to server if no response is received within the configured timeout period.	1-3	1
Accounting Mode	This field is enabled based on customer requirements. The accounting packet is transmitted based on the mode selected. 1. Start-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station is connected and then disconnects. 2. Start-Interim-Stop Accounting packets are transmitted by AP to the AAA server when a wireless station connects and then at regular intervals of configured Interim Update Interval and then when it disconnects. 3. None	-	Disabled

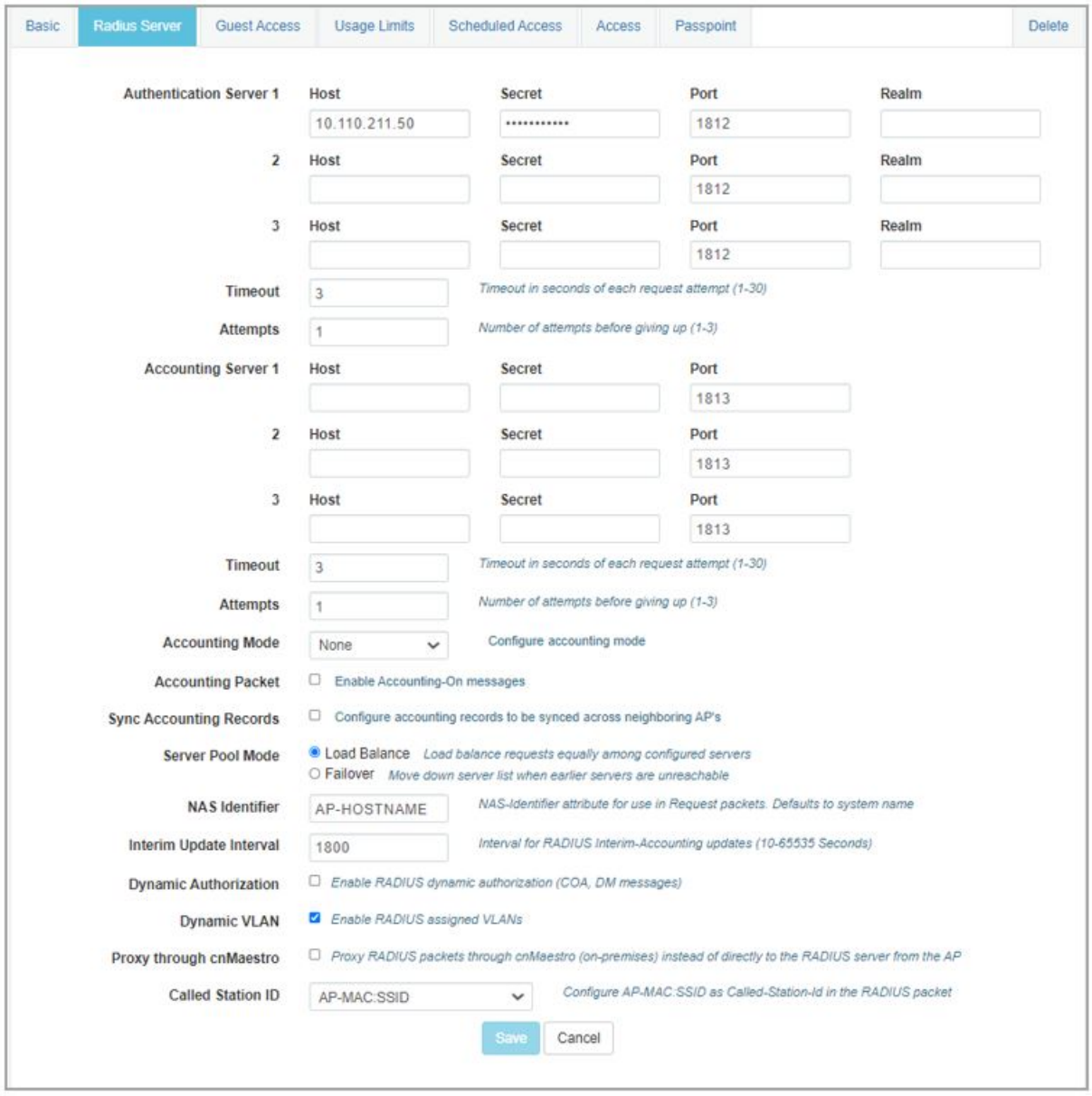
Parameters	Description	Range	Default
	The accounting mode will be disabled.		
Accounting Packet	When enabled, Accounting-On is sent for every client when connected.	-	Disabled
Server Pool Mode	Users can configure multiple Authorization and Accounting servers. Based on a number of wireless stations, the user can choose Failover mode. 1. Failover AP selects the RADIUS server which is up and running based on the order of configuration.	-	Failover
NAS Identifier	This is a configurable parameter and is appended in the RADIUS request packet.	-	Hostname/ System Name
Dynamic Authorization	This option is required, where there is CoA request from AAA/RADIUS server.	-	Disabled
Dynamic VLAN	When enabled, AP honors the VLAN information provided in the RADIUS transaction. Wireless station requests IP address from the same VLAN learned through RADIUS.	-	Enabled
Called Station ID	The following information can be communicated to the RADIUS server: • AP-MAC • AP-MAC: SITE-NAME • AP-MAC: SSID • AP-MAC: SSID-SITE-NAME • AP-NAME • AP-NAME: SITE-NAME • AP-NAME: SSID • SITE-NAME • SSID • CUSTOM	-	AP-MAC: SSID

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

1. Enter the RADIUS Authentication server details such as Hostname, Shared Secret, Port Number or Realm in the **Authentication Server 1** textbox.
2. Enter the time in seconds of each request attempt in the **Timeout** textbox.
3. Enter the number of attempts before a request is given up in the **Attempts** textbox.
4. Select the configuring **Accounting Mode** from the drop-down list.
5. Enable **Accounting Packet** checkbox.

6. Enable **Failover** in the Server Pool Mode checkbox.
7. Enter the **NAS Identifier** parameter in the textbox.
8. Enter the **Interim Update Interval** parameter value in the textbox.
9. Enable **Dynamic Authorization** checkbox to configure dynamic authorization for wireless clients.
10. Enable **Dynamic VLAN** checkbox.
11. Enable **Proxy through cnMaestro** checkbox.
12. Select **Called Station ID** from the drop-down list.
13. Click **Save**.

Figure 15: *The Radius Server parameter page*



Guest Access

Internal Access Point

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

Table 19: Internal Access Point parameters

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

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

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

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

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

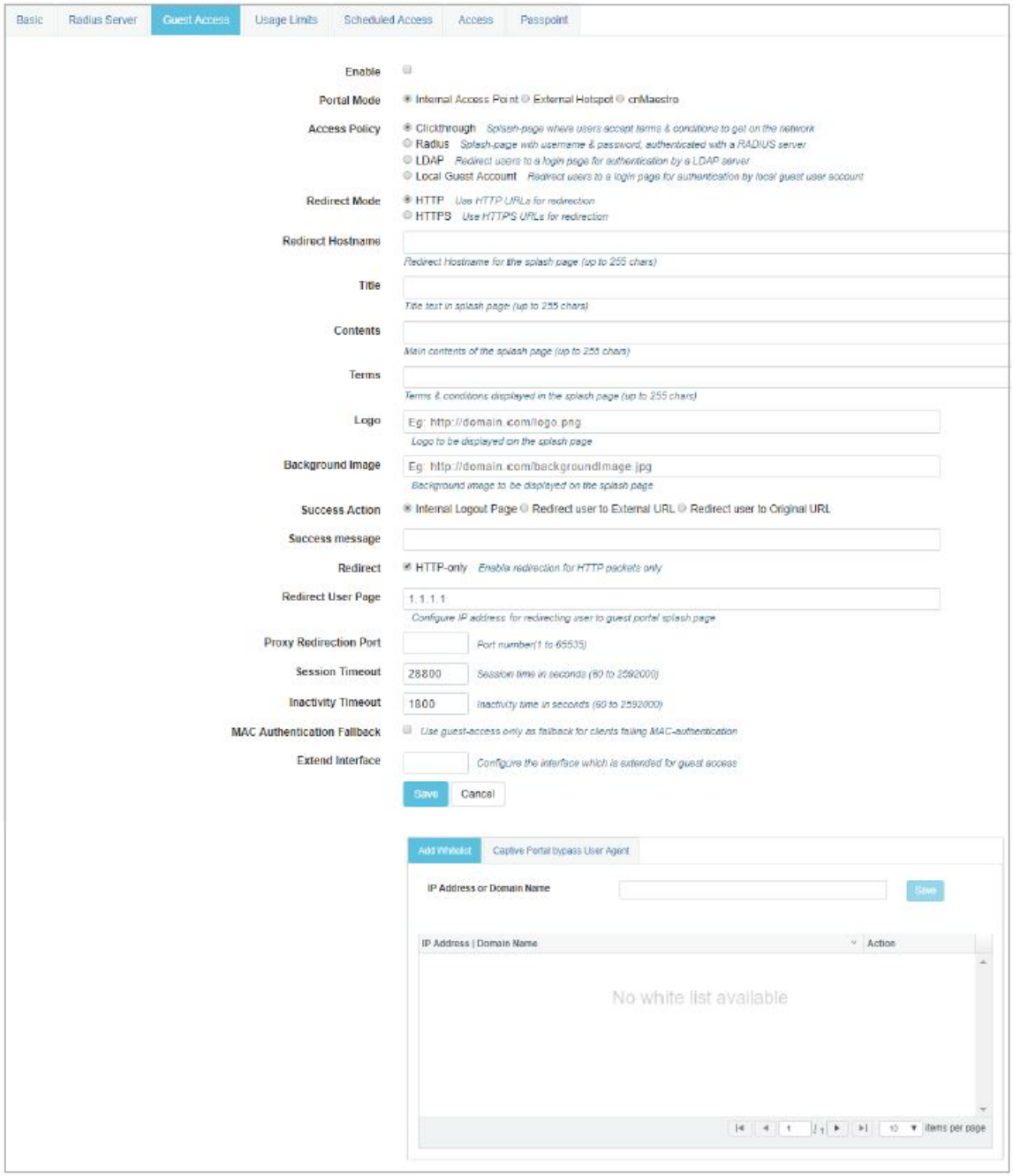
1. Select **Enable** checkbox to enable the Guest Access feature.
2. Enable **Internal Access Point** checkbox.
3. Enable the required access types from the **Access Policy** checkbox.
4. Enable HTTP or HTTPS from the **Redirect Mode** checkbox.
5. Enter **Redirect Hostname** in the textbox.
6. Enter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

17. Enter the inactivity timeout in seconds in the **Inactivity Timeout** textbox.
18. Enable **MAC Authentication Fallback** checkbox if guest-access is used only as a fallback for clients failing MAC-authentication.
19. Click **Save**.

To configure Whitelist parameter:

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

Figure 16: *The Internal Access Point parameter*



External Hotspot

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

Table 20: External Hotspot parameters

Parameters	Description	Range	Default
WLAN > Guest Access > External Hotspot			
Access Policy	There are four types of access types provided for the end user: 1. **Clickthrough** This mode allows users to get access data without any authentication mechanism. The user can access the internet as soon as he is connected and accepts the Terms and Conditions. 2. **RADIUS** The user has to provide a username and password, which is then redirected to a RADIUS server for authentication. If successful, the user is provided with data access. 3. **Local Guest Account** The user has to configure username and password on the device, which has to be provided on the redirection page for successful authentication and data access.	–	Clickthrough
Redirect Mode	Provision to configure the HTTP or HTTPS mode of redirection URL. 1. **HTTP** AP sends an HTTP POSTURL to the associated client, which will be http://<Pre-defined-URL>. 2. **HTTPS** AP sends an HTTPS POSTURL to the associated client, which will be https://<Pre-defined-URL>.	–	HTTP

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

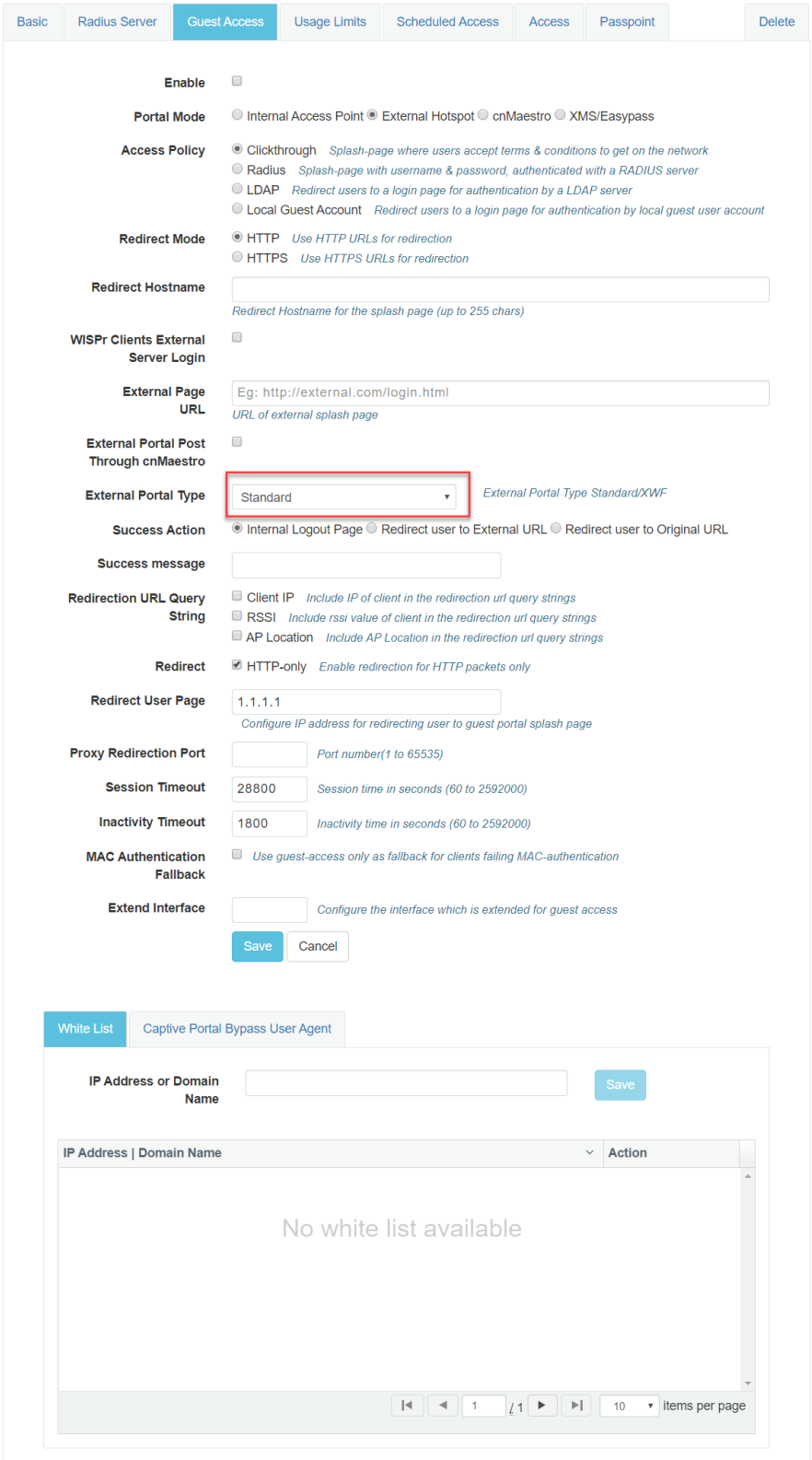
Parameters	Description	Range	Default
	This option is selected by default. The following information is appended in the redirection URL: ◦ SSID ◦ AP MAC ◦ NAS ID ◦ AP IP ◦ Client MAC • Redirection URL Users can provide either HTTP or HTTPS URLs.		
Redirection user to Original URL	Users will be redirected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

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

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

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

Figure 17: *The External Hotspot (Standard) parameter*



cnMaestro

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

Table 21: The cnMaestro parameters

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	Provision to configure the name of the Guest Access profile which is hosted on CnMaestro.	–	–
Redirect	• If enabled, only HTTP URLs will be redirected to the Guest Access login page. • If disabled, both HTTP and HTTPs URLs will be redirected to Guest Access login page.	–	Enabled
Redirect User Page	The IP address configured in this field is used as a logout URL for Guest Access sessions. The IP address configured should be not reachable to the internet.	–	1.1.1.1
Proxy Redirection Port	The proxy port can be configured with which proxy server is enabled. This allows URLs accessed with proxy port to be redirected to the login page.	1 - 65535	–
Inactivity Timeout	Provision to configure timeout period to disconnect wireless stations that are associated but have no data traffic. AP starts a timer when there is no data received from a wireless station and disconnects when the timer reaches zero.	60 - 2592000	1800
Whitelist	Provision to configure either IPs or URLs to bypass traffic, such that user can access those IPs or URLs without Guest Access authentication.	–	–

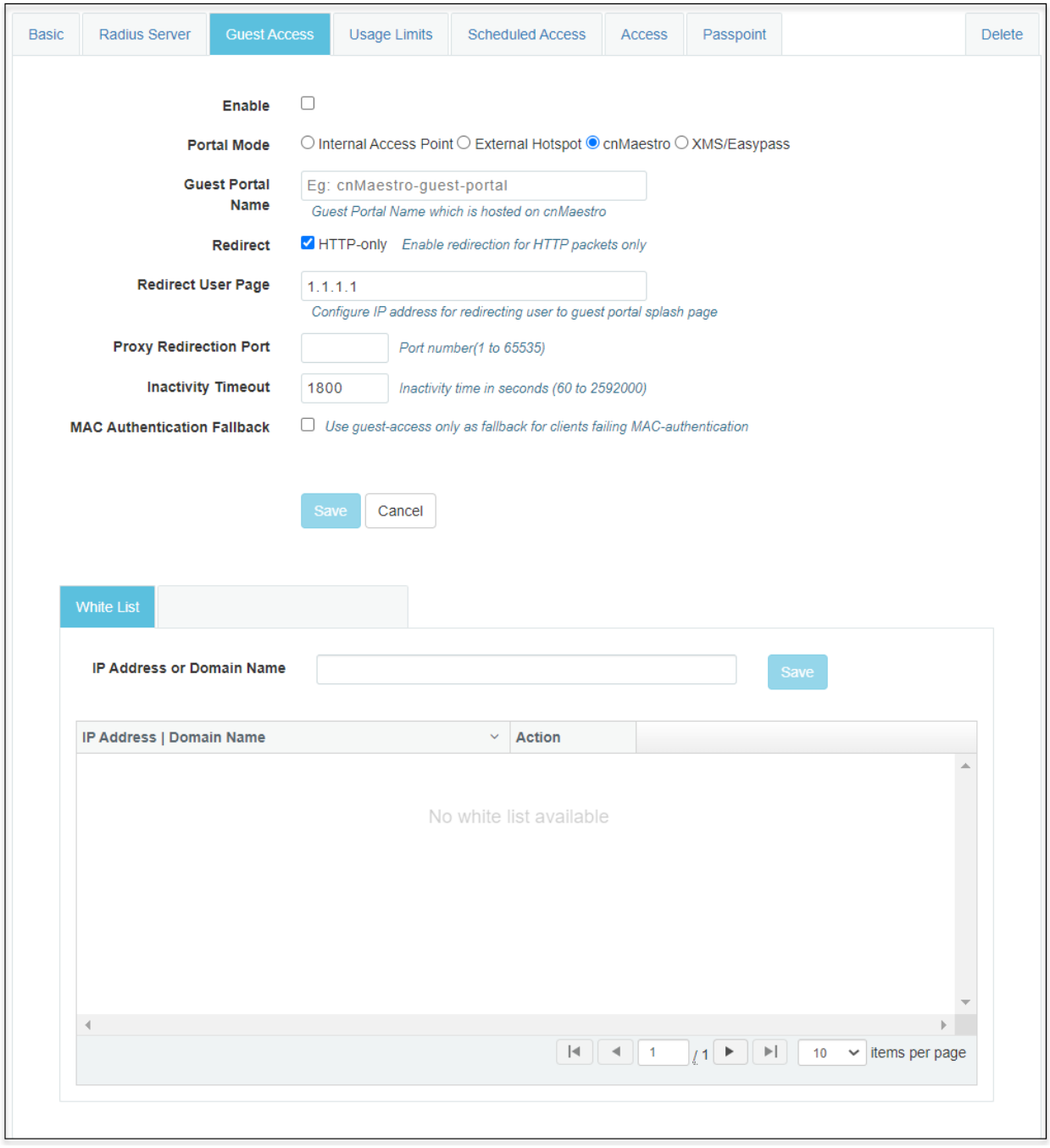
To configure the above parameters, navigate to the **Configure > WLAN > cnMaestro** tab and provide the details as given below:

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

To configure the **Whitelist parameter**:

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

Figure 18: *The cnMaestro parameter*



XMS/EasyPass

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

Table 22: XMS/EasyPass parameters

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

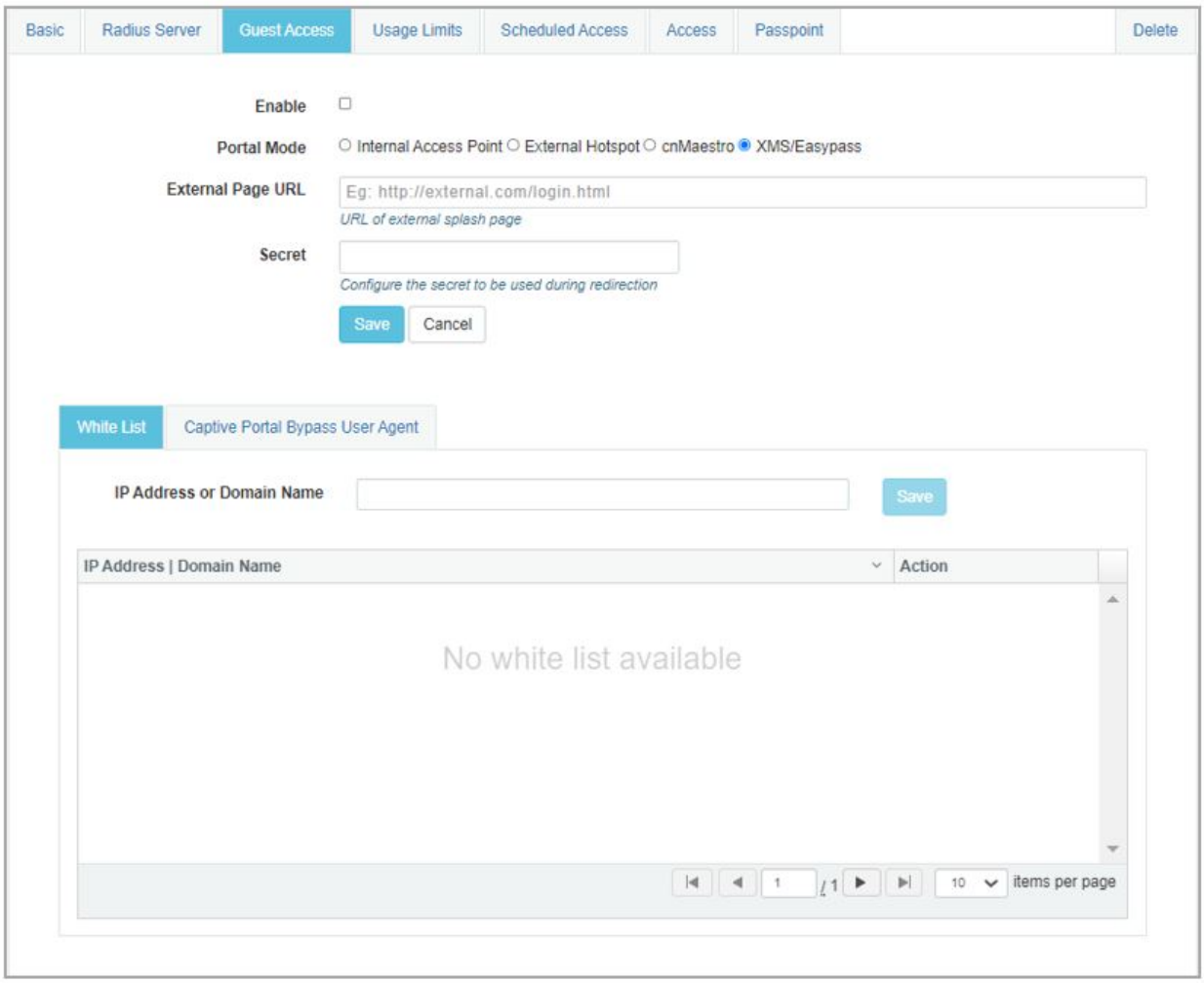
To configure the above parameters, navigate to the **Configure > WLAN > XMS/EasyPass** tab and provide the details as given below:

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

To configure the Whitelist parameter:

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

Figure 19: *XMS/EasyPass*



Note

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

Note

For more information about cnMaestro Guest Access Portal and onboarding, refer to the cnMaestro Guest Access portal.

Usage Limits

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

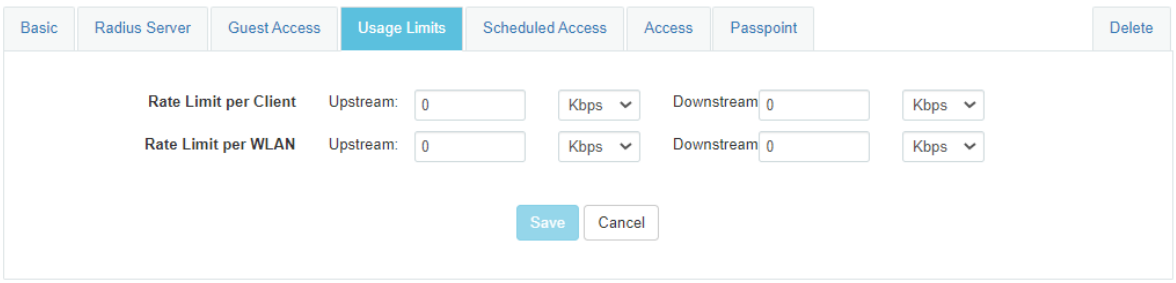
Table 23: Usage Limits parameters

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

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

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

Figure 20: *The Usage Limits parameters*



Scheduled Acess

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

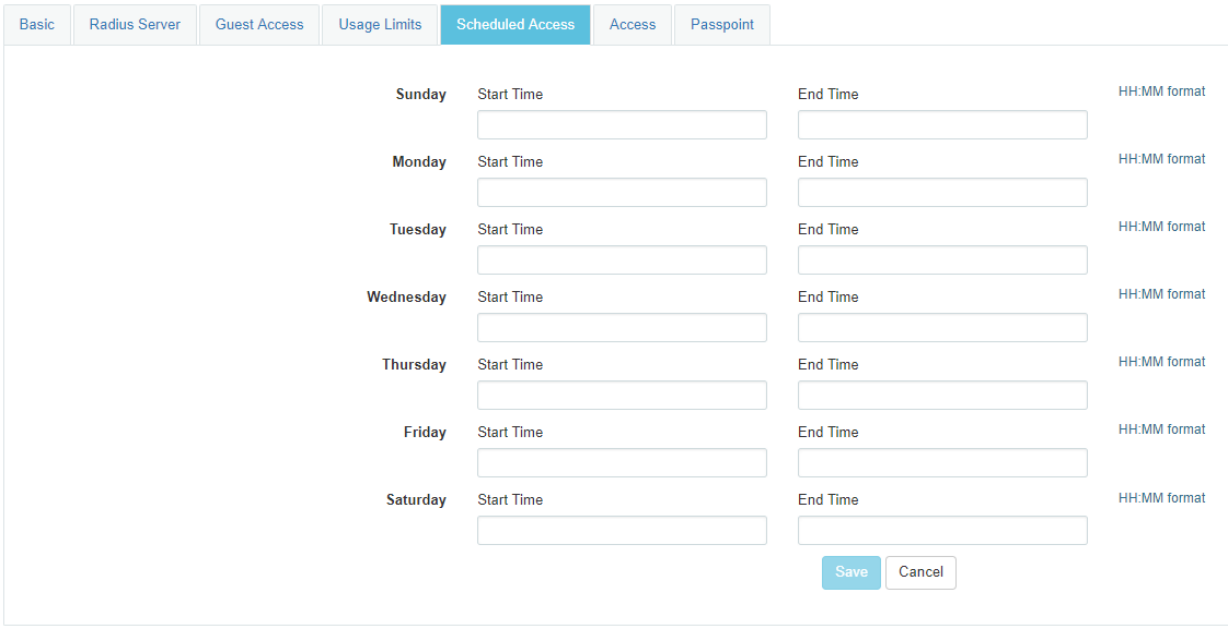
Table 24: The Scheduled Access parameters

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

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

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

Figure 21: *The Scheduled Access parameters*



CLI Configuration:

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

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



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

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

Access

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

Table 25: The Access parameters

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

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

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

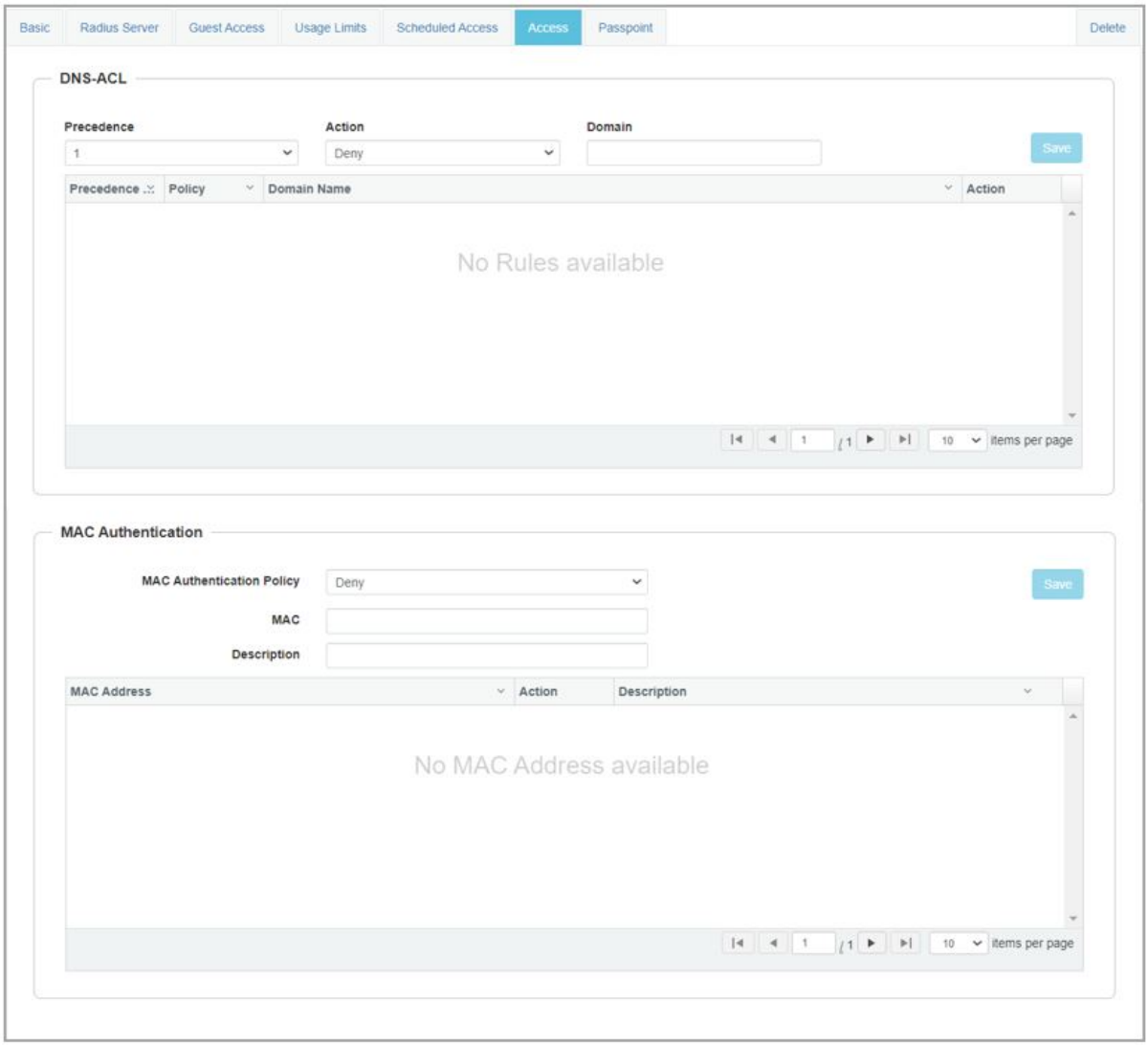
To configure **DNS ACL**:

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

To configure **MAC Authentication**:

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

Figure 22: *The Access parameters*



Passpoint

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

Table 26: Passpoint parameters

Parameters	Description	Range	Default
Configuration > Hotspot2.0 / Passpoint			
Enable	Passpoint (Release 2) enables secure hotspot network access, online sign-up, and policy provisioning.	–	Disabled
DGAF	Downstream Group Addressed Forwarding when enabled the WLAN does not transmit any multicast and broadcast packets.	–	Disabled
ANQP	ANQP domain identifier is included when the HS 2.0 indication	0-	0

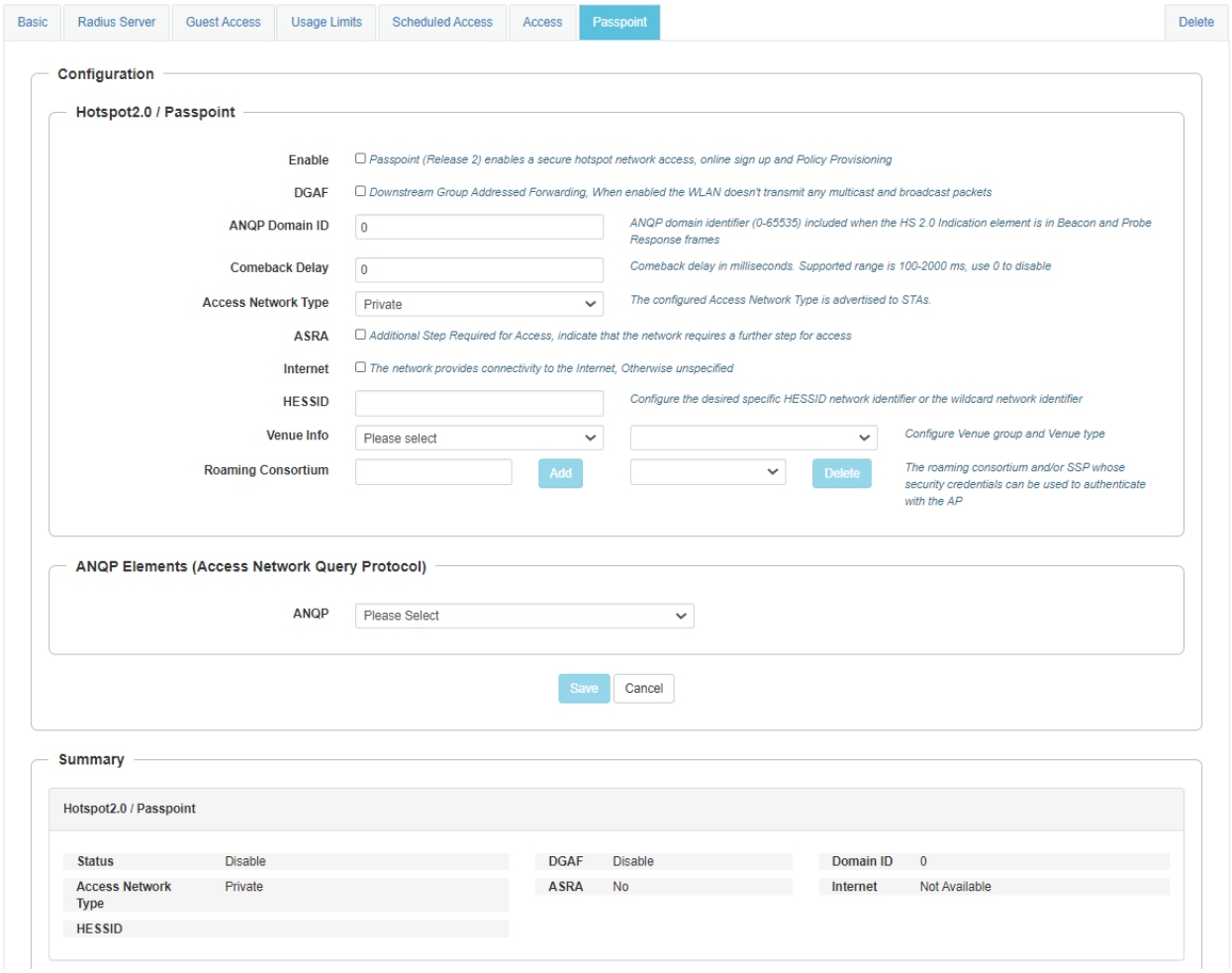
Parameters	Description	Range	Default
Domain ID	element is in Beacon and Probe Response frames.	65535	
Comeback Delay	Comeback Delay in milliseconds.	100-2000	0
Access Network Type	The configured Access Network Type is advertised to STAs. Following are the different network types supported: • Private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

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

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

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

Figure 23: *The Passpoint parameters*



Link Aggregation Control Protocol (LACP)

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

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 the 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	• Assign station to a user group • Re-assign station to a different user group (RFC 5176)
Standard	Framed-IP-Address	8	Session identification (RFC 5176)
Standard	Idle-Timeout	28	Specifies the amount of time a station may remain idle before its session is terminated
Standard	NAS-IP-Address	4	NAS identification (RFC 5176)
Standard	NAS-Identifier	32	NAS identification (RFC 5176)
Standard	Session-Timeout	27	Specifies the interval at which session is terminated
Standard	Termination-Action	29	Specifies the action to take when the session is terminated
Standard	Tunnel-Type	64	Dynamic VLAN assignment (1 of 3 required), should be set to VLAN (Integer = 13)
Standard	Tunnel-Medium-Type	65	Dynamic VLAN assignment (2 of 3 required), should be set to 802 (Integer = 6)
Standard	Tunnel-Private-Group-ID	81	Dynamic VLAN assignment (3 of 3 required), should be set to the VLAN ID or name
Standard	User-Name	1	• Station username update • Session identification (RFC 5176)
Microsoft Vendor-Specific	MS-MPPE-Send-Key	16	Session key distribution
Microsoft Vendor-Specific	MS-MPPE-Recv-Key	17	Session key distribution
Cambium Vendor-Specific	Cambium-Vlan-Pool-Id	157	Radius based VLAN pool
Nas Port ID	NAS-Port-Id	87	NAS identification (RFC 5176)

enhanced PSK (ePSK)

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

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

Note:

ePSK scale is a Premium feature where users can configure more than 300 ePSK (up to 1024 ePSK) per WLAN and it is controlled by cnMaestro X.

RADIUS based ePSK Premium feature

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

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

Note:

ePSK feature is not supported with WPA3.

Configuration CLI:

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

  RADIUS                : Configure RADIUS based ePSK
  username              : Configure Username



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

Chapter 7: Configuring the Network

This chapter describes the following topics

Overview

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

Configuring Network parameters

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

IPv4 network parameters

VLAN

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

Table 28: VLAN (IPv4) parameters

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

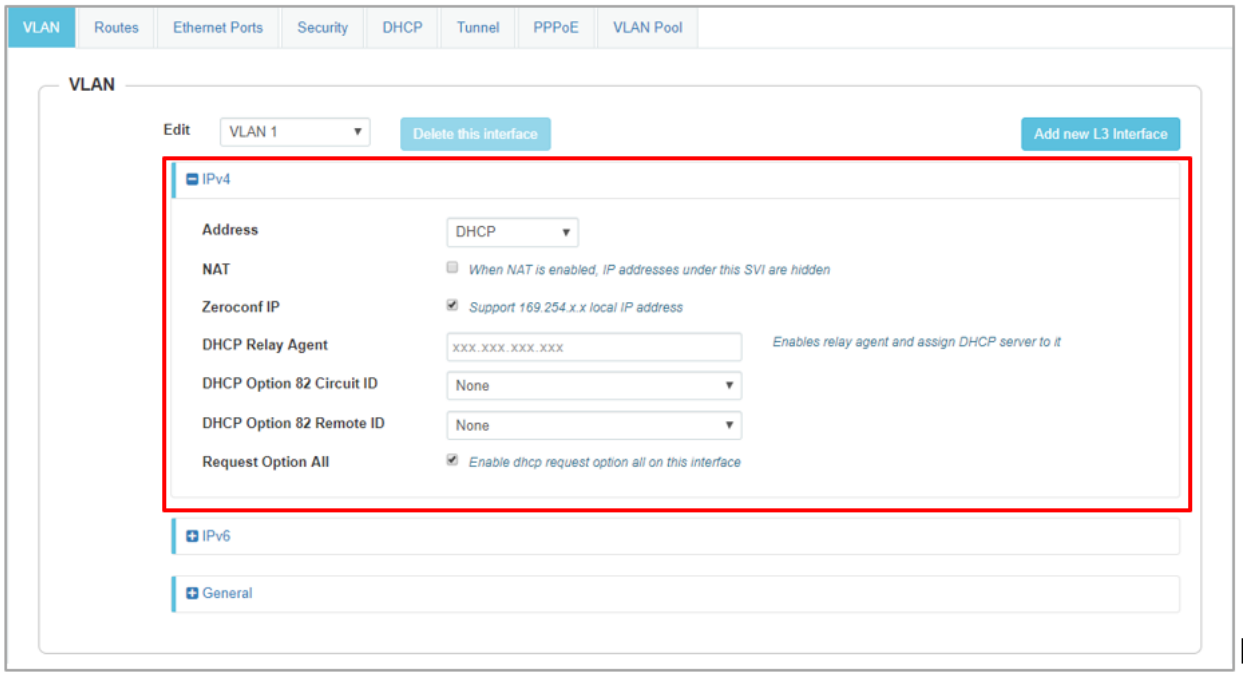
Parameters	Description	Range	Default
NAT	This option enables wireless traffic gets NAT'ed with APs respective uplink interface IP. This option is recommended when DHCP pools are configured in AP.	–	Disabled
Zeroconf IP	Zeroconf IP is recommended to be enabled. This interface is available only in the VLAN1 configuration section. If VLAN 1 is not allowed in Ethernet interfaces, this IP will not be accessible.	–	Enabled
Request Option All	This configuration decides the interface on which Enterprise Wi-Fi AP will learn the following: • IPv4 default gateway • DHCP client options like Option 43 and Option 15 (Controller discovery like controller host name / IPv4 address) • DNS Servers • Domain Name	–	Enabled on VLAN1

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

To configure VLAN IPv4:

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

Figure 24: *Network (IPv4)parameters*



DHCP Client Options

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

Table 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 the state of "Request Option All", the device chooses a subnet mask from the respective VLAN interface.	`show ip route`
Option 3	This option specifies a list of IP addresses for routers on the client's subnet.	Based on the state of "Request Option All", the device chooses a route learned from the respective VLAN interface. The only first route is honored.	`show ip route`
Option 6	The domain name server option specifies a list of Domain Name System (STD 13, RFC 1035) name servers available to the client. Servers SHOULD be listed in order of preference.	Based on the state of "Request Option All", the device chooses a subnet mask from the respective VLAN interface. the top two DNS servers are honored by Enterprise Wi-Fi AP devices.	`show ip name-server`

Options	Description	Usage	Reference CLI
Option 15	This option specifies the domain name that the client should use when resolving hostnames via the Domain Name System.	More details are provided in Option 15.	`show ip dhcp-client info`
Option 26	This option specifies MTU size in a network.	More details are provided in Configuring the Network.	`show ip dhcp-client info`
Option 28	This option specifies the broadcast address that the client should use.	A broadcast address learned for all VLAN interfaces are used respectively as per standards	`show ip dhcp-client-info`
Option 43	This option is used to help the AP in obtaining the cnMaestro IP address from the DHCP server while a DHCP request to get an IP address is sent to the DHCP server.	More details are provided in Option 43 (cnMaestro On-Premises 2.4.0 User Guide).	`show ip dhcp-client info`
Option 51	This option is used in a client request to allow the client to request a lease time for the IP address. In a server reply, a DHCP server uses this option to specify the lease time it is willing to offer.	Enterprise Wi-Fi AP renew leases for all VLAN interfaces configured based on lease time that has been learned from the DHCP server.	`show ip dhcp-client info`
Option 54	DHCP clients use the contents of the **server identifier** field as the destination address for any DHCP messages unicast to the DHCP server.	Enterprise Wi-Fi AP learns DHCP server IP for all VLAN interfaces configured.	`show ip dhcp-client info`
Option 60	This option is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.	For Enterprise Wi-Fi AP device, value is updated as Cambium-Wi-Fi-AP.	`show ip dhcp-client info`

DHCP Option 43 - Zero-touch onboarding

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

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

DHCP Option 43 format

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

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

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

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

Note

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

Routing and DNS

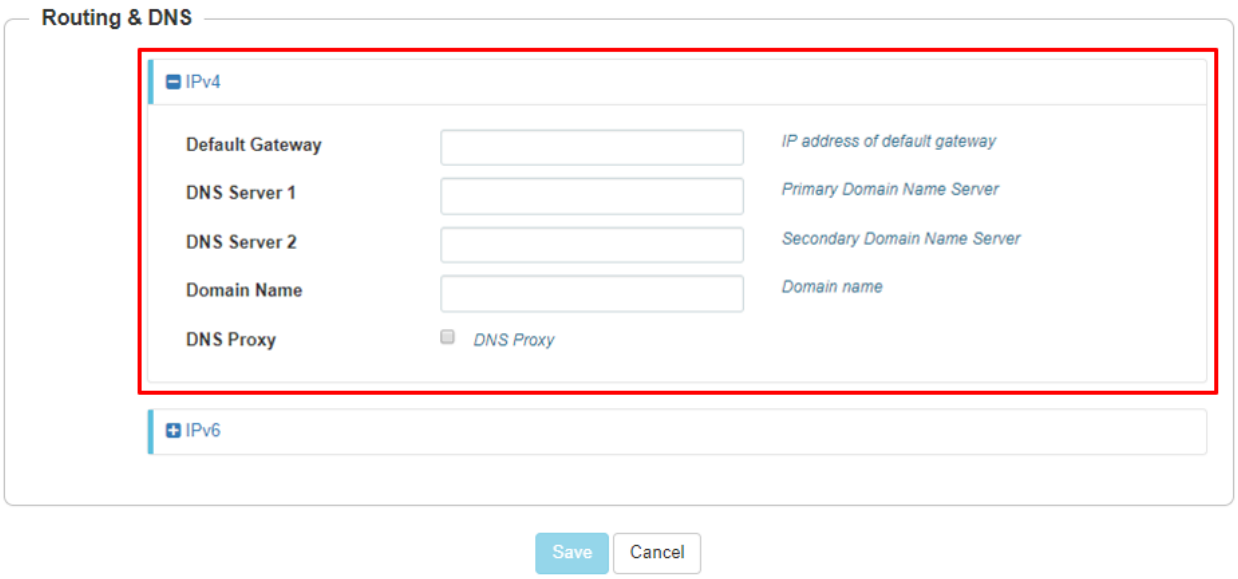
Table 30: Configure: Network > VLAN > Routing & DNS > IPv4 parameters

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

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

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

Figure 25: *Routing & DNS (IPv4) parameters*



Routes

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

Table 31: Routes (IPv4) parameters

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

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

To configure Gateway Source Precedence:

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

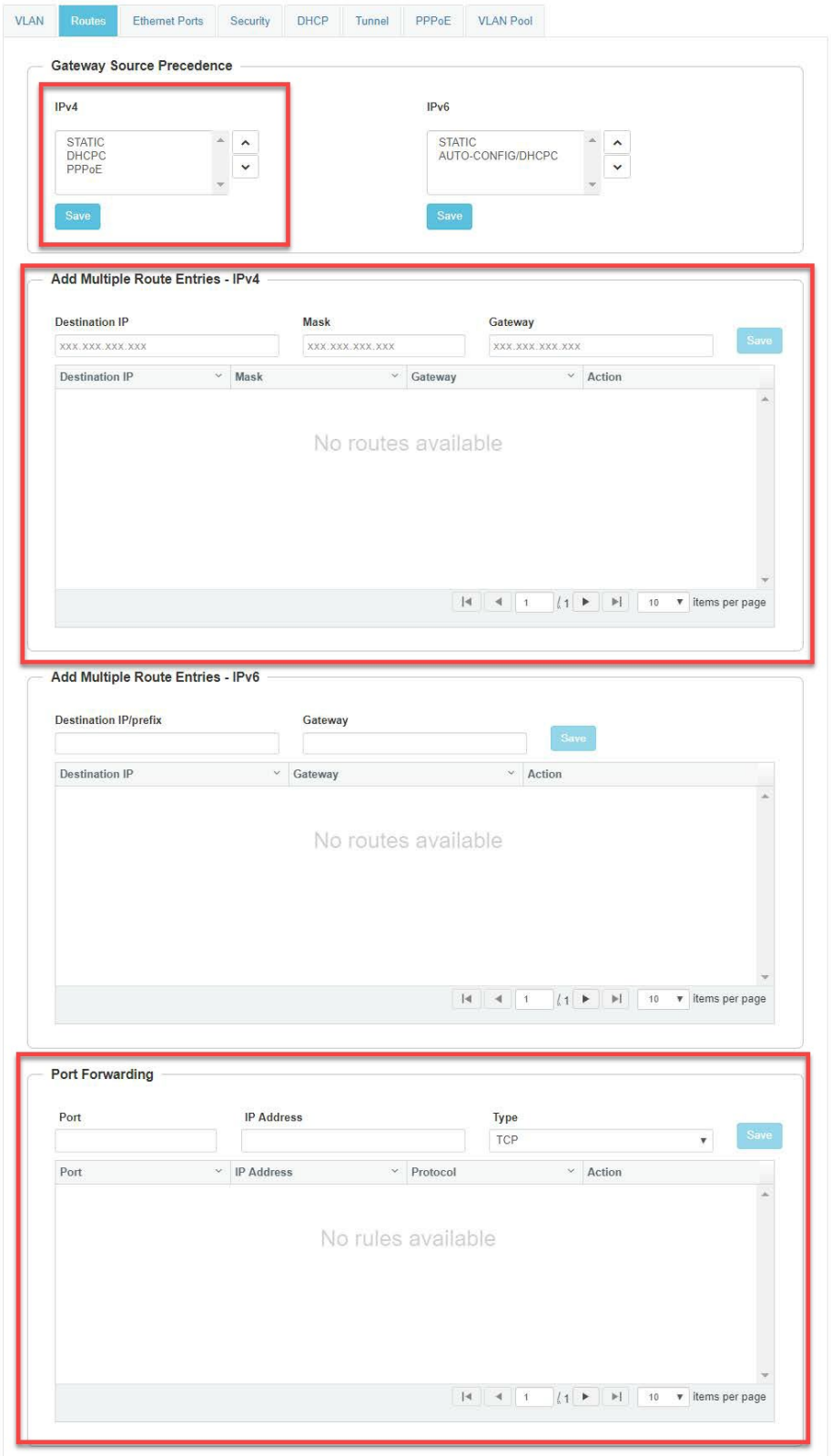
To configure Add Multiple Route Entries:

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 26: *Routes (IPv4) parameters*



IPv6 network parameters

VLAN

Table 32: VLAN (IPv6) parameters

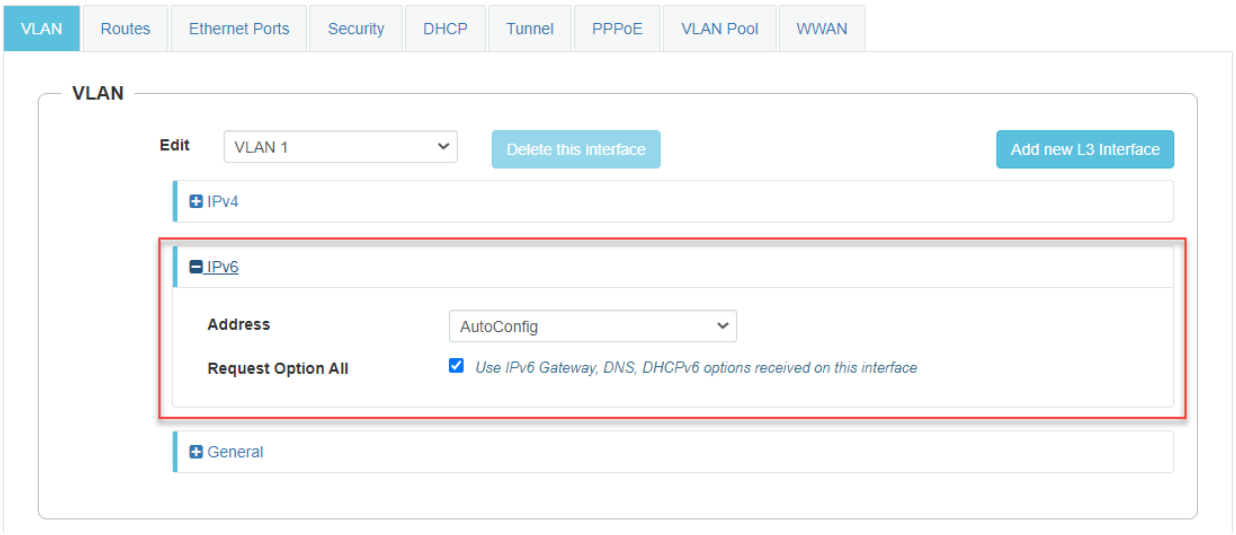
Parameters	Description	Range	Default
Address	Provision to configure the mode of IPv6 address configuration for an interface selected. Five modes are supported: • Disabled • AutoConfig • Static • Stateless DHCPv6 • Stateful DHCpv6	–	AutoConfig
Request Option All	This configuration decides the interface on which AP will learn the following: • IPv6 default gateway • DHCP client options like Option 52 and Option 24 (Controller discovery like controller hostname / IPv6 address) • DNS Servers • Domain Name	–	Enabled on VLAN1

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

To configure **VLAN IPv6**:

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

Figure 27: *Configure: Network > VLAN > IPv6 parameters*



Routing & DNS

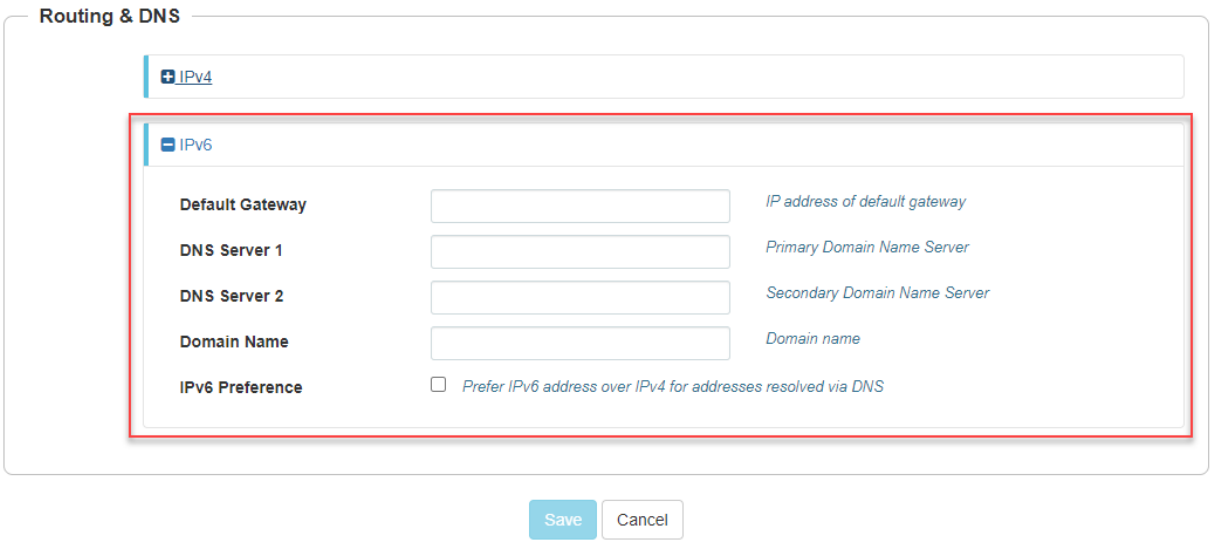
Table 33: Routing & DNS (IPv6) parameters

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

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

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

Figure 28: *Routing & DNS (Pv6) parameters*



Routes

Table 34: Routes (IPv6) parameters

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

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

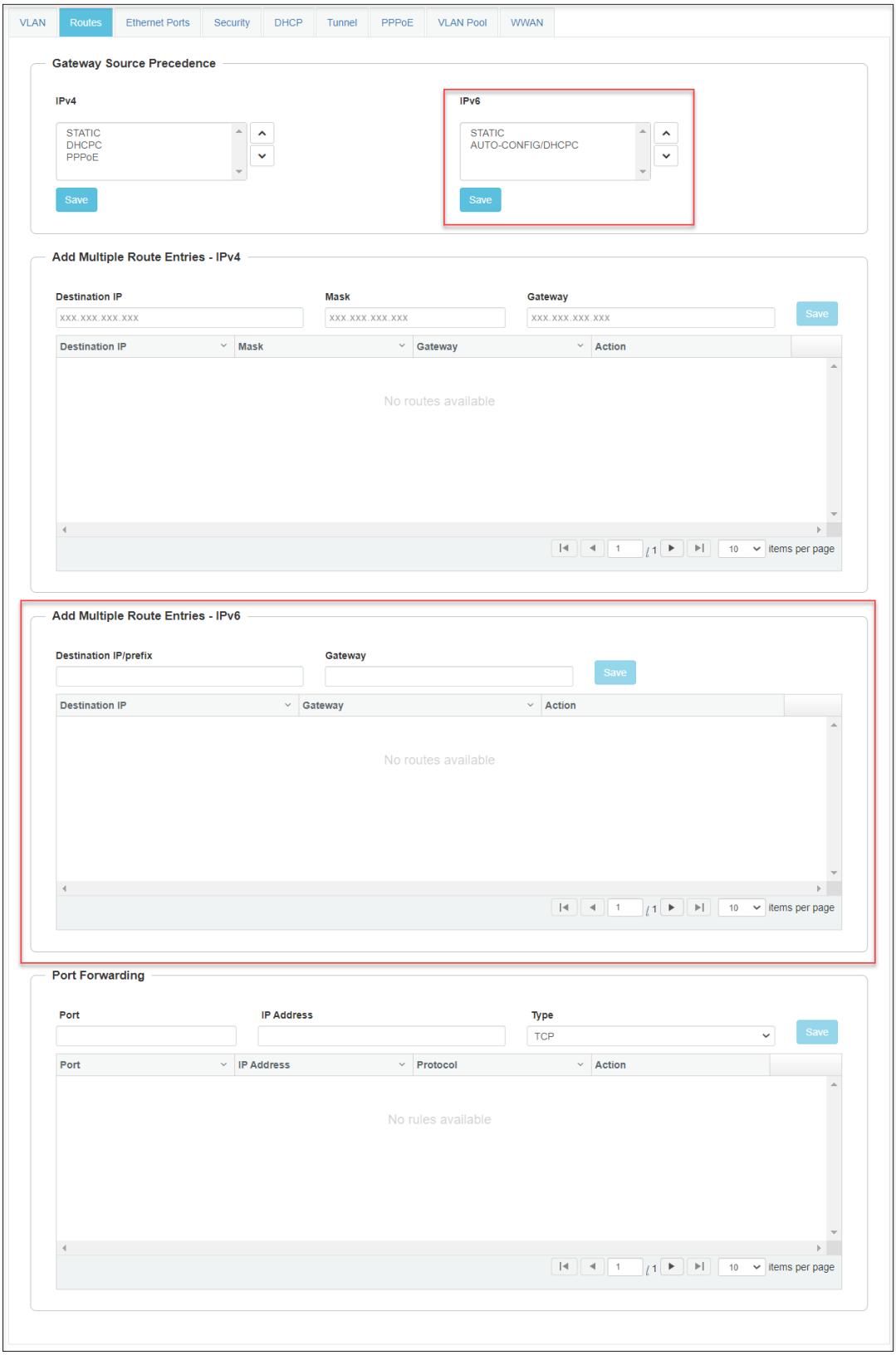
To configure **Gateway Source Precedence**:

1. Select STATIC or AUTO-CONFIG/DHCPC from the **Gateway Source Precedence** 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 29: *Routes (IPv6) parameters*



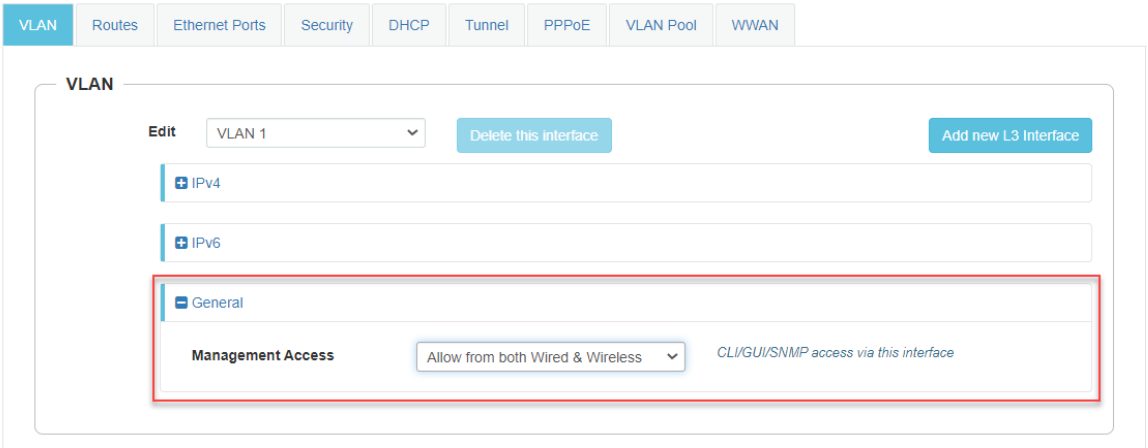
General network parameters

Table 35: VLAN (General) parameters

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

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

Figure 30: *VLAN (General) parameters*



Ethernet Ports

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

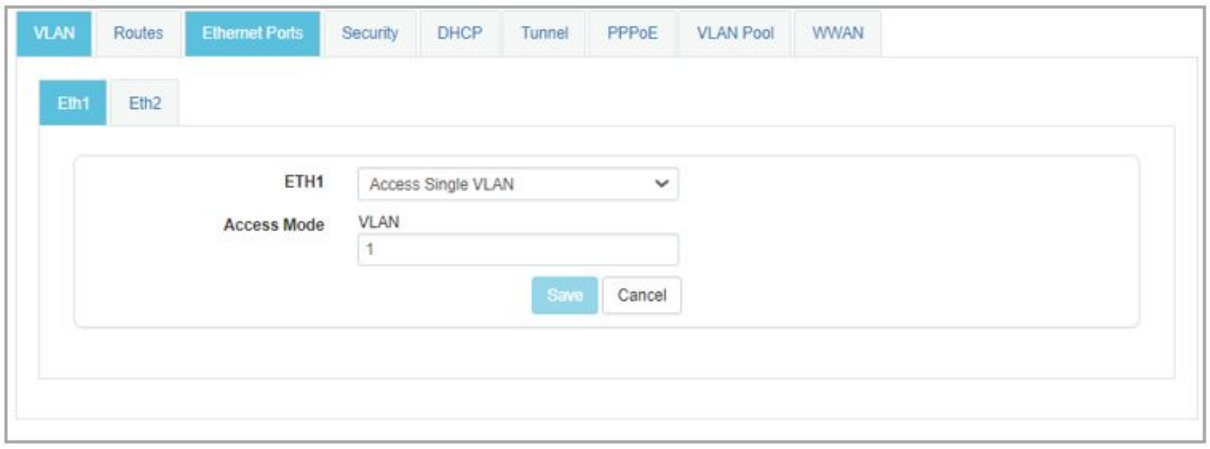
Table 36: Ethernet Ports parameters

Parameters	Description	Range	Default
Ethernet	Enterprise Wi-Fi AP devices Ethernet port is provisioned to operate in the following modes: 1. Access Single VLAN Single VLAN traffic is allowed in this mode. 2. Trunk Multiple VLANs Multiple VLANs are supported in this mode.	–	Access 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 31: *Ethernet Ports parameters*



General network parameters

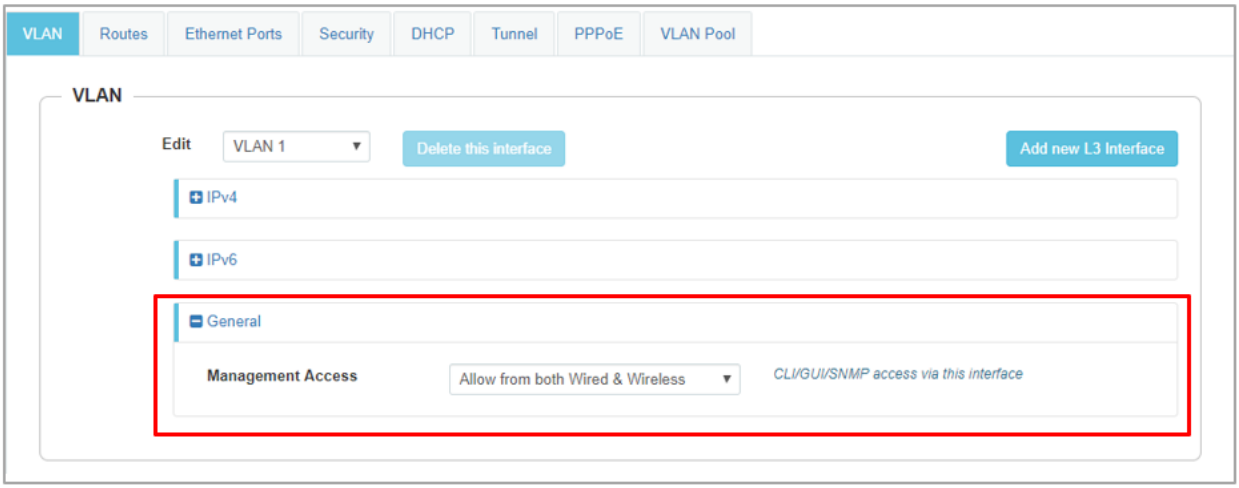
Below table lists the fields that are displayed in **Configure >Network > VLAN > General parameters** tab:

Table 37: The General parameters

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

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

Figure 32: *The General parameters*



Security

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

Table 38: Security parameters

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

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

Figure 33: *Security parameters*

DHCP

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

Table 39: DHCP parameters

Parameters	Description	Range	Default
Edit	Provision to select DHCP Pool if multiple Pools are defined on Enterprise Wi-Fi AP device.	–	–
Address Range	Users can configure start and end addresses for a DHCP Pool selected from the drop-down box.	–	–
Default Router	Provision to configure next hop for a DHCP pool selected from the drop-down box.	–	–
Domain Name	Provision to configure the domain name for a DHCP pool selected from the drop-down box.	–	–
DNS Address	Provision to configure DNS server for a DHCP pool selected from the drop-down box.	–	–
Network	Provision to configure Network ID for a DHCP pool selected from the drop-down box.	–	–
Lease	Provision to configure lease for a DHCP pool selected from the drop-down box.	–	–
Add Bind List			
	For every DHCP pool configured, the user can bind MAC and IP from the address pool defined, so that the wireless station gets the same IP address every time they connect. Following parameters are required to bind IP address: • MAC Address • IP Address	–	–

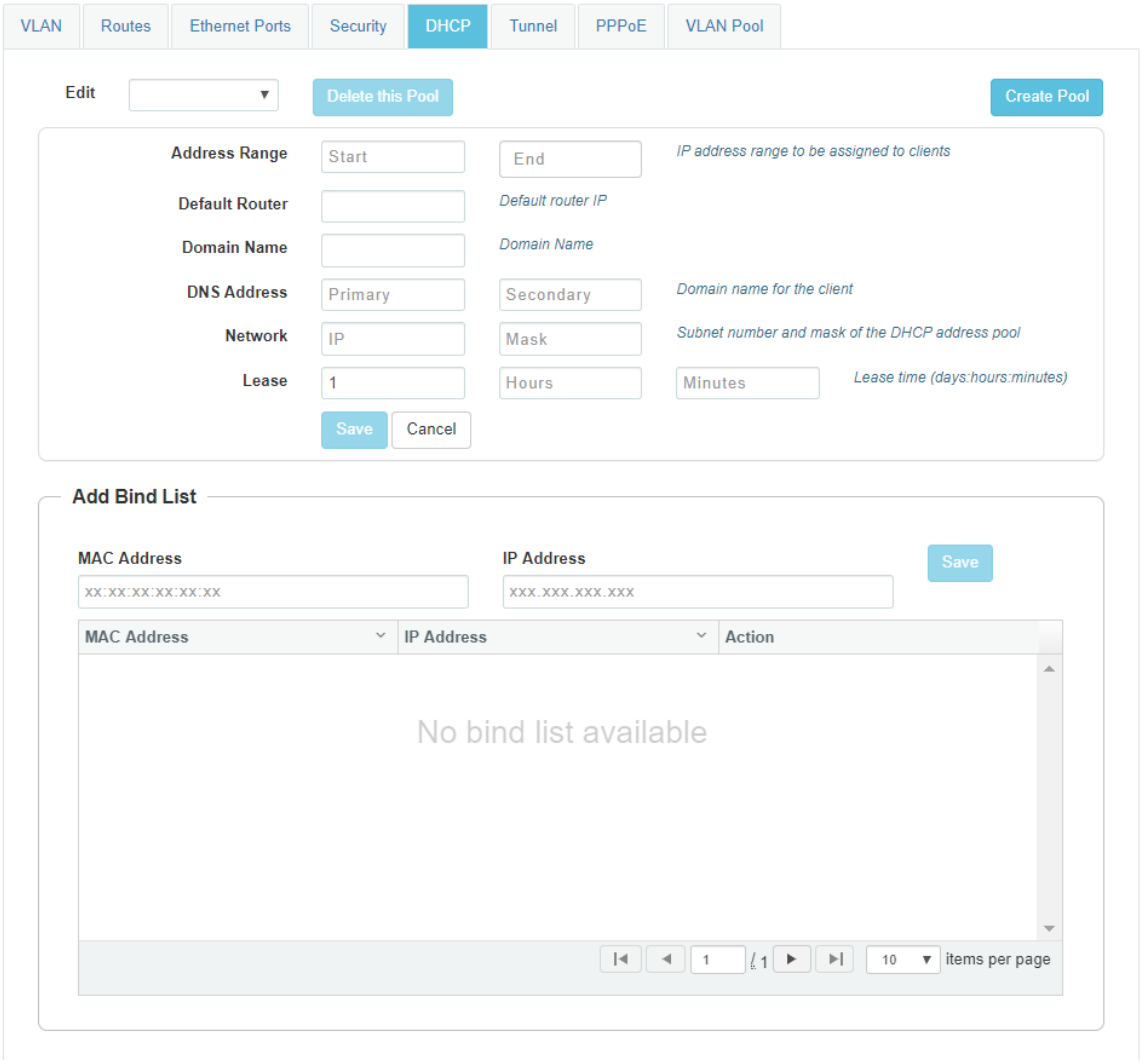
To configure the above parameter, navigate to the **Configure > Network > DHCP** tab and provide the details as given below:

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

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

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

Figure 34: *DHCP parameters*



Tunnel

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

Table 40: The Tunnel parameters

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

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

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

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

To configure **L2TP**:

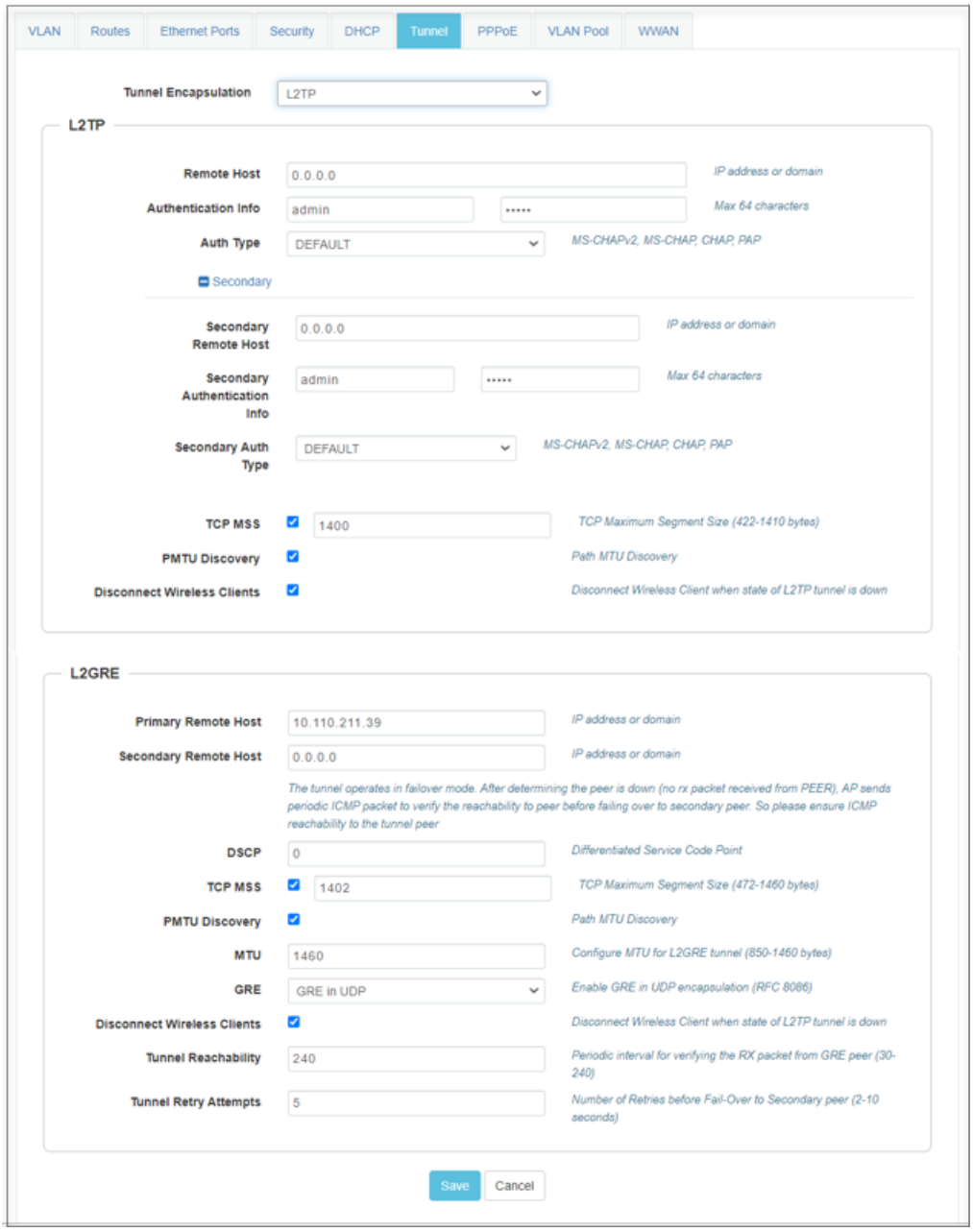
2. Enter IP address or domain name in the **Remote Host** text box.
3. Enter credentials required for L2TP authentication in the **Authentication Info** text box.
4. Select authentication type from the **Auth Type** drop-down list.
5. Enter IP address or domain name in the **Secondary Remote Host** text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

7. Select authentication type from the **Secondary Auth Type** drop-down list.
8. Enter TCP Maximum Segment Size in the **TCP MSS** text box.
9. Enable **PMTU Discovery** check box.
10. Enable **Disconnect Wireless Clients** check box.
11. Click **Save**.

To configure **L2GRE**:

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

Figure 35: *The Tunnel parameters*



Point-to-Point Protocol over Ethernet (PPPoE)

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

Table 41: PPPoE parameters

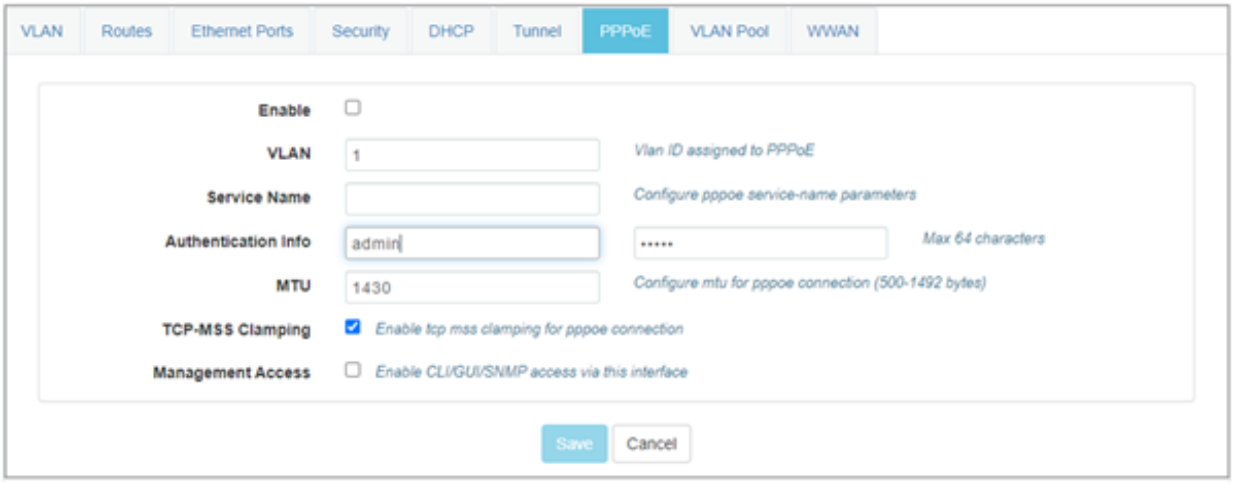
Parameters	Description	Range	Default
Enable	Provision to enable PPPoE client.	–	Disabled

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

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

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

Figure 36: *PPPoE parameters*



VLAN Pool

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

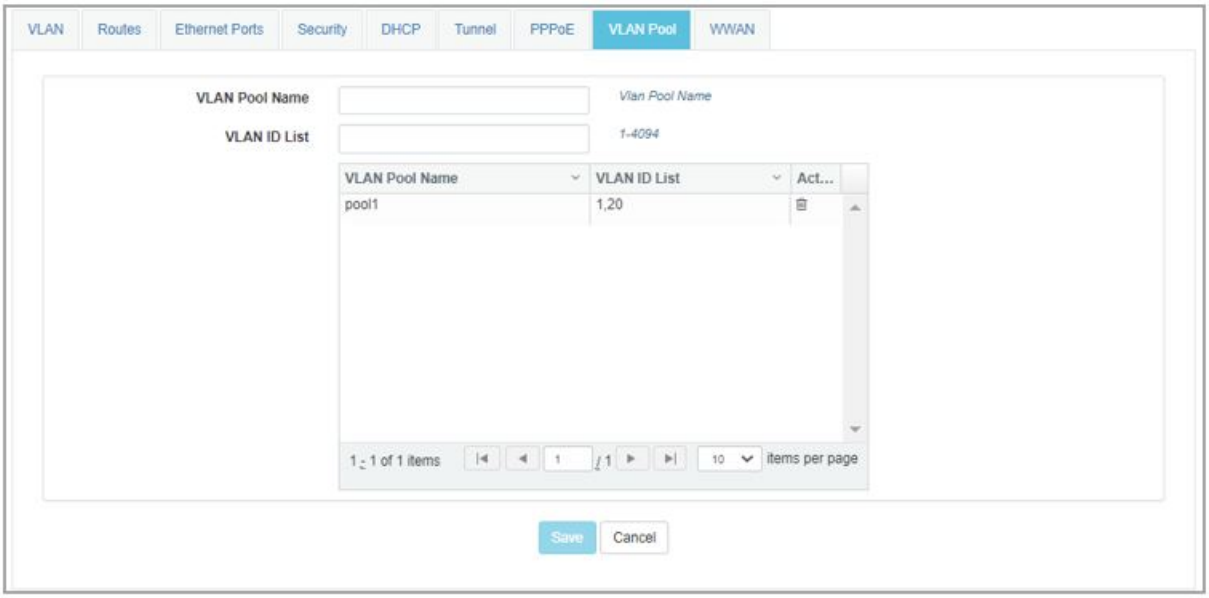
Table 42: The VLAN Pool parameters

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

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

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

Figure 37: *The VLAN Pool parameters*



Chapter 8: Filter Management

This chapter describes the following topics:

Overview

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

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

Filter list

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

Filters

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

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

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

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

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

Configuring filter CLI

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

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

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

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

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

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

  air-cleaner           : Configure Preset air cleaner filters
  application-control   : Enable application control
  clear                 : Clear command
  disable               : Disable filter list
  filter                : Configure filter rules in precedence order
  stateful              : Enable stateful filtering


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

   - **Stateful filtering** 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

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

5. Layer 3 filter has the below provisions.

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

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

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

Note:

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

Note

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

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

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

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

9. Layer 2 filter has below options:

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

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

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

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

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

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

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

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

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

Example:

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

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

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

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

Example:

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

Sample configuration

```
filter  global-filter
  stateful
  application-control

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

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

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

14. To show filter statistics:

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

  Filter ID | global
```

Air Cleaner

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

Configuration CLI:

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

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

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

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

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

Note

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

Application control Premium feature

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

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

Deep Packet Inspection (DPI)

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

Application control policy

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

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

Risk and productivity

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

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

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

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

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

Selection criteria

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

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

```
XV3-8-441BCC(config)# show application-statistics by-application
Applications Count = 24
Application Statistics for All Applications
================================================================================
Protocol or              Productivity       TX          TX          RX          RX
Application              Index & Risk     Packets       Bytes     Packets       Bytes
--------------------------------------------------------------------------------
 Ad Analytics              4    1         4             220         3             231
 Amazon                    2    1         75            31437       69            8337
 Bonjour                   4    1         15            1737        14            1664
 Doubleclick               1    1         84            30190       65            12228
 Google Ads                3    1         103           47136       78            12223
 Google Analytics          4    1         13            3750        15            1711
 Google APIs               3    1         4713          6288091     892           153251
 Google                    3    1         2544          3248915     568           48664
 Google Play               3    1         350           396456      181           15261
 Mozilla                   3    1         54            44708       48            5854
 NetBIOS NS                1    3         0             0           12            936
 NTP                       1    3         2             152         2             152
 OCSP                      3    1         63            6404        71            5247
 OpenX                     1    1         32            8374        27            3507
 Quantcast                 1    1         14            4733        17            2341
 Rapleaf                   3    1         19            6745        19            2288
 Reddit                    3    1         1227          1477596     752           74695
 Scorecard Research        1    1         26            5876        27            2748
 SSDP                      4    1         329           146086      20            4000
 SSL                       3    3         226           136435      176           22509
 TCP                       3    1         2376          1617471     1665          330377
 Twitter                   3    4         79            53301       68            7532
 Wikipedia                 3    3         19            3126        28            3873
 YouTube                   1    4         95            26393       99            12233
```

```
XV3-8-441BCC(config)# show application-statistics by-category
Application Categroy  Statistics for All Applications
================================================================================
Application              Productivity       TX          TX          RX          RX
category                 Index & Risk     Packets       Bytes     Packets       Bytes
--------------------------------------------------------------------------------
 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)#
```

- **SSID**: This gives the application list seen on a 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              Productivity       TX          TX          RX          RX
Application              Index & Risk     Packets       Bytes     Packets       Bytes
--------------------------------------------------------------------------------
 Ad Analytics              4    1        4             220          3            231
 Amazon                    2    1        75            31437        69           8337
 Bonjour                   4    1        0             0            15           1810
 Doubleclick               1    1        84            30190        65           12228
 Google Ads                3    1        103           47136        78           12223
 Google Analytics          4    1        13            3750         15           1711
 Google APIs               3    1        4713          6288091      892          153251
 Google                    3    1        2544          3248915      568          48664
 Google Play               3    1        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 wants to check for statistics.

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

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

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

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

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

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


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

VLAN         STA_COUNT
 1              1
```

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

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

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

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

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

DPI CLI configuration

Users can enable Application Control globally by using the 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
  abscbn                : ABS-CBN
  acas                  : ACA Services
  accweath              : accuweather.com
XV3-8-441BCC(config-global-filter-precedence-1)# application-control youtube

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


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

  permit                : Allow this Application
```

Set per category policy

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

CLI Configuration

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

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

Chapter 9: Configuration - Services

This chapter describes the following topics:

Overview

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

Configuring services

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

User Groups **Premium feature**

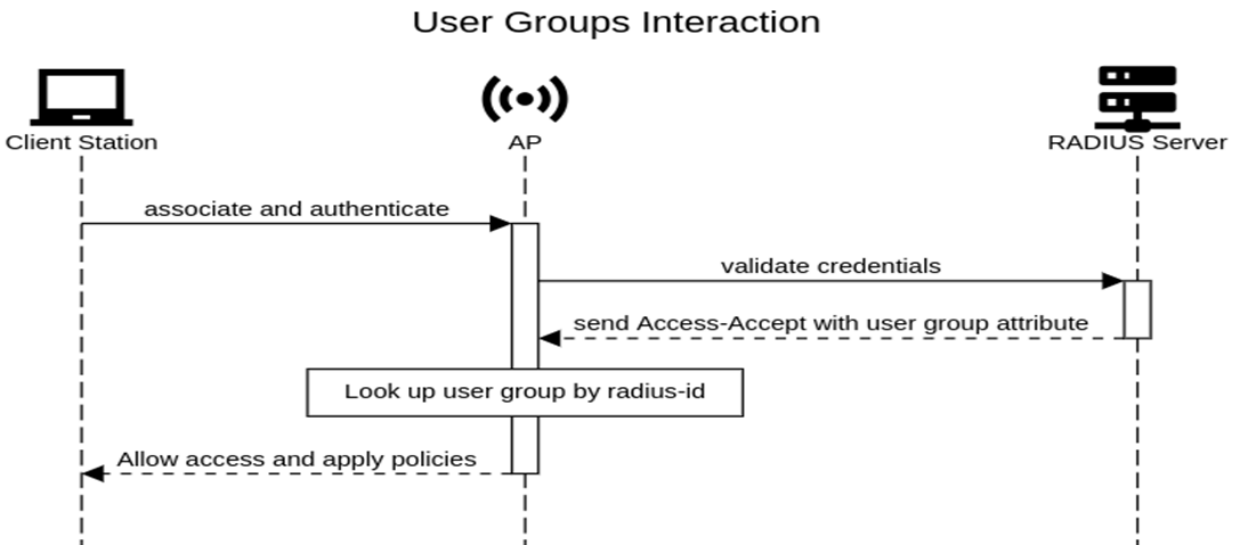
Some policies, like VLAN, require many RADIUS attributes to be sent by the RADIUS server and processed by the AP. Some wireless network administrators do not have administrative access to the RADIUS server, so making changes to wireless policies would require waiting for the RADIUS administrator to make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

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

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

The User Group feature is natively supported by XMS Cloud.

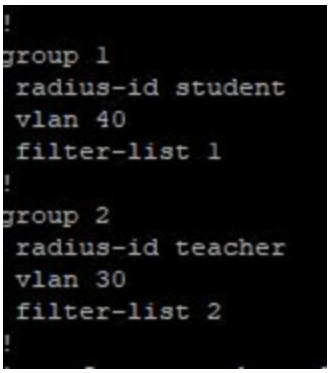
Figure 38: *User Groups interaction*



CLI Configuration:

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

  Specify user group number <1-16>



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

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


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

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

Example:



User group properties and actions

A user group supports the following properties and actions:

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

User group policies

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

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

Location API

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

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

Table 43: Location API parameters

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

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

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

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

Figure 39: *Location API parameters*

Note

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

Speed Test

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

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

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

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

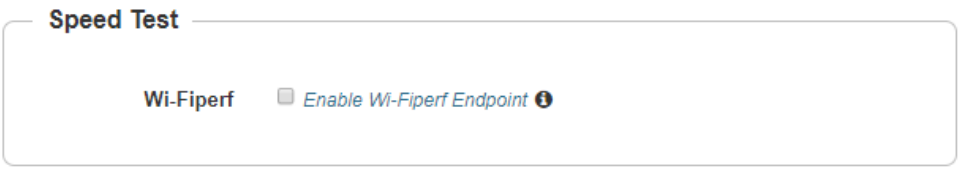
Table 44 lists the fields that are displayed in the **Configuration > Services > Speed Test** tab.

Table 44: 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 40: *Speed Test parameters*



BT location API

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

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

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

Table 45: BT Location API parameters

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

Sending report

After enabling BLE Scanning on AP it will start processing:

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

To configure the BT Location-API in the CLI:

```
XV3-8-EC7708(config)# location-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. (0xfe1f)\n',
'bt_timestamp': u' 1.811127'
}
```

Bonjour Gateway

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

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

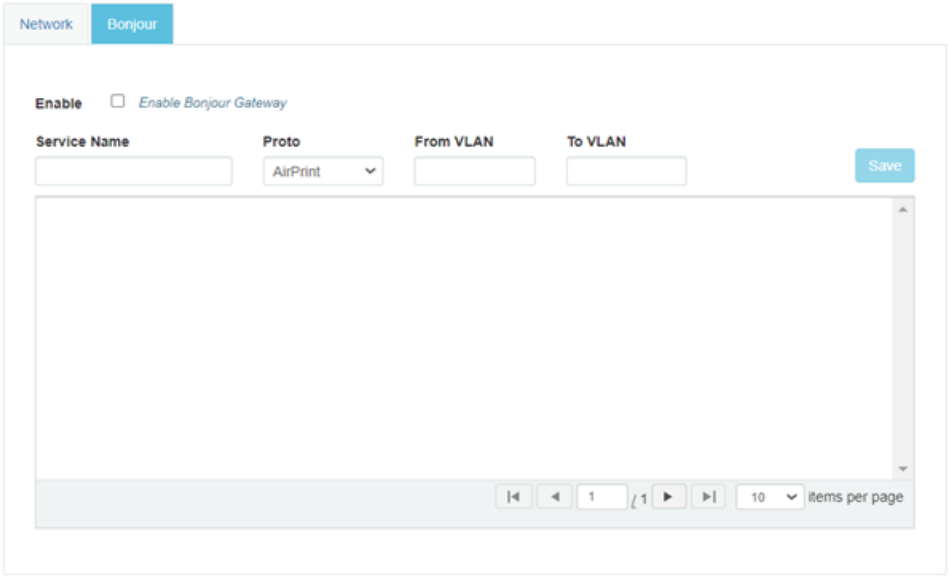
Table 47: Bonjour Gateway parameters

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

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

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

Figure 41: *Bonjour parameter*



CLI Configuration:

1. Enable Bonjour Gateway on AP.

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

2. To configure Bonjour rule.

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

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

3. To control mDNS repeated packet to WAN side.

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

  all                 : Forward all bonjour mdns packets queries and response repeated with vlan to WAN side
  queries             : Forward bonjour mdns Query packets repeated with vlan to WAN side
  responses           : Forward bonjour mdns Response packets repeated with vlan to WAN side
```

Note

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

Link Aggregation Control Protocol (LACP)

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

LACP provides the following benefits:

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

Configuration:

To Add ethernet to port channels:

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

Port-channel configuration:

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

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


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

Syntax:

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

Real Time Location System (RTLS)

Stanley AeroScout Location Engine **Premium feature**

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

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

CLI Configuration:

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

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

Chapter 10: Operations

This chapter describes the following topics:

Overview

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

Firmware upgrade

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

Note

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

Warning

Platform: e410, e510, e430, e600 and e700

- Firmware upgrade should be in HTTTP 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: Firmware update parameters

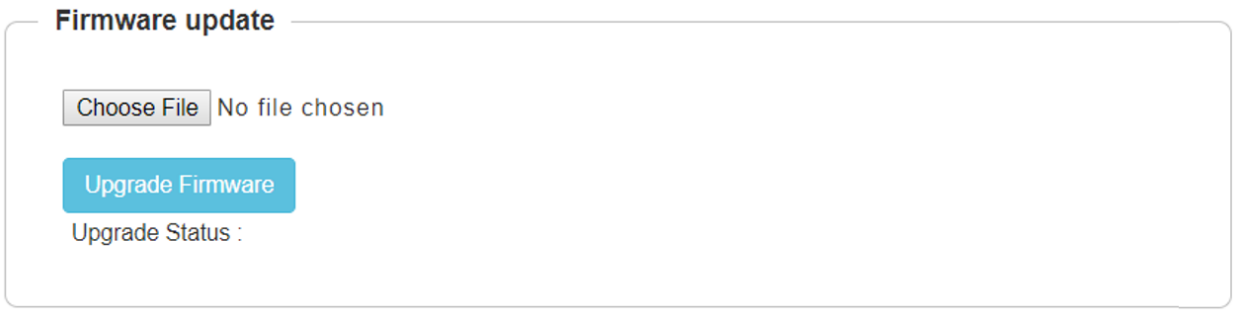
Parameters	Description	Range	Default
Choose File	Provisions to select upgrade files.	–	–
Upgrade Firmware	Provision to initiate upgrade once the file is selected.	–	–

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

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

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

Figure 42: *Firmware update parameters*



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:

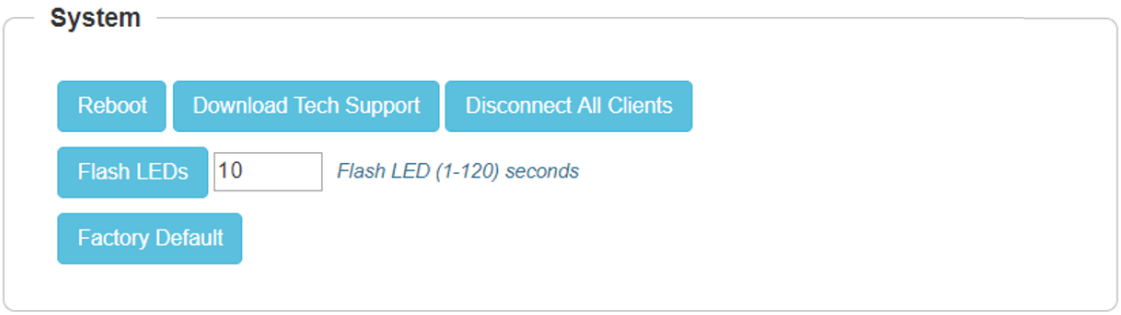
Table 49: System parameters

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

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

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

Figure 43: *System parameters*



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.

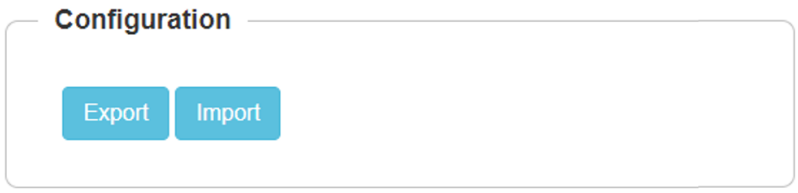
Figure 44: *Configuration parameters*

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

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

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

Figure 45: *Configuration parameters*



Chapter 11: Troubleshoot

Overview

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

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

Logging

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

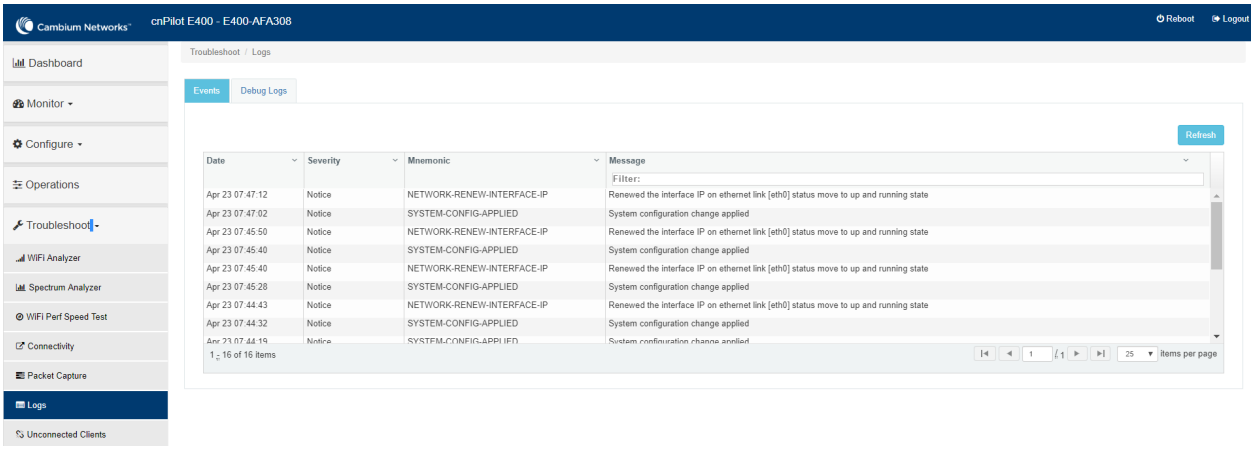
Events

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

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

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

Figure 46: *Troubleshoot > Logs > Events*

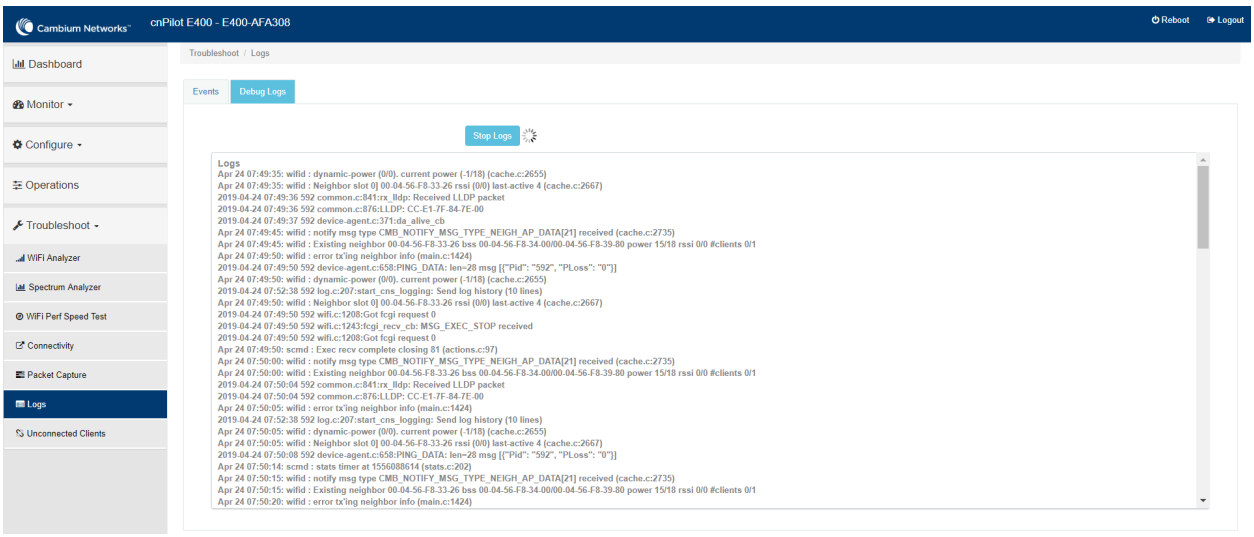


Debug Logs

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 the user clicks **Start Logs** and can be terminated when clicked on Stop Logs. By default, debug logs auto terminate after 1 minute when clicked on Start Logs.

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

Figure 47: *Troubleshoot > Logs > Debug Logs*



Radio Frequency (RF)

Wi-Fi Analyzer

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

- Interference

This tool shares more information about each channel as below:

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

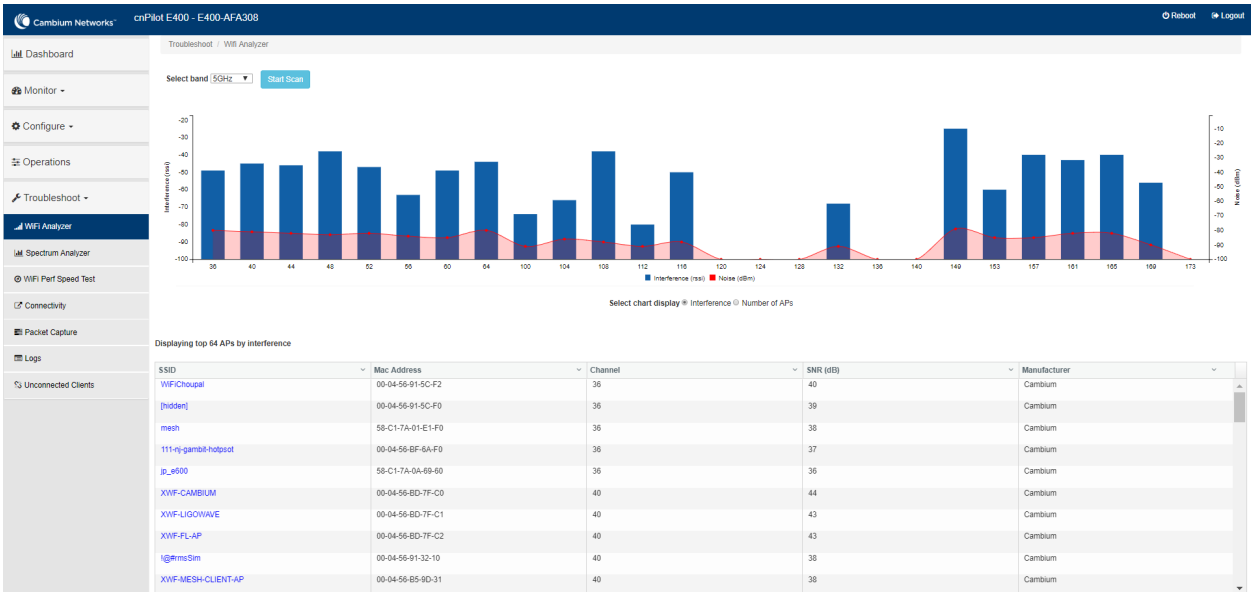
- Number of APs

This tool shares more information about each channel as below:

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

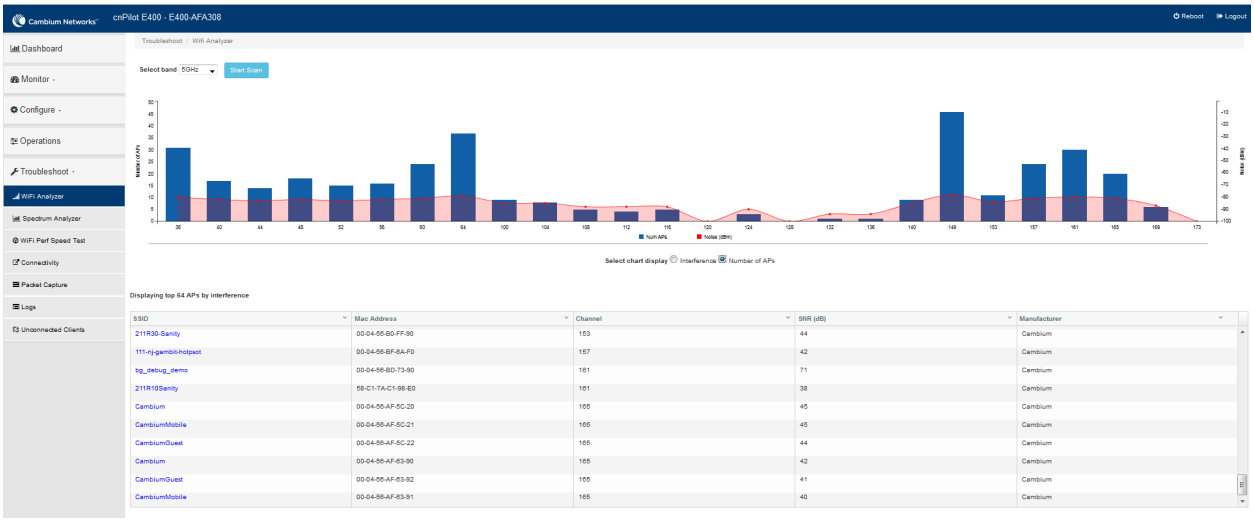
Channel analyzer is available at **Troubleshoot > Wi-Fi Analyzer > Interference Mode**.

Figure 48: *Interference Mode*



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

Figure 49: *Troubleshoot > Wi-Fi Analyzer > Number of APs Mode*



Packet capture

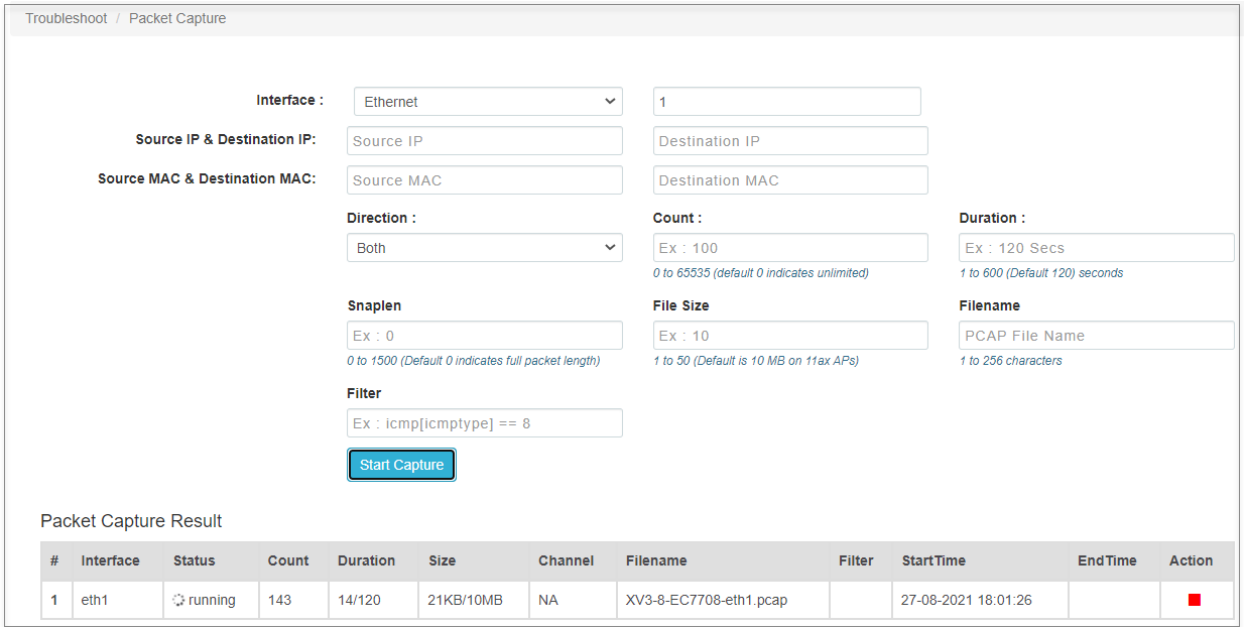
Allows the administrator to capture packets from the APs UI, cnMaestro UI, or XMS-Cloud. The administrator can filter the packets being captured by specifying a particular MAC address, IP address, and port number. The user can trigger packet capture on one or more interfaces, simultaneously view the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

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

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

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

Figure 50: *Packet Capture page*



Performance

Speedtest on Access Point

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

Configuration:

Syntax:

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

  <server url> <download MB> <upload MB>


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

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

To configure **Ping**:

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

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

To configure **DNS Lookup**:

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

To configure Traceroute:

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

Figure 51: *Connectivity (Ping) parameters*

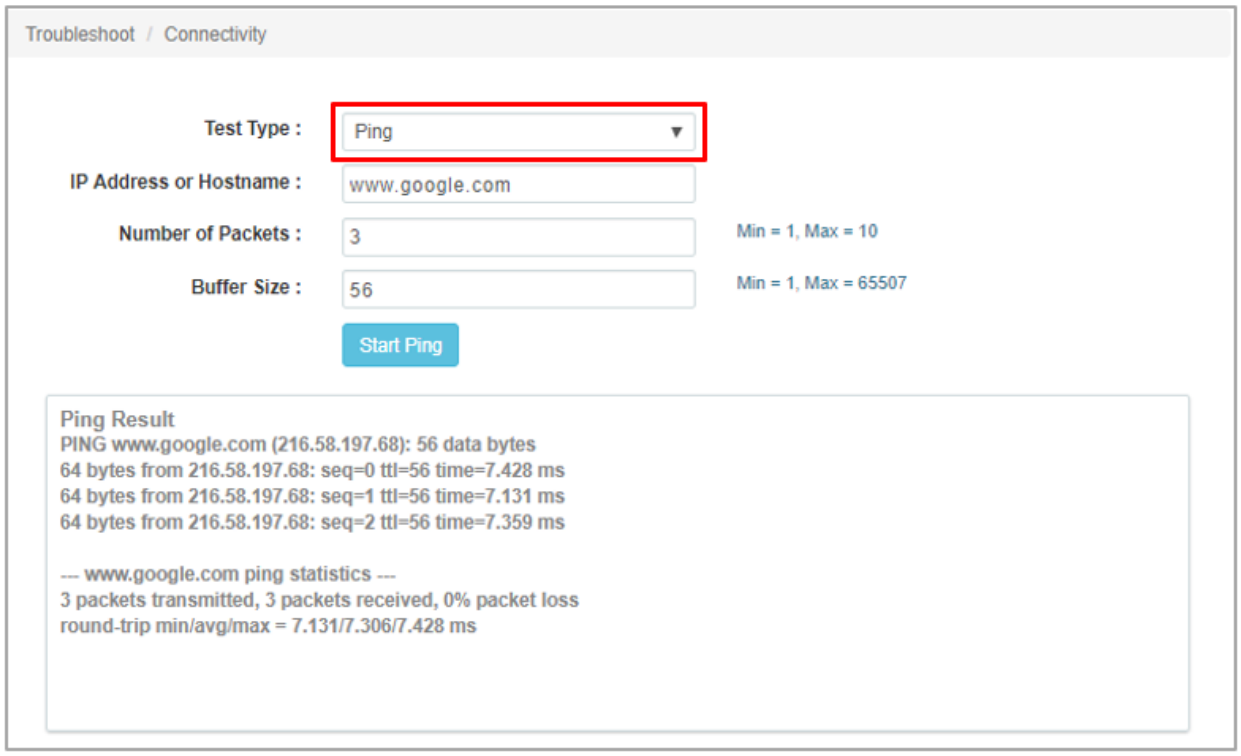


Figure 52: *Connectivity (DNS Lookup) parameters*

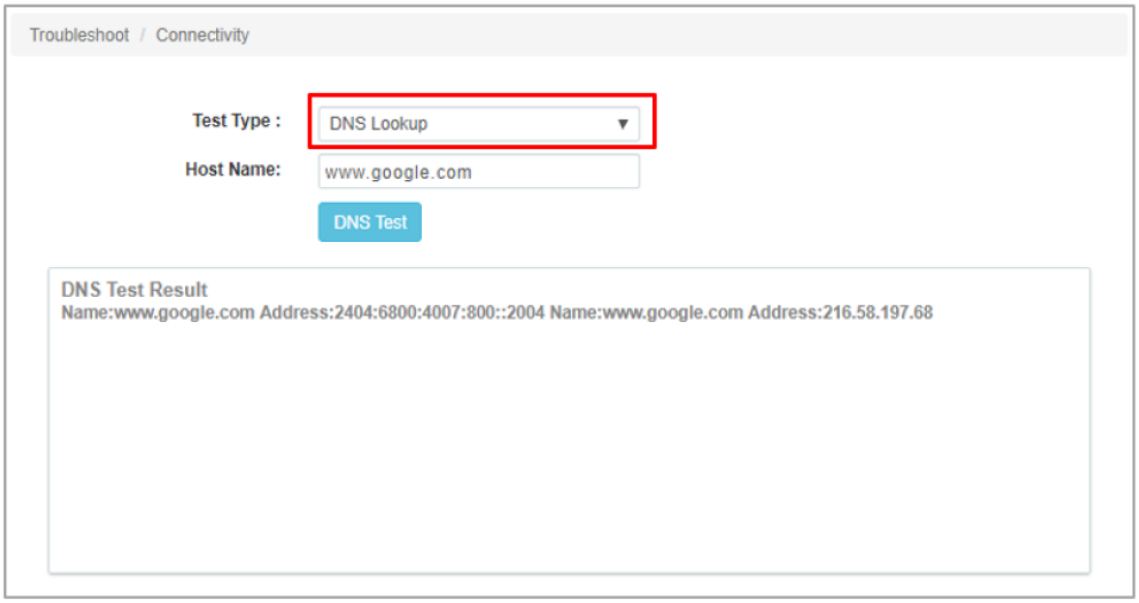
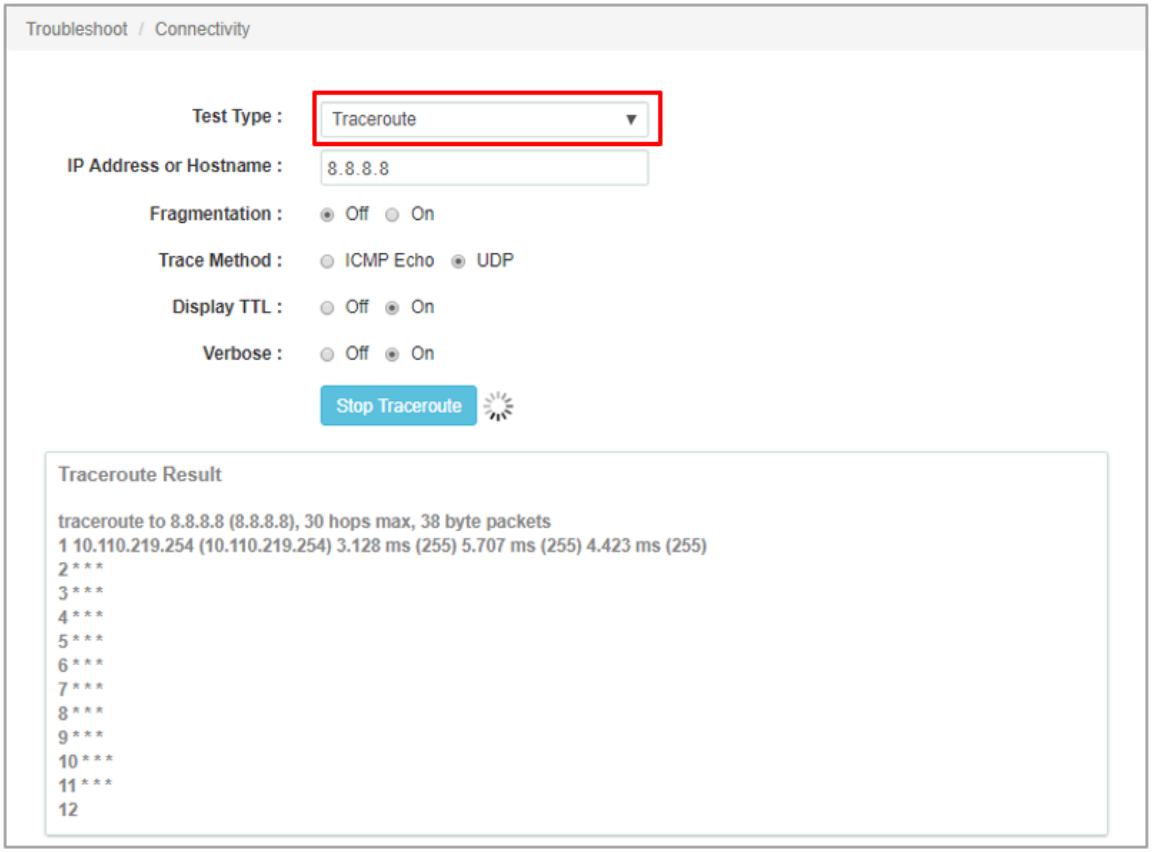


Figure 53: *Connectivity (Traceroute) parameters*



XIRCON tool support

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

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

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

XIRCON tool support for Linux 1.0.0.40

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

Chapter 12: Management Access

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

- Local authentication
- SSH-Key authentication
- RADIUS authentication

Local authentication

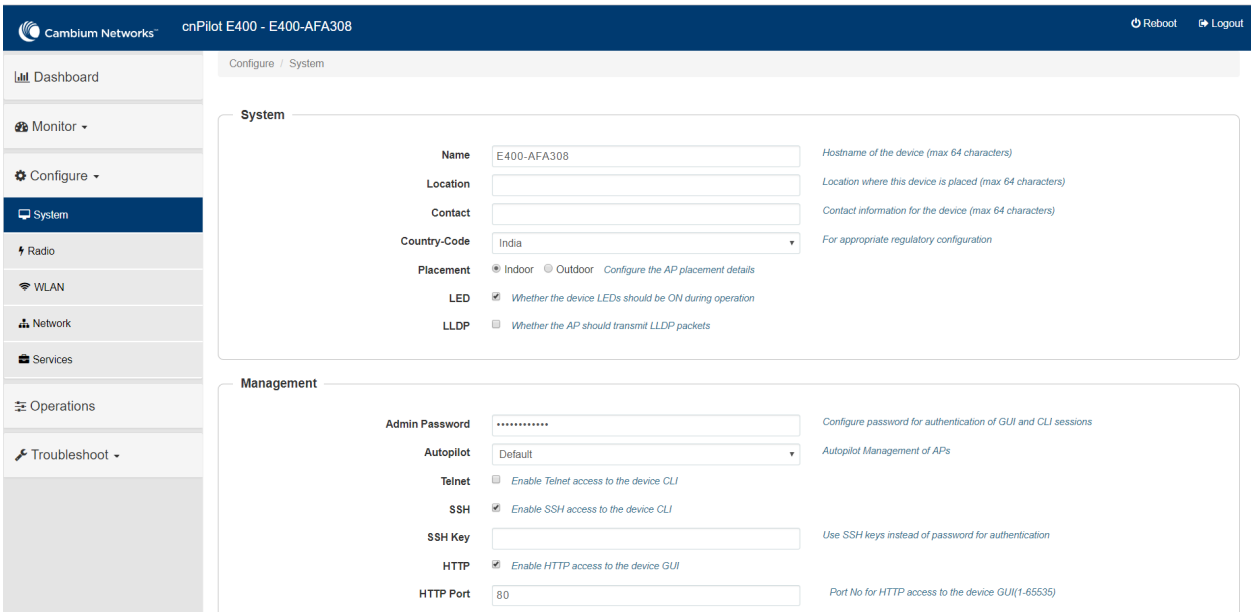
This is the default authentication mode enabled on the device. Only one username is supported which is “admin”. The default password for the “admin” username is “admin”. The user has a provision to configure/update password.

Device configuration

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

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

Figure 54: *Configure/update default password of the admin user*



SSH Key authentication

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

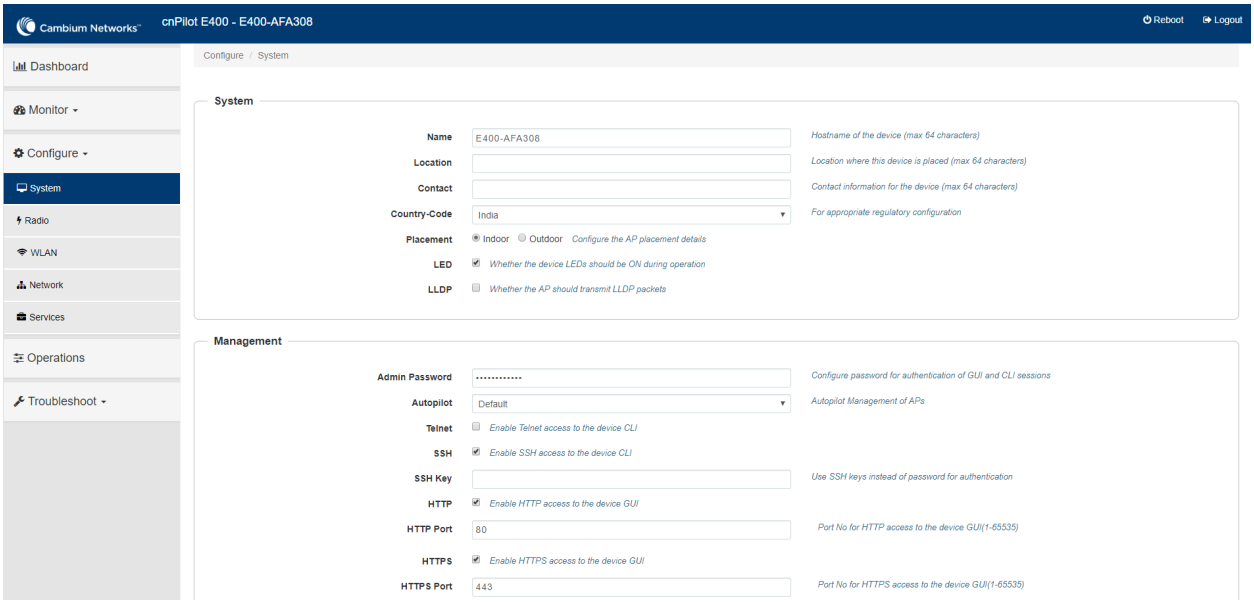
machine of the user and a public key, which is stored to any remote machine (AP) the user wants to connect. So, whenever a user initiates an SSH connection with a remote machine, SSH first checks if the user has a private key that matches any of the public keys in the remote machine and if not, it prompts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

Device configuration

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

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

Figure 55: *Management parameters*



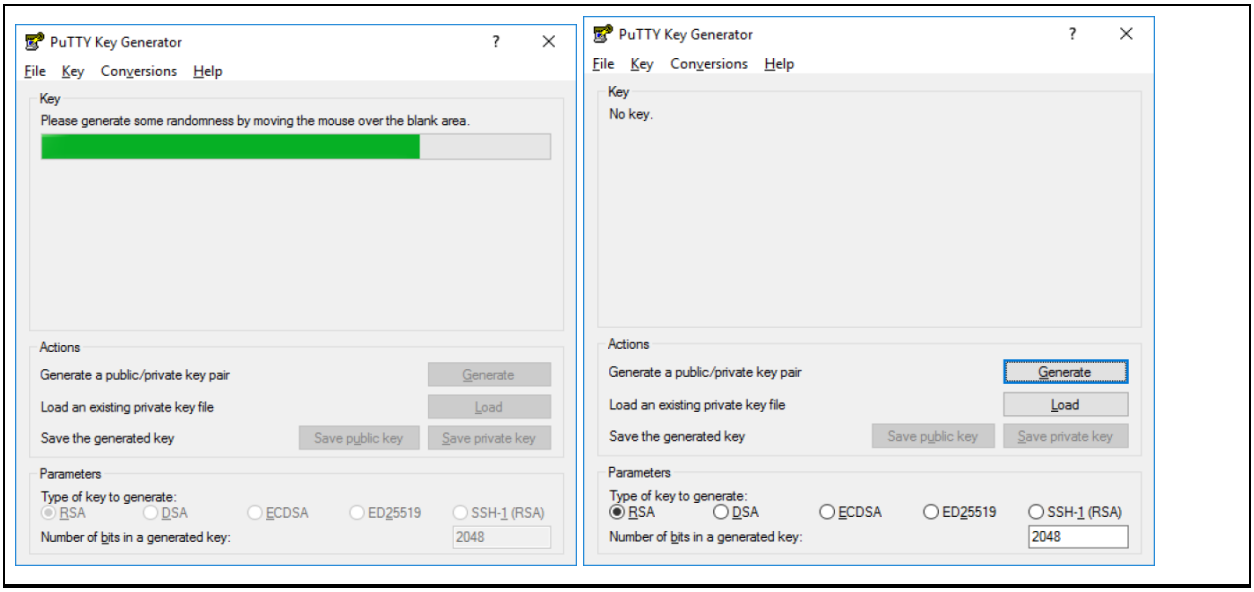
SSH Key generation

Windows

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

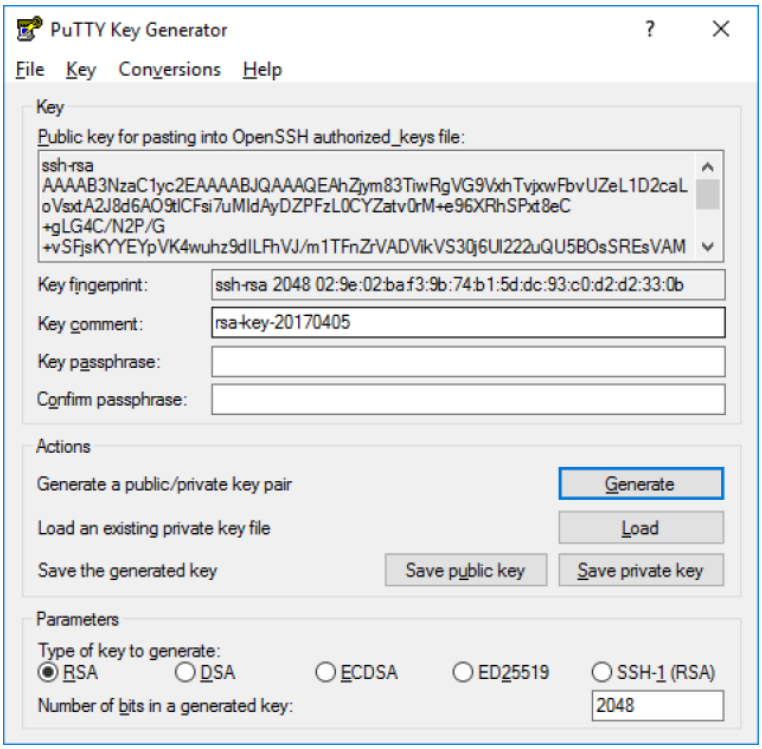
1. Generate a key pair in PUTTY Key Generator (Chapter 12) and save private and public keys as shown in Figure 57.

Figure 56: *Generating public/private Key*



2. Save the Public key and Private key once the key pair is generated as shown in Figure 57.

Figure 57: *Public and Private Key*



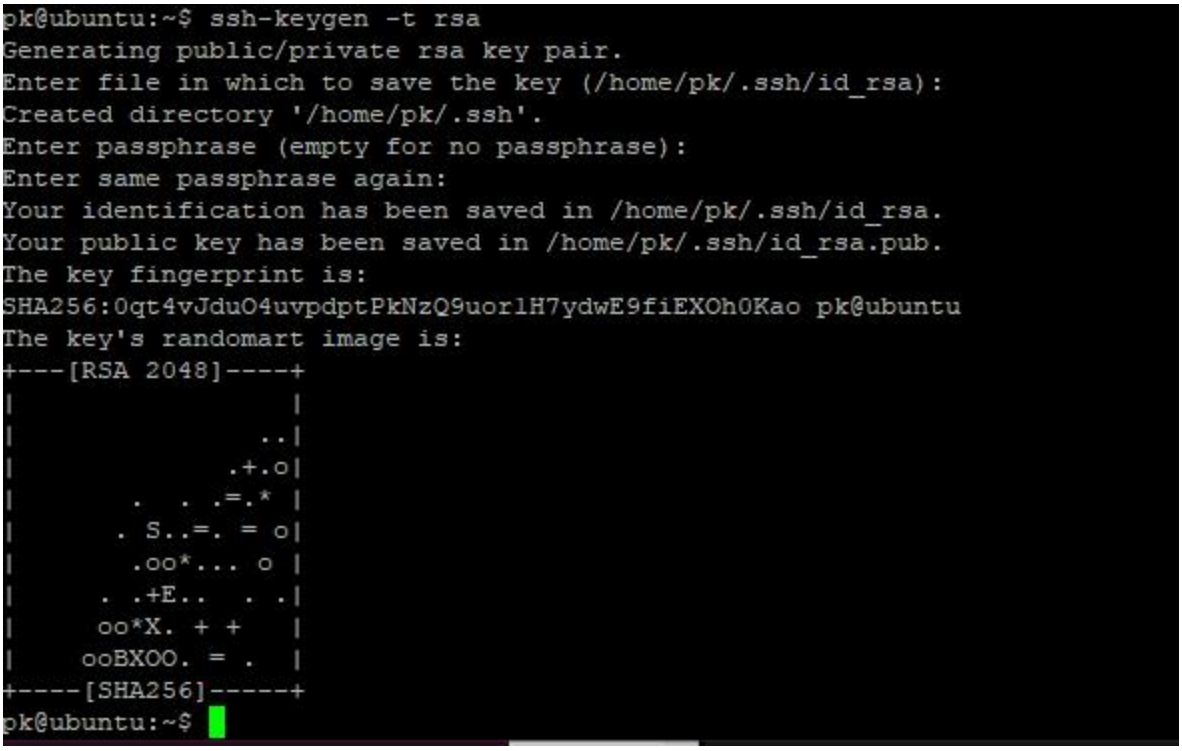
3. Save the Public key generated in the step above as described in Device configuration section.
4. Login to device using Private key generated above with username as “admin”.

Linux

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

1. Generate key pair executing below command on Linux console as shown in Figure 58.

Figure 58: *Public Key location path*



2. The Public key is now located in PATH mentioned in Figure 58.

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

3. The private key (identification) is now saved in PATH as mentioned in Figure 59.

   PATH = “Your identification has saved in <>”

Figure 59: *Private Key saved path*

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

RADIUS authentication

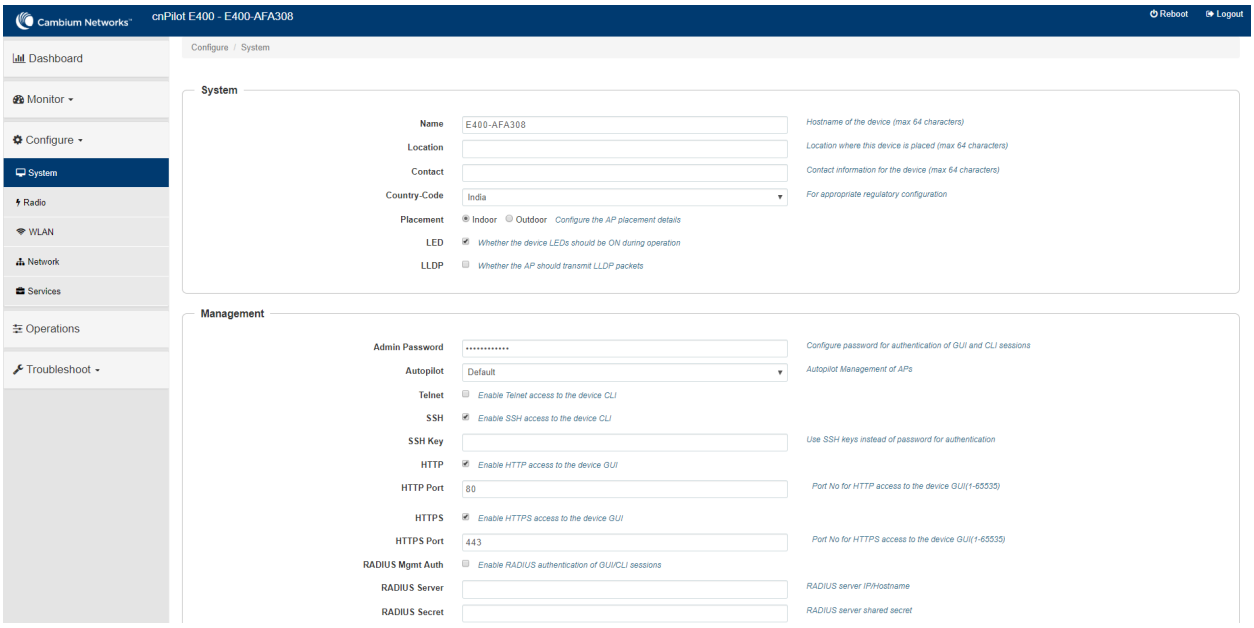
Device management access using RADIUS authentication allows multiple users to access using unique credentials and is secured.

Device configuration

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

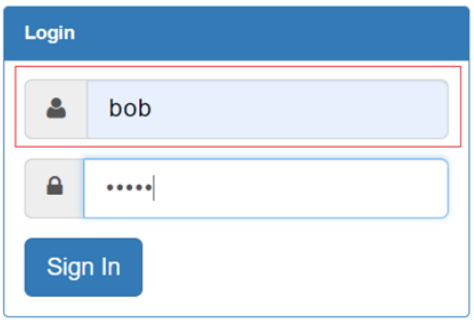
1. Enable **RADIUS Mgmt Auth** checkbox.
2. Configure **RADIUS IPv4/Hostname** and shared secret in **RADIUS Server** and **RADIUS Secret** parameters respectively.
3. Click **Save**.

Figure 60: *RADIUS Server and RADIUS Secret parameters*



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

Figure 61: *UI Login page*



Chapter 13: Guest Access Portal- Internal

Introduction

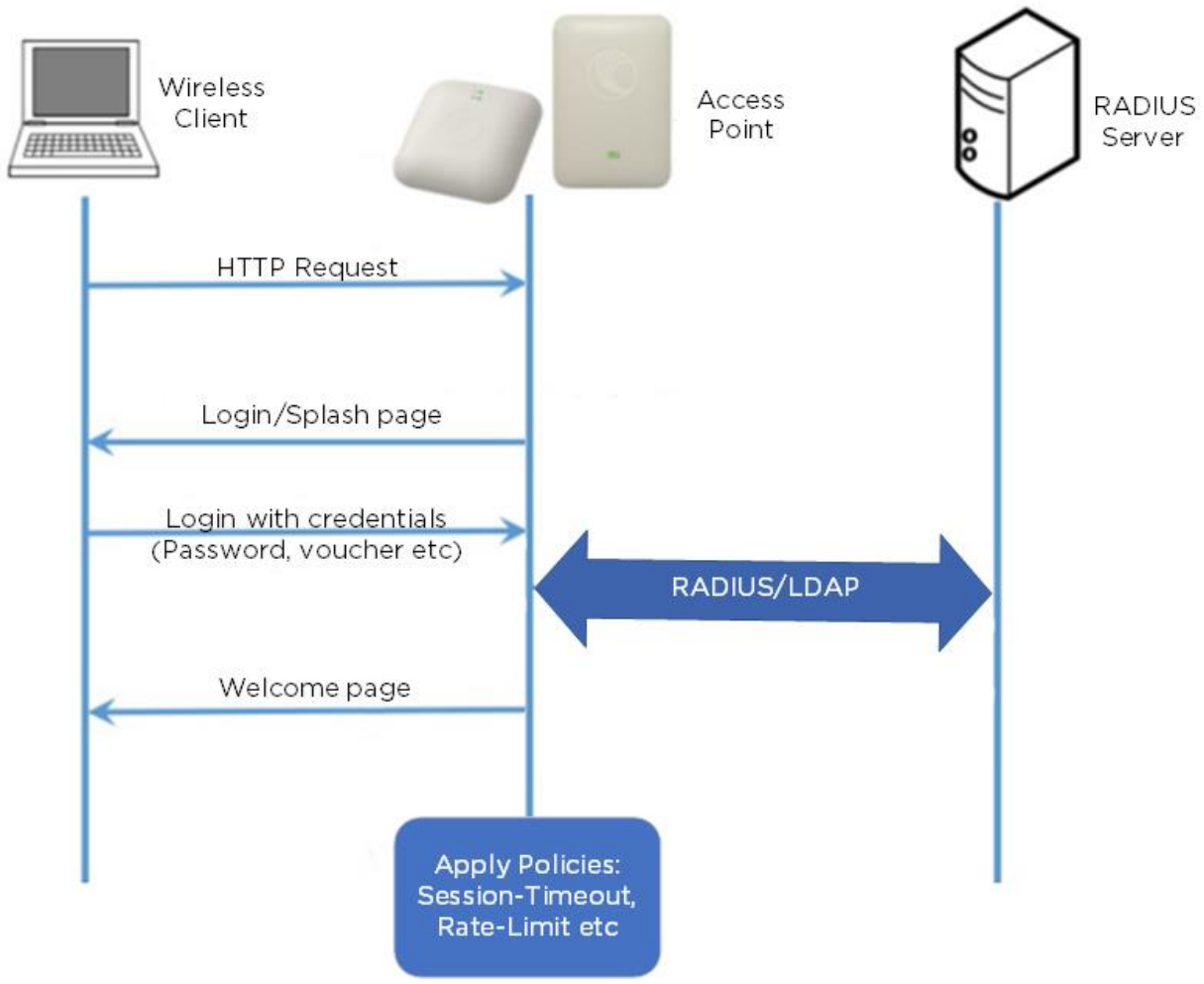
Guest Access Portal services offer a simple way to provide secure access to the internet for users and devices using a standard web browser. Guest access portal allows enterprises to offer authenticated access to the network by capturing and re-directing a web browser's session to a captive portal login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

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

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

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

Figure 62: *Topology*



Configurable parameters

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

Figure 63: *Configure: WLAN > Guest Access > Internal Access Point parameter*

Access policy

Click through

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

Splash page

Title

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

Contents

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

Terms and conditions

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

Logo

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

Background image

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

Redirect parameters

Redirect hostname

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

Success action

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

- Internal logout Page

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

- Redirect users to external URL

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

- Redirect users to the Original URL

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

Figure 64: *Success action*

Redirect

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

Figure 65: *Redirect*

Redirect Mode

There are two redirect modes available:

- **HTTP Mode**

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

- **HTTP(s) Mode**

  When enabled, AP sends HTTPS POST URL to the client

Success message

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

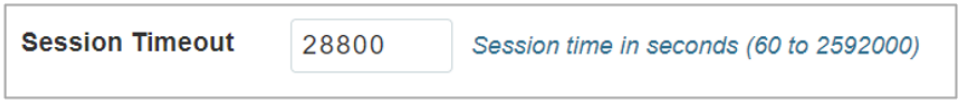
Figure 66: *Success Message*

Timeout

Session

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

Figure 67: *Session timeout*



Inactivity

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

Figure 68: *Inactivity timeout*

Whitelist

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

Configuration examples

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

Access Policy – Clickthrough

Configuration

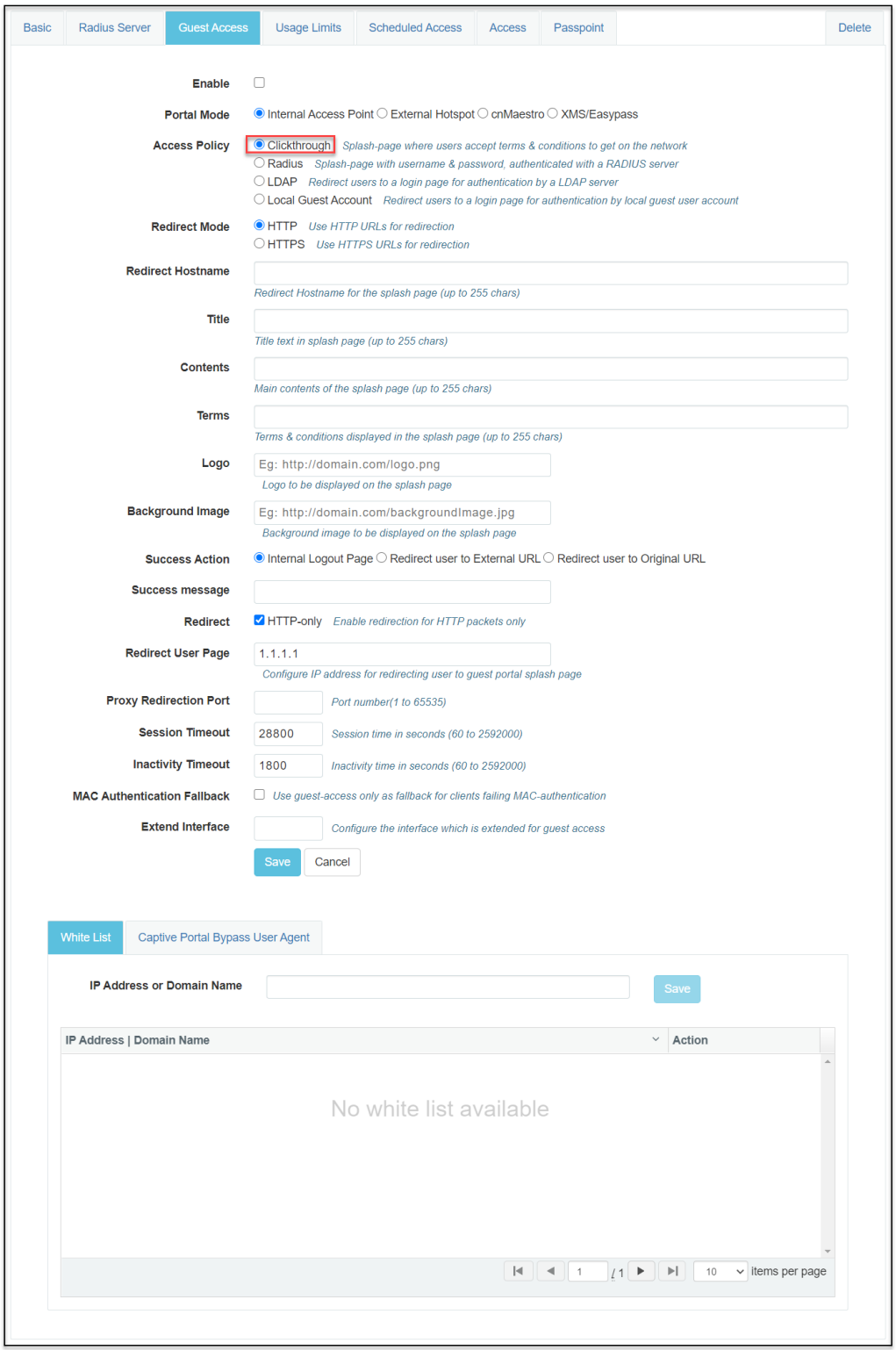


Figure 69: *Authentication – redirected splash page*

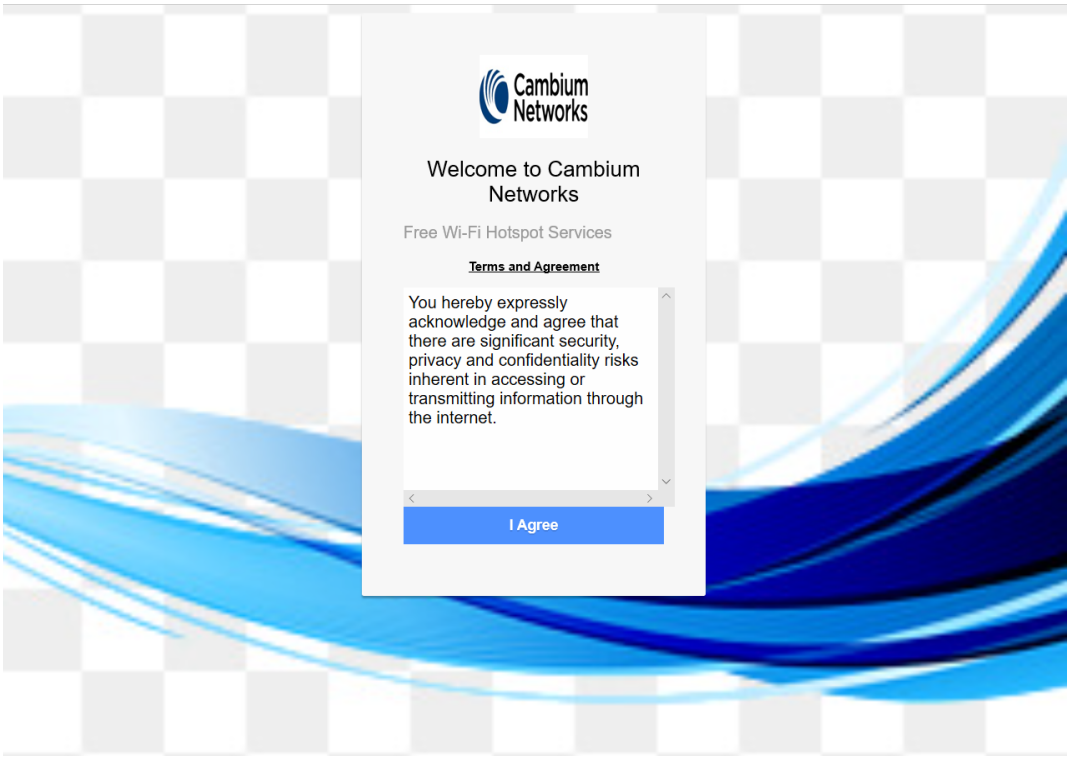
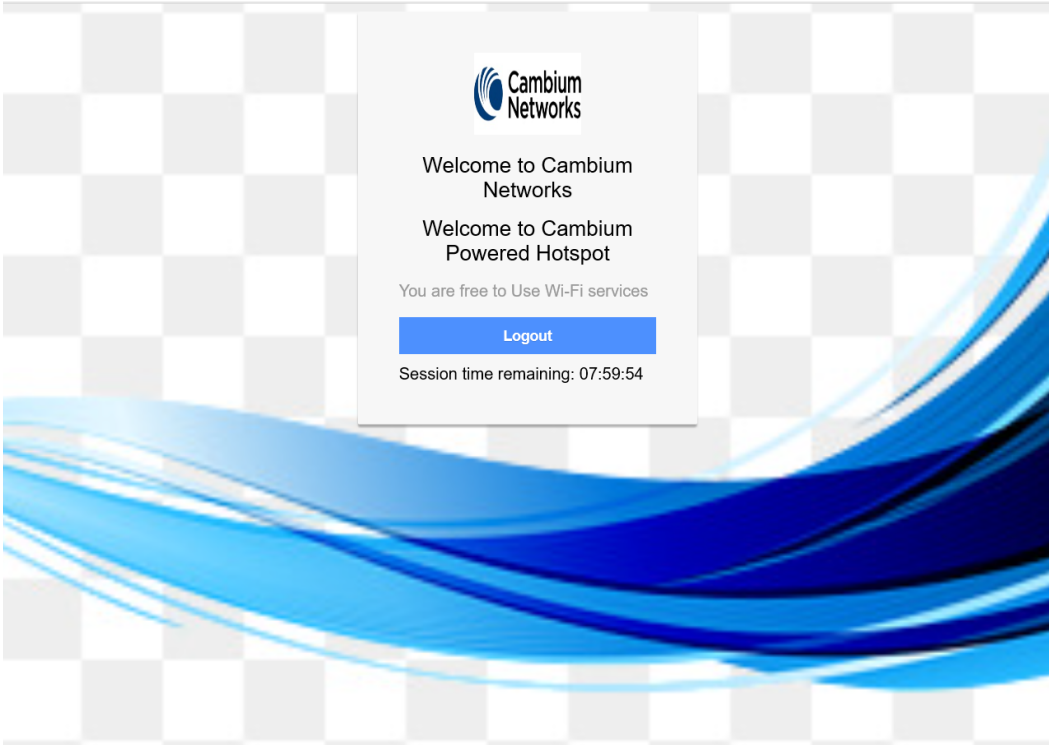


Figure 70: *Successful login – redirected splash page*



Chapter 14: Guest Access Portal- External

Introduction

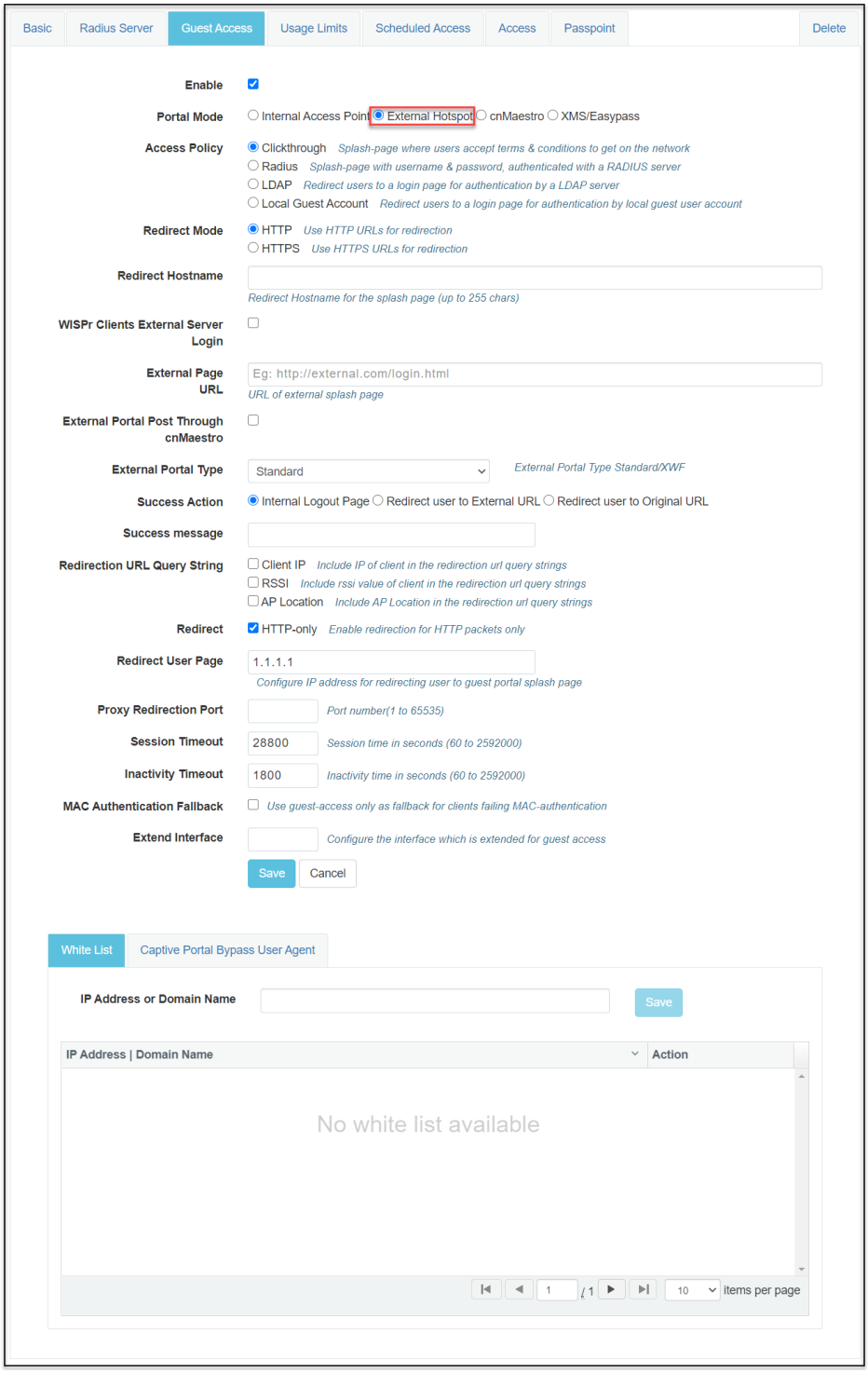
Guest access WLAN is designed specifically for BYOD (Bring Your Own Device) setup, where large organizations have both staff and guests running on the same WLAN or similar WLANs. Cambium Networks provides different options to the customers to achieve this based on where the captive portal page is hosted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

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

Configurable parameters

Figure 71 displays multiple configurable parameters supported for External Guest Access hosted on AP.

Figure 71: *External Access Point parameter*



Access policy

Clickthrough:

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

WISPr

WISPr clients external server login

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

External portal post through cnMaestro

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

Note

This feature is supported only for cnMaetro 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. Users can configure three modes of redirection URL:

- Internal logout Page

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

- Redirect users to external URL

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

- Redirect users to the original URL

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

Figure 72: *Success action*

Redirect

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

Figure 73: *Redirect*

Redirect mode

There are two redirect modes available:

- HTTP Mode

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

- HTTP(s) Mode

  When enabled, AP sends HTTPS POST URL to the client

Success message

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

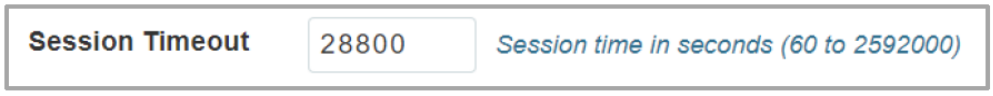
Figure 74: *Success Message*

Timeout

Session

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

Figure 75: *Session timeout*



Inactivity

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

Figure 76: *Inactivity timeout*

Whitelist

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

Configuration examples

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

Access Policy – Clickthrough

Configuration

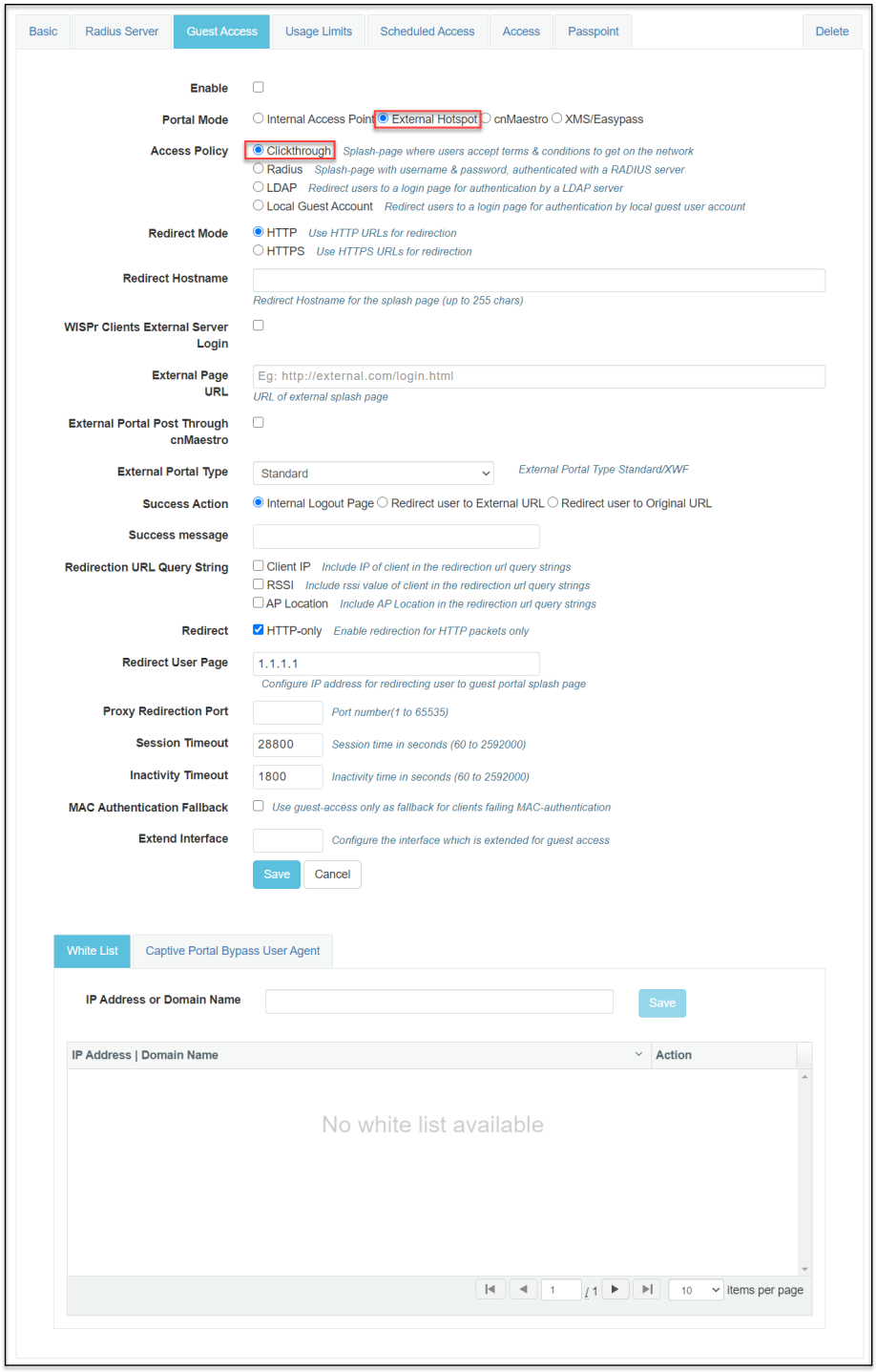


Figure 77: *Authentication – redirected splash page*

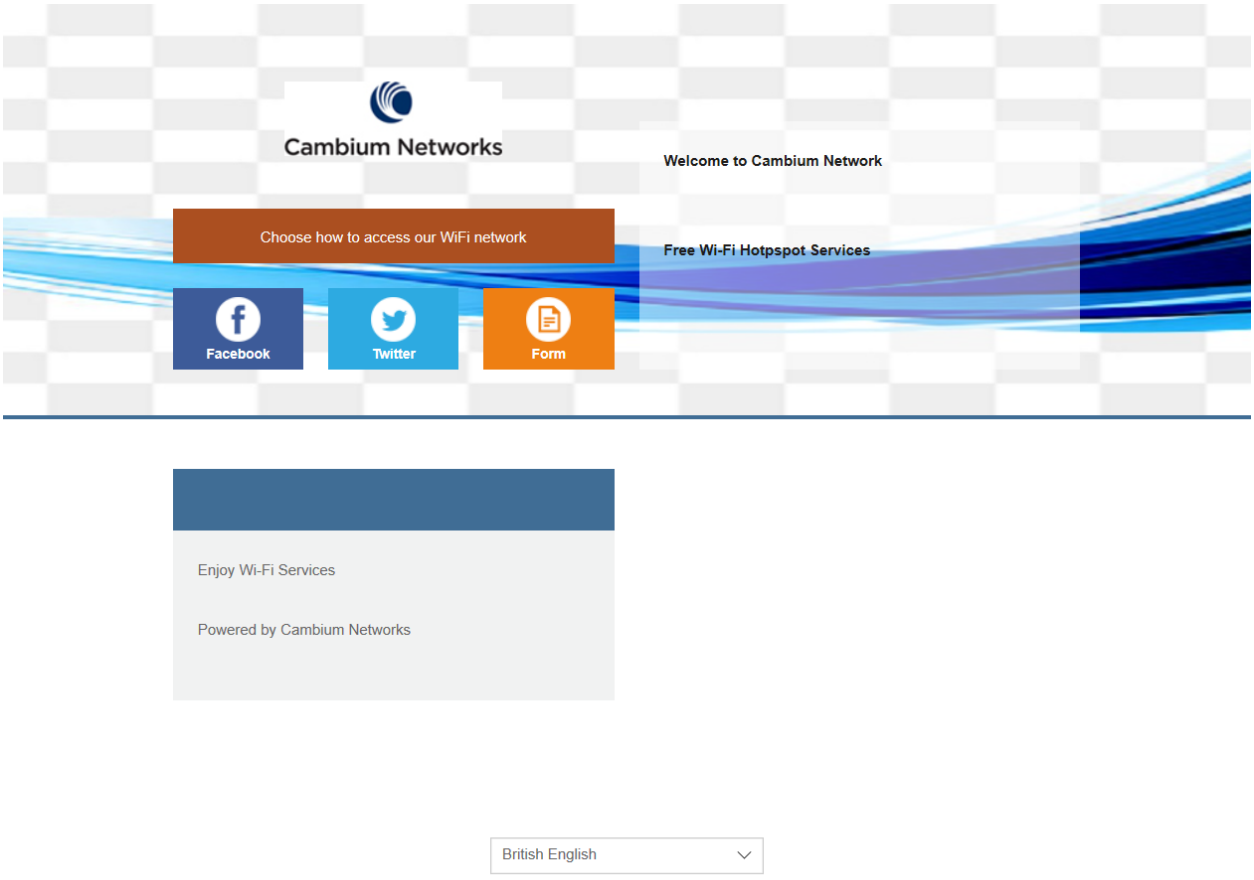
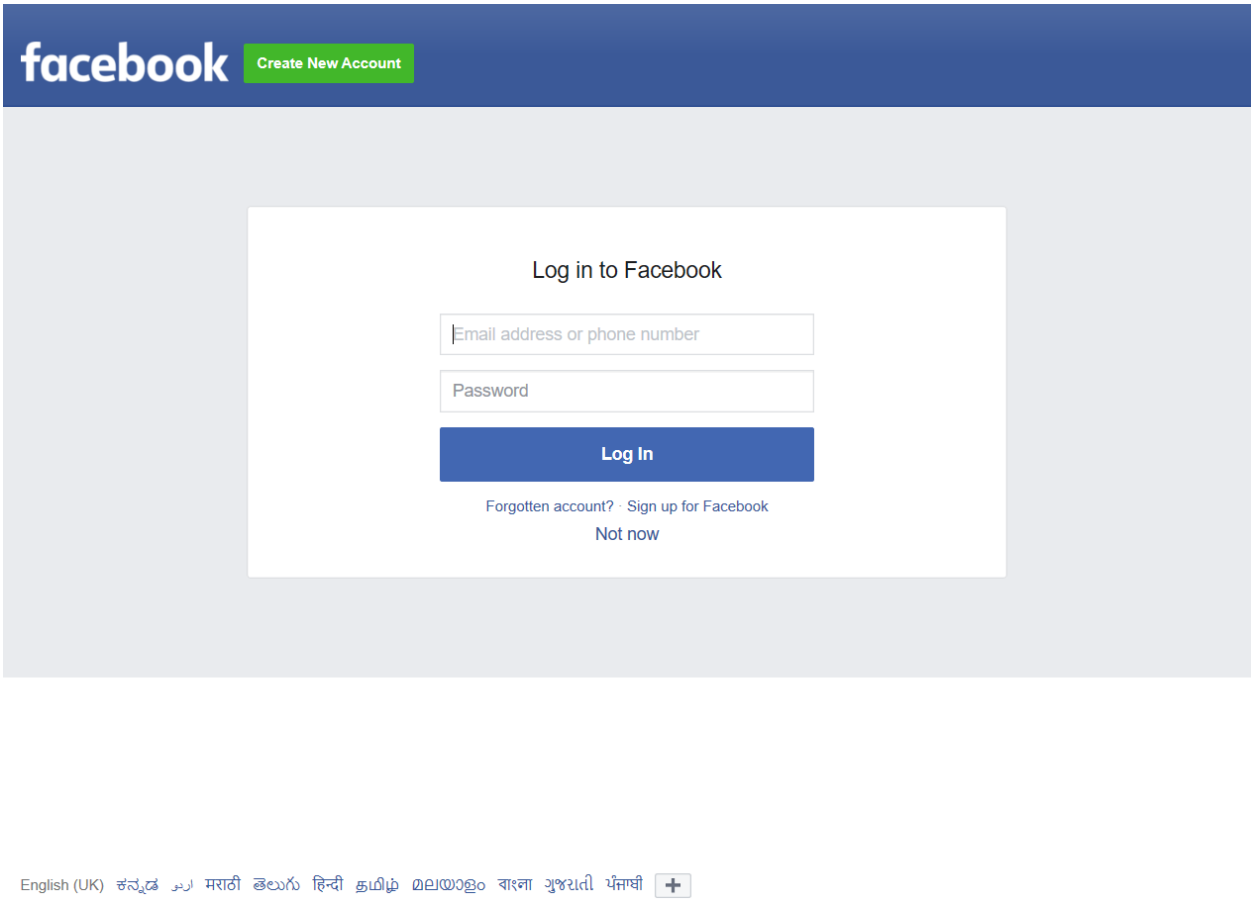


Figure 78: *Successful Login – redirected splash page*



Chapter 15: Guest Access – cnMaestro

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

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

Chapter 16: 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 the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XV2-2T	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
XE3-4	Press and hold the Reset button for 15 seconds	Both LEDs will be OFF and turned onto Amber
e410	Press and hold the Reset button for 25 seconds	LED will be OFF and turned onto Amber
e510	Press and hold the Reset button for 20 seconds	Both LEDs will be OFF and turned onto Amber
e430	Press and hold the Reset button for 25 seconds	LED will be OFF and turned onto Amber
e600	Press and hold the Reset button for 20 seconds	LED will be OFF and turned onto Amber
e700	Press and hold the Reset button for 25 seconds	Both LEDs will be OFF and turned onto Amber

Boot partition change via power cycle

Table 52: Boot partition change via power cycle

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

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

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. The protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus, DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system.
Ethernet Protocol	Any of several IEEE standards that define the contents of frames that are transferred from one network element to another through Ethernet connections.
FCC	Federal Communications Commission of the U.S.A.
GPS	Global Positioning System. A network of satellites that provides absolute time to networks on earth, which use the time signal to synchronize transmission and reception cycles (to avoid interference) and to provide reference for troubleshooting activities.
UI	User interface.
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web.
HTTPS	Hypertext Transfer Protocol Secure
HT	High Throughput
IP Address	The 32-bit binary number identifies a network element by both network and host. See also Subnet Mask.
IPv4	The traditional version of Internet Protocol, defines 32-bit fields for data transmission.
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

Term	Definition
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
Maximum Information Rate (MIR)	The cap is 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.
PSE	Power Sourcing Equipment.
PoE	Power over Ethernet.
SLA	Service Level Agreement
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
VPN	A virtual private network for communication over a public network. One typical use is to connect remote employees, who are at home or in a different city, to their corporate network over the Internet. Any of several VPN implementation schemes are possible. SMs support L2TP over IPSec (Level 2 Tunneling Protocol over IP Security) VPNs and PPTP (Point to Point Tunneling Protocol) VPNs, regardless of whether the Network Address Translation (NAT) feature enabled.
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/learn
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list	http://www.cambiumnetworks.com/contact-us/
User Guides	http://www.cambiumnetworks.com/guides
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom

Cambium Networks™

www.cambiumnetworks.com