



Wi-Fi 6 Access Point

Software Release 12.3.0

User Manual

User Manual

Wi-Fi 6 Access Point

Cloud-Enabled Enterprise Access Points

EAP101

EAP102

EAP104

OAP103-BR (for project only)

How to Use This Guide

This guide includes detailed information on Edgecore access point (AP) software, including how to operate and use the management functions of APs. To deploy APs effectively and ensure trouble-free operation, you should first read the relevant sections in this guide so that you are familiar with all software features.

Who Should Read This Guide? This guide is for network administrators who are responsible for operating and maintaining network equipment. The guide assumes a basic working knowledge of LANs (Local Area Networks) and the Internet Protocol (IP).

How This Guide is Organized The organization of this guide is based on the AP's web management interface. An introduction and initial configuration information is also provided.

The guide includes these sections:

- Section I [“Getting Started”](#) — Includes an introduction to AP management and initial configuration settings.
- Section II [“Web Configuration”](#) — Includes all management options available through the web interface.
- Section III [“Appendices”](#) — Includes information on troubleshooting AP management access.

Related Documentation This guide focuses on AP software configuration, it does not cover hardware installation of an AP. For specific information on how to install an AP, see the following guide:

Quick Start Guide

For all safety information and regulatory statements, see the following documents:

Quick Start Guide

Conventions The following conventions are used throughout this guide to show information:



Note: Emphasizes important information or calls your attention to related features or instructions.



Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History This section summarizes the changes in each revision of this guide.

January 2023 Revision

This is the ninth revision of this guide. It is valid for software release v12.3.0 and includes the following changes:

- Updated QR code Onboarding, see [“QR Code Onboarding” on page 25](#)
- Updated wireless status, see [“Wireless Status” on page 37](#)
- Added support for dynamic PSK, see [“Wireless Networks — Security Settings” on page 66](#)
- Updated Hotspot 2.0 settings, see [“Wireless Networks — Network Settings” on page 71](#)
- Added CAPWAP Tunnel Interface to Ethernet Settings, see [“Ethernet Settings” on page 45](#)

November 2022 Revision

This is the eighth revision of this guide. It is valid for software release v12.2.0 and includes the following changes:

- Added Airtime Fairness, see [“Physical Radio Settings” on page 61](#)
- Modified the value range of BSS Coloring, see [“Physical Radio Settings” on page 61](#)
- Modified wireless security default, see [“Wireless Networks — Security Settings” on page 66](#)
- Added 802.11v, see [“Wireless Networks — Security Settings” on page 66](#)
- Added SNMP Trap, see [“SNMP” on page 89](#)
- Added BLE Scan, see [“BLE” on page 91](#)

November 2022 Revision

This is the seventh revision of this guide. It is valid for software release v12.1.0 and includes the following changes:

- Updated SNMP read/write community settings, see [“SNMP” on page 89](#)
- Added BLE radio Tx Power, see [“BLE” on page 91](#)
- Added Interference Detection, see [“Physical Radio Settings” on page 61](#)
- Added zero-touch provisioning information, see [“Zero-Touch Provisioning” on page 18](#)
- Modified the default value for Minimum Signal Allowed, see [“Physical Radio Settings” on page 61](#)
- Added 160MHz channel bandwidth option, see [“Physical Radio Settings” on page 61](#)
- Removed uCentral cloud option from the Setup Wizard.

July 2022 Revision

This is the sixth revision of this guide. It is valid for software release v12.0.0 and includes the following changes:

- Updated Setup Wizard for uCentral cloud, see [“AP Setup Wizard” on page 20](#)
- Added Proxy ARP, see [“Wireless Networks — Network Settings” on page 71](#)
- Added Multicast-to-Unicast Conversion, see [“Wireless Networks — General Settings” on page 65](#)
- Added Bandsteering, see [“Physical Radio Settings” on page 61](#)
- Added WPA3 Enterprise 192-bit and OWE security, see [“Wireless Networks — Security Settings” on page 66](#)
- Added multiple PSK keys, see [“Wireless Networks — Security Settings” on page 66](#)
- Added Short Guard Interval (SGI), see [“Wireless Networks — Advanced Radio Settings” on page 75](#)
- Added Multicast/Broadcast Rate, see [“Physical Radio Settings” on page 61](#)
- Added UPnP, see [“LAN Settings” on page 48](#)
- Added DHCP Snooping, see [“DHCP Snooping” on page 57](#)
- Added ARP Inspection, see [“ARP Inspection” on page 58](#)

- Added DHCP Relay, see [“DHCP Relay” on page 59](#)
- Added IPv6 for Internet access, see [“IPv6 Settings” on page 45](#)
- Added Hotspot 2.0, see [“Wireless Networks — Network Settings” on page 71](#)
- Added Device Discovery Tool, see [“Device Discovery” on page 93](#)
- Added Discovery Agent settings, see [“Edgecore Networks Discovery Tool” on page 86](#)
- Added Reset button and LED enable, see [“System Settings” on page 79](#)
- Added PoE Out setting, see [“Ethernet Settings” on page 45](#)
- Added caution on firmware upgrades in uCentral mode, see [“Upgrading Firmware” on page 83](#)

April 2022 Revision

This is the fifth revision of this guide. It is valid for software release v11.6.0 and includes the following changes:

- Added Client mode, see [“Physical Radio Settings” on page 61](#)
- Added Site Survey, see [“Wireless Networks — General Settings” on page 65](#)
- Added Custom LAN, see [“LAN Settings” on page 48](#)
- Added WME configuration, see [“Physical Radio Settings” on page 61](#)
- Added BSS Coloring, see [“Physical Radio Settings” on page 61](#)
- Added OFDMA, see [“Physical Radio Settings” on page 61](#)
- Added Target Wake Time, see [“Physical Radio Settings” on page 61](#)
- Added HTTPS captive portal, see [“Captive Portal Settings” on page 55](#)
- Added HTTPS certificate upload, see [“Upload Certificate” on page 84](#)

December 2021 Revision

This is the fourth revision of this guide. It is valid for software release v11.4.0 and includes the following changes:

- Updated QR code onboarding, see [“QR Code Onboarding” on page 25](#)
- Added mesh traffic graph to the dashboard, see [“Traffic Graphs” on page 39](#)
- Added MSP mode, see [“System Settings” on page 79](#)

November 2021 Revision

This is the third revision of this guide. It is valid for software release v11.3.1 and includes the following changes:

- Updated the Setup Wizard, see [“AP Setup Wizard” on page 20](#)
- Updated the Dashboard, see [“Status Information” on page 32](#)
- Added Smart Isolation, see [“LAN Settings” on page 48](#)
- Added Hotspot Settings, see [“Hotspot Settings” on page 52](#)
- Updated wireless network settings, see [“Wireless Networks — Network Settings” on page 71](#)
- Updated wireless open mesh settings, see [“Wireless Networks — Open Mesh Settings” on page 74](#)
- Added Telnet settings, see [“Telnet” on page 86](#)
- Added web server settings, see [“Web Server” on page 87](#)
- Added multicast DNS, see [“Multicast DNS” on page 90](#)
- Added firewall settings, see [“Firewall Rules” on page 50](#)
- Added a guest network, see [“LAN Settings” on page 48](#)

July 2021 Revision

This is the second revision of this guide. It is valid for software release v11.2.0 and includes the following changes:

- Added WPA3-Personal transition, WPA3-Enterprise, and WPA3-Enterprise transition. See [“Wireless Networks — Security Settings” on page 66](#)
- Support for IEEE 802.11 k/r, see [“Wireless Networks — Security Settings” on page 66](#)
- Added Minimum signal allowed (RSSI Threshold), see [“Physical Radio Settings” on page 61](#)
- Support for Open Mesh, see [“Wireless Networks — Open Mesh Settings” on page 74](#)
- SNMP v2 support, see [“SNMP” on page 89](#)
- Support for remote Syslog, see [“Remote System Log Setup” on page 88](#)
- Support for LLDP, see [“LLDP” on page 91](#)

- Support for management by an EWS-Series Controller, see [“System Settings” on page 79](#)

April 2021 Revision

This is the first revision of this guide. It is valid for software release v11.1.1.

Contents

How to Use This Guide	3
Contents	9
Figures	12
Tables	15

Section I	Getting Started	16
	1 Introduction	17
	Configuration Options	18
	Zero-Touch Provisioning	18
	Connecting to the Web Interface	19
	LAN Port Connection	19
	AP Setup Wizard	20
	QR Code Onboarding	25
	Main Menu	28
	Dashboard	29
	Common Web Page Buttons	29

Section II	Web Configuration	31
	2 Status Information	32
	General Status	33
	Network Status	35
	Wireless Status	37
	Traffic Graphs	39
	Services	39
	3 Network Settings	41

Internet Settings	42
IPv6 Settings	45
Ethernet Settings	45
LAN Settings	48
Firewall Rules	50
Port Forwarding	51
Hotspot Settings	52
Network Settings	52
DHCP Snooping	57
ARP Inspection	58
DHCP Relay	59
4 Wireless Settings	60
Radio Settings	61
Physical Radio Settings	61
Wireless Networks — General Settings	65
Wireless Networks — Security Settings	66
Wireless Networks — Network Settings	71
Wireless Networks — Open Mesh Settings	74
Wireless Networks — Advanced Radio Settings	75
VLAN Settings	76
5 System Settings	78
System Settings	79
Maintenance	81
Displaying System Logs	81
Downloading the Diagnostics Log	82
Rebooting the Access Point	82
Resetting the Access Point	82
Backing Up Configuration Settings	83
Restoring Configuration Settings	83
Upgrading Firmware	83
Upload Certificate	84
User Accounts	84
Services	85

SSH	85
Telnet	86
Edgecore Networks Discovery Tool	86
Web Server	87
Remote System Log Setup	88
Network Time	88
SNMP	89
Multicast DNS	90
LLDP	91
BLE	91
Diagnostics	92
Device Discovery	93

Section III	Appendices	94
	A Troubleshooting	95
	Problems Accessing the Management Interface	95
	Using System Logs	95

Figures

Figure 1: Web Management Login	19
Figure 2: Select ecCloud, EWS Controller, or Stand-Alone	20
Figure 3: CAPWAP Setup	21
Figure 4: Wireless Setup	22
Figure 5: Network Setup	22
Figure 6: Change Password	23
Figure 7: Select Country	23
Figure 8: Scanning the AP QR Code	25
Figure 9: Setup Wizard - Network Setup	26
Figure 10: Setup Wizard - Device Management	26
Figure 11: Connect to New SSID	26
Figure 12: ecCLOUD Login Page	27
Figure 13: ecCLOUD Device Registration	28
Figure 14: The Dashboard	29
Figure 15: Saving Configuration Changes	30
Figure 16: General Status Information	33
Figure 17: Local Networks	35
Figure 18: ARP Table	35
Figure 19: Active DHCP Leases	36
Figure 20: Wireless Status	37
Figure 21: Traffic Graphs	39
Figure 22: Services	39
Figure 23: Internet Settings	42
Figure 24: IP Address Mode – Static IP	43
Figure 25: IP Address Mode – PPPoE	44
Figure 26: IPv6 Settings	45
Figure 27: Ethernet Settings – Internet Source	46
Figure 28: Ethernet Settings – Network Behavior	46
Figure 29: Bridge to Internet	47

Figure 30: Route to Internet	47
Figure 31: Network – LAN Settings	48
Figure 32: Firewall Rules	50
Figure 33: Port Forwarding	51
Figure 34: Hotspot Settings (Network Settings)	52
Figure 35: Hotspot Settings (RADIUS Settings)	54
Figure 36: Hotspot Settings (Captive Portal Settings)	55
Figure 37: DHCP Snooping	57
Figure 38: ARP Inspection	58
Figure 39: DHCP Relay	59
Figure 40: Physical Settings for Radio 5 GHz	61
Figure 41: Physical Settings for Radio 2.4 GHz	62
Figure 42: Radio Settings (General Settings)	65
Figure 43: Wireless Security Settings	66
Figure 44: Wireless Network Settings	71
Figure 45: Open Mesh Settings	75
Figure 46: Advanced Radio Settings	75
Figure 47: Configuring VLANs	77
Figure 48: System Settings	79
Figure 49: Maintenance	81
Figure 50: System Log	81
Figure 51: Rebooting the Access Point	82
Figure 52: Resetting to Defaults	82
Figure 53: Restoring Configuration Settings	83
Figure 54: Upgrading Firmware	83
Figure 55: Upload Certificate	84
Figure 56: User Accounts	84
Figure 57: SSH Settings	85
Figure 58: Telnet Server Settings	86
Figure 59: Discovery Agent Settings	86
Figure 60: Web Server Settings	87
Figure 61: Remote System Log Settings	88
Figure 62: NTP Settings	89
Figure 63: SNMP Settings	89
Figure 64: Multicast DNS Settings	90

Figures

Figure 65: LLDP Settings	91
Figure 66: BLE Settings	91
Figure 67: BLE Scan	92
Figure 68: Network Utilities	93
Figure 69: Device Discovery Tool	93

Tables

Table 1: Troubleshooting Chart

95

Section I

Getting Started

This section provides an overview of the access point, and introduces some basic concepts about wireless networking. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- [“Introduction” on page 17](#)

Introduction

The access point (AP) runs software that includes a network management agent. The agent offers a variety of management options, including a web-based interface. The AP can also be accessed through Secure Shell (SSH) for configuration using a command line interface (CLI).



Note: This manual describes the configuration interface for stand-alone mode. Refer to the *Edgecore ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface.

This chapter includes the following sections:

- [“Configuration Options” on page 18](#)
- [“Connecting to the Web Interface” on page 19](#)
- [“AP Setup Wizard” on page 20](#)
- [“QR Code Onboarding” on page 25](#)
- [“Main Menu” on page 28](#)

Configuration Options

The access point's web agent allows you to configure AP parameters, monitor wireless connections, and display statistics using a standard web browser. The AP's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed remotely by a Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The AP's web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Configure IP settings
- Configure 2.4 GHz and 5 GHz radio settings
- Control access through wireless security settings
- Filter packets using Access Control Lists (ACLs)
- Download system firmware
- Download or upload configuration files
- Display system information

Zero-Touch Provisioning

APs can be automatically managed by the Edgecore ecCLOUD controller or an EWS-Series controller. If an AP is already registered with the ecCLOUD controller, it will be automatically managed when the WAN port of the AP is connected to the Internet.

When an AP is connected to a local LAN with an EWS-Series controller, the AP can be configured with the controller IP address through DHCP Option 138 and then automatically managed by the controller.

As an alternative to zero-touch provisioning, you can manually set the preferred management method from the web interface, see ["System Settings" on page 79](#).

Connecting to the Web Interface

For first-time access to the AP's web management interface, you can connect a PC directly to one of the AP's LAN ports or use the quick-setup QR code (printed on a label next to the AP's ports). The first-time you access the web interface, it automatically runs the Setup Wizard for initial AP configuration.

For information on the Setup Wizard, see ["AP Setup Wizard" on page 20](#).

For information on using the QR code, see ["QR Code Onboarding" on page 25](#).

LAN Port Connection When connecting to the web management interface through one of the AP's LAN ports, the AP has a default management IP address of 192.168.2.1 and a subnet mask of 255.255.255.0. Therefore, you must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start with 192.168.2.x).



Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

To access the AP's web management interface, use your web browser to connect to the management interface by entering the default IP address of 192.168.2.1.

For first-time access, there is no user login and the Setup Wizard starts automatically. Follow the steps described in ["AP Setup Wizard" on page 20](#).

Figure 1: Web Management Login

SETUP WIZARD

Will this device be managed?

☒ Yes, I will manage this device by ecCloud controller.

☐ Yes, I will manage this device by EWS-Series controller.

☐ No, I will be operating this device in stand-alone mode.

[+ Select Your Country](#)

Done



Note: To configure the AP with a different management IP address that is compatible with your network, see ["LAN Settings" on page 48](#).

AP Setup Wizard

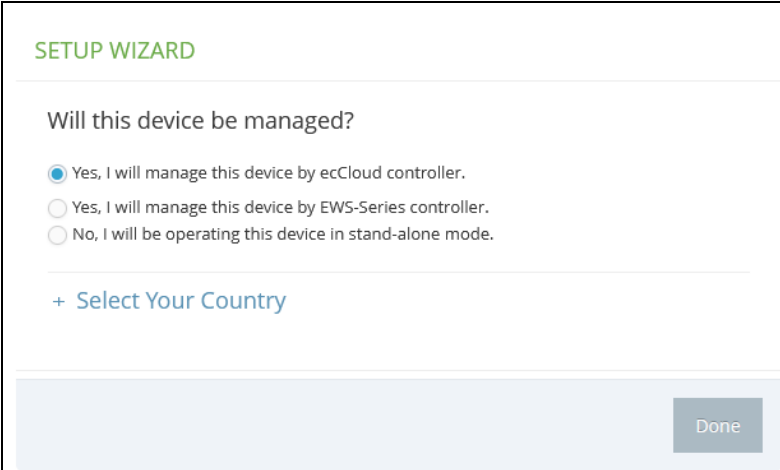
The Setup Wizard is designed to help you configure the basic settings required to get the AP up and running.

Step 1 Select How the AP will be Managed — To manage the AP using the Edgecore ecCLOUD controller, select “Yes, I will manage this device by ecCloud controller,” and then continue to [Step 6](#).

To manage the AP using the an Edgecore EWS-series controller, select “Yes, I will manage this device by EWS-Series controller,” and then continue to [Step 2](#).

Otherwise, select “No, I will be operating this device in stand-alone mode” and continue to [Step 3](#).

Figure 2: Select ecCloud, EWS Controller, or Stand-Alone



If you select to manage the AP using the Edgecore ecCLOUD controller, go to cloud.ignitenet.com to register your AP. Log in and select Devices from the menu. Click Add Device and enter the AP serial number and MAC address to register the AP with your cloud network. The serial number and MAC address can be found on the product packaging or label.



Note: This manual describes the configuration interface for stand-alone mode. Refer to the *Edgecore ecCLOUD Controller User Manual* for information on configuring the AP through the cloud interface or the *EWS-Series Controller User Manual* for information on managing the AP through an EWS controller.

Step 2 CAPWAP Setup — When EWS-Series Controller management is selected, you can set the mode for discovering the controller. Once the AP has discovered the controller on the network it can then send a CAPWAP (Control And Provisioning of Wireless Access Points) join request.

In Auto mode, the AP uses four methods to discover the controller. These methods require no further configuration.

In manual mode, two options are available. Specify the Domain Name Suffix so that the AP can use DNS server records to discover the EWS controller. Or, just specify a static IP address for the controller.

For more information on CAPWAP setup, see [“System Settings” on page 79](#).

Figure 3: CAPWAP Setup

The screenshot shows the 'SETUP WIZARD' interface. At the top, it asks 'Will this device be managed?' with three radio button options: 'Yes, I will manage this device by ecCloud controller.', 'Yes, I will manage this device by EWS-Series controller.' (which is selected), and 'No, I will be operating this device in stand-alone mode.' Below this is a section titled '- CAPWAP Setup'. It features a 'Mode' dropdown menu currently set to 'Auto'. A note below the dropdown states: '(In auto configuration, Broadcast Discovery, Multicast Discovery, DNS SRV Discovery and DHCP Option Discovery are enabled.)'. At the bottom of the wizard, there is a 'Change Your Password' link and a 'Done' button.

After completing the CAPWAP setup, continue with [Step 5](#).

Step 3 Wireless Setup — If you select to manage the AP in stand-alone mode, you can configure the default wireless network.

The default wireless network name (SSID) consists of the AP model and its serial number, and there is a default wireless password. You have the option to modify the wireless network name and password to your preferred configuration. The wireless name must be 1-32 ASCII characters, and the password must be 8 to 63 ASCII characters (no special characters are allowed).

Figure 4: Wireless Setup

The screenshot shows the 'SETUP WIZARD' interface. At the top, it asks 'Will this device be managed?' with three radio button options: 'Yes, I will manage this device by ecCloud controller.', 'Yes, I will manage this device by EWS-Series controller.', and 'No, I will be operating this device in stand-alone mode.' The third option is selected. Below this, there is a section for 'Wireless Setup' which is currently collapsed, indicated by a minus sign. The SSID is set to 'EAP101-EC2107004231' and the Wireless password is '12345678'. There is a 'Show Key' checkbox which is checked. Below the wireless setup section, there is a section for 'Network Setup' which is expanded, indicated by a plus sign. At the bottom right of the wizard, there is a 'Done' button.

Step 4 Network Setup — For AP stand-alone mode, you also have the option to configure the IP address mode used to provide an IP address for the Internet access port.

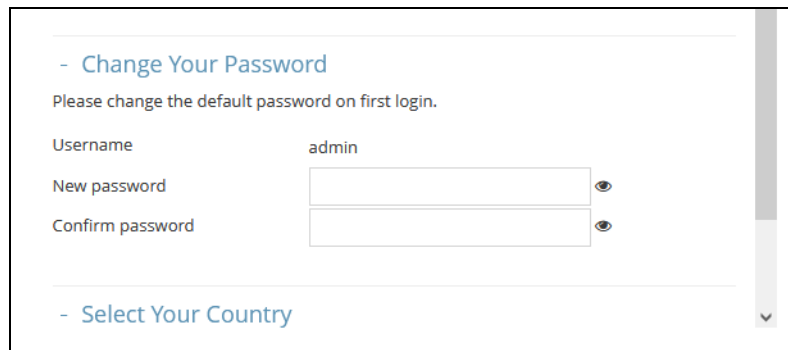
The default IP Address Mode is DHCP and other options include Static IP and PPPoE. For more information, see [“Internet Settings” on page 42](#).

Figure 5: Network Setup

The screenshot shows the 'SETUP WIZARD' interface. At the top, it asks 'Will this device be managed?' with three radio button options: 'Yes, I will manage this device by ecCloud controller.', 'Yes, I will manage this device by EWS-Series controller.', and 'No, I will be operating this device in stand-alone mode.' The third option is selected. Below this, there is a section for 'Wireless Setup' which is collapsed, indicated by a plus sign. The 'Network Setup' section is expanded, indicated by a minus sign. The IP Address Mode is set to 'DHCP' in a dropdown menu. Below the network setup section, there is a section for 'Change Your Password' which is collapsed, indicated by a plus sign. At the bottom right of the wizard, there is a 'Done' button.

- Step 5** Change Your Password — Set a new password for management access to the AP (the default user name is “admin” with password “admin”). The password must be 6-20 ASCII characters (case sensitive with no special characters).

Figure 6: Change Password



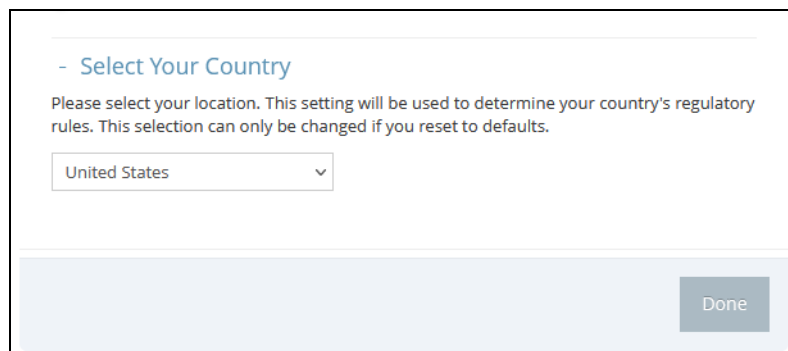
The screenshot shows a web interface titled "Change Your Password". Below the title is a sub-header "- Change Your Password" and a message: "Please change the default password on first login." There are three input fields: "Username" with the value "admin", "New password", and "Confirm password". Each password field has a toggle icon (an eye) to the right. Below these fields is another sub-header "- Select Your Country" and a dropdown arrow icon.



Note: For information on changing user names and passwords, see [“User Accounts”](#) on page 84.

- Step 6** Select Your Country — Select the access point’s country of operation from the drop-down menu. You must set the AP’s country code to be sure that the radios operate according to permitted local regulations. That is, setting the country code restricts operation of the AP to the radio channels and transmit power levels permitted for wireless networks in the specified country.

Figure 7: Select Country



The screenshot shows a web interface titled "Select Your Country". Below the title is a sub-header "- Select Your Country" and a message: "Please select your location. This setting will be used to determine your country's regulatory rules. This selection can only be changed if you reset to defaults." There is a dropdown menu showing "United States" with a downward arrow. At the bottom right of the interface is a "Done" button.



Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.



Note: The country code selection is for non-US models only and is not available to any US models. Per FCC regulation, all Wi-Fi products marketed in the US must be fixed to US operation channels only.

Step 7 After completing the Setup Wizard, click “Done.”

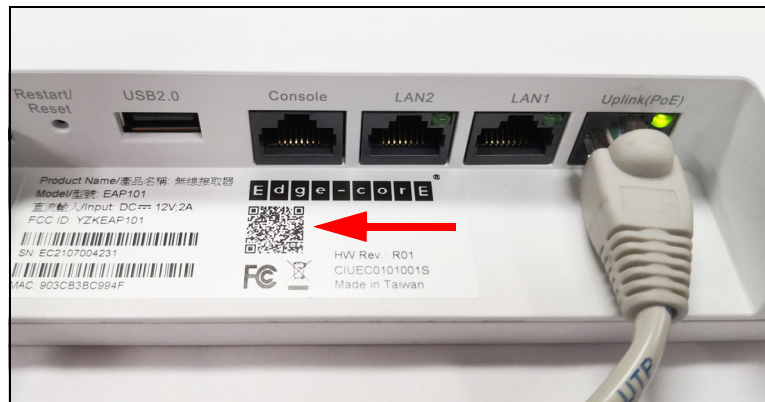
QR Code Onboarding

For quick set up and registration of your AP with the ecCLOUD controller, you can scan the QR code on the AP using a phone.

Follow these steps:

1. Power on the AP.
2. Connect the AP to the Internet. Connect your network or Internet access device to the AP's RJ-45 Uplink port.
3. Use the camera or a barcode app on your phone to scan the AP's QR code. The QR code is printed on a label next to the AP's ports.

Figure 8: Scanning the AP QR Code



4. When a message pops up, tap “yes” to join the Wi-Fi network. (iPhone requires you to go to Settings > Wi-Fi or open the browser for the message to pop up.)

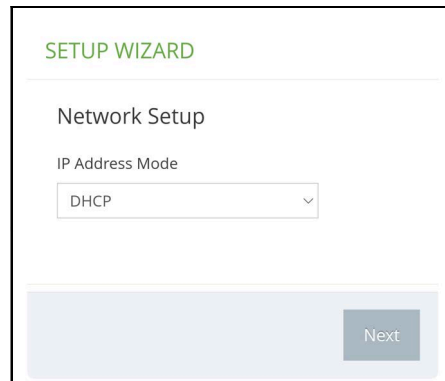
The web browser should open and redirect to the Setup Wizard page.



Note: If the phone cannot connect to the Wi-Fi network, type the SSID (network name) and password manually. The SSID name is the AP serial number (for example, EC0123456789), and the password is the AP MAC address (for example, 903CB3BC1234).

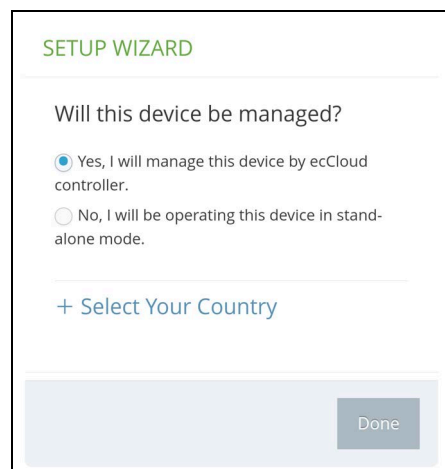
5. Select the IP address setup mode for the AP: DHCP, Static IP, or PPPoE.

Figure 9: Setup Wizard - Network Setup



6. Select to manage the AP using the ecCLOUD controller or to manage the AP in stand-alone mode.

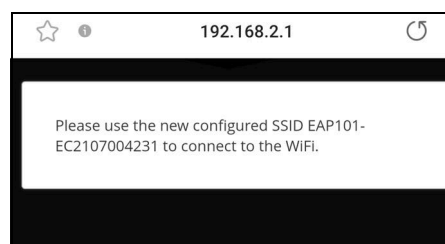
Figure 10: Setup Wizard - Device Management



- a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. Change the login password and set the country of operation. Tap “Done” to finish the setup wizard.

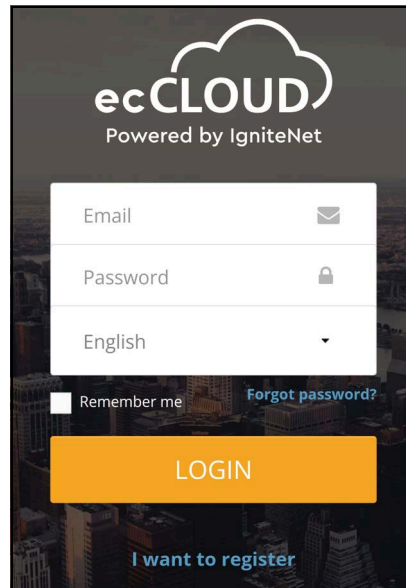
Wait about two minutes for the AP configuration to update, and then connect to the wireless network name configured in the Setup Wizard.

Figure 11: Connect to New SSID



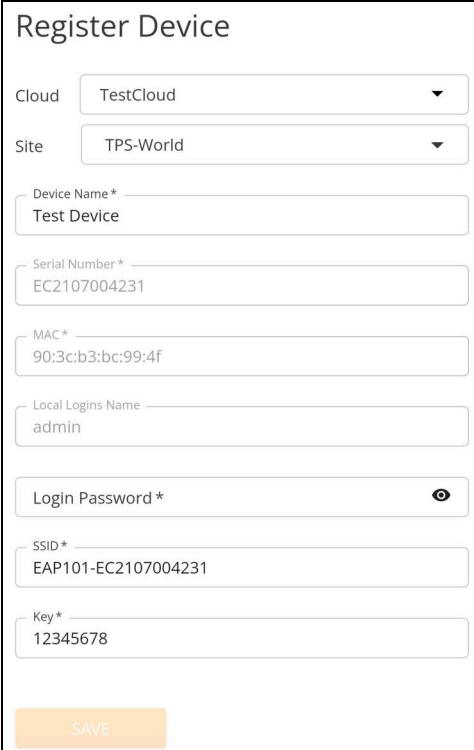
- b.** Cloud-Managed Mode: Set the country of operation and then tap “Done” to finish the Setup Wizard. The browser is redirected to the ecCLOUD login page.

Figure 12: ecCLOUD Login Page



If you already have an ecCLOUD account, log in and select a site for the AP. The AP is automatically registered for cloud management. Modify the device name, login password, SSID, and security key. After you tap “Save,” wait about five minutes for the cloud controller to configure the AP.

Figure 13: ecCLOUD Device Registration

The image shows a web form titled "Register Device". It contains several input fields: "Cloud" with a dropdown menu showing "TestCloud"; "Site" with a dropdown menu showing "TPS-World"; "Device Name *" with the text "Test Device"; "Serial Number *" with the text "EC2107004231"; "MAC *" with the text "90:3c:b3:bc:99:4f"; "Local Logins Name" with the text "admin"; "Login Password *" with a password field icon; "SSID *" with the text "EAP101-EC2107004231"; and "Key *" with the text "12345678". At the bottom of the form is an orange "SAVE" button.

Register Device

Cloud TestCloud

Site TPS-World

Device Name *
Test Device

Serial Number *
EC2107004231

MAC *
90:3c:b3:bc:99:4f

Local Logins Name
admin

Login Password *

SSID *
EAP101-EC2107004231

Key *
12345678

SAVE

If you do not have an ecCLOUD account, tap "I want to register" and set up an account. Create a cloud and site before confirming the regulatory country. After tapping "Next," the AP is then automatically registered for cloud management.

After you tap "Save," wait about five minutes for the cloud controller to configure the AP.



Note: Refer to the Edgecore ecCLOUD Controller User Manual for more information on setting up and configuring APs through ecCLOUD.

Main Menu

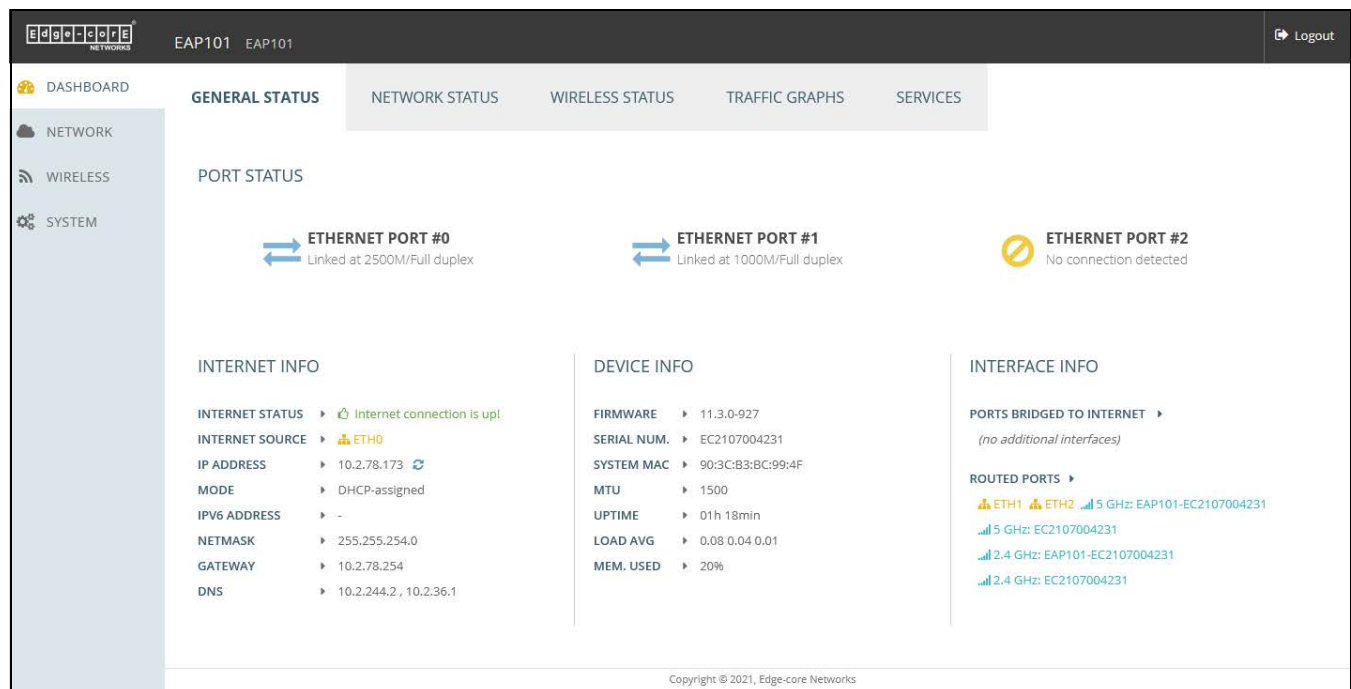
The web interface Main Menu provides access to all the configuration settings available for the AP.

To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Dashboard** — The dashboard shows basic settings for the AP, including general status, local network settings, and wireless radio status. See [“Status Information” on page 32](#).
- **Network** — Configures Internet, Ethernet, and LAN settings. See [“Network Settings” on page 41](#).
- **Wireless** — Configures 5 GHz Radio, 2.4 GHz Radio, and VLAN settings. See [“Wireless Settings” on page 60](#)
- **System** — Configures System (including cloud agent and various system settings), Maintenance (such as view log, reboot, reset defaults, backup defaults, restore defaults, and firmware upgrade), User Accounts, Services (network time), and Diagnostics (including ping, traceroute).

Dashboard After logging in to the web interface, the dashboard displays. The dashboard shows basic settings for the AP, including Internet status, local network settings, and wireless radio status.

Figure 14: The Dashboard



Common Web Page Buttons The list below describes the common buttons found on many of the web management pages:

- **Save** – Applies the new parameters and saves them to temporary RAM memory. Also displays a message at the top of the screen to inform you that the

changes have not yet been saved to Flash memory. The running configuration will not be saved upon a reboot unless you click the “Save & Apply” button.

Figure 15: Saving Configuration Changes



- **Save & Apply** – Saves the changes made on a page and then applies them so that the configuration is retained after a restart.
- **Revert** – Cancels newly entered settings and restores the originals.
- **Logout** – Ends the web management session.

Section II

Web Configuration

This section provides details on configuring the access point using the web browser interface.

This section includes these chapters:

- [“Status Information” on page 32](#)
- [“Network Settings” on page 41](#)
- [“Wireless Settings” on page 60](#)
- [“System Settings” on page 78](#)

2

Status Information

The Dashboard displays information on the current system configuration, including Internet status, local network settings, wireless radio status, traffic graphs, and services.

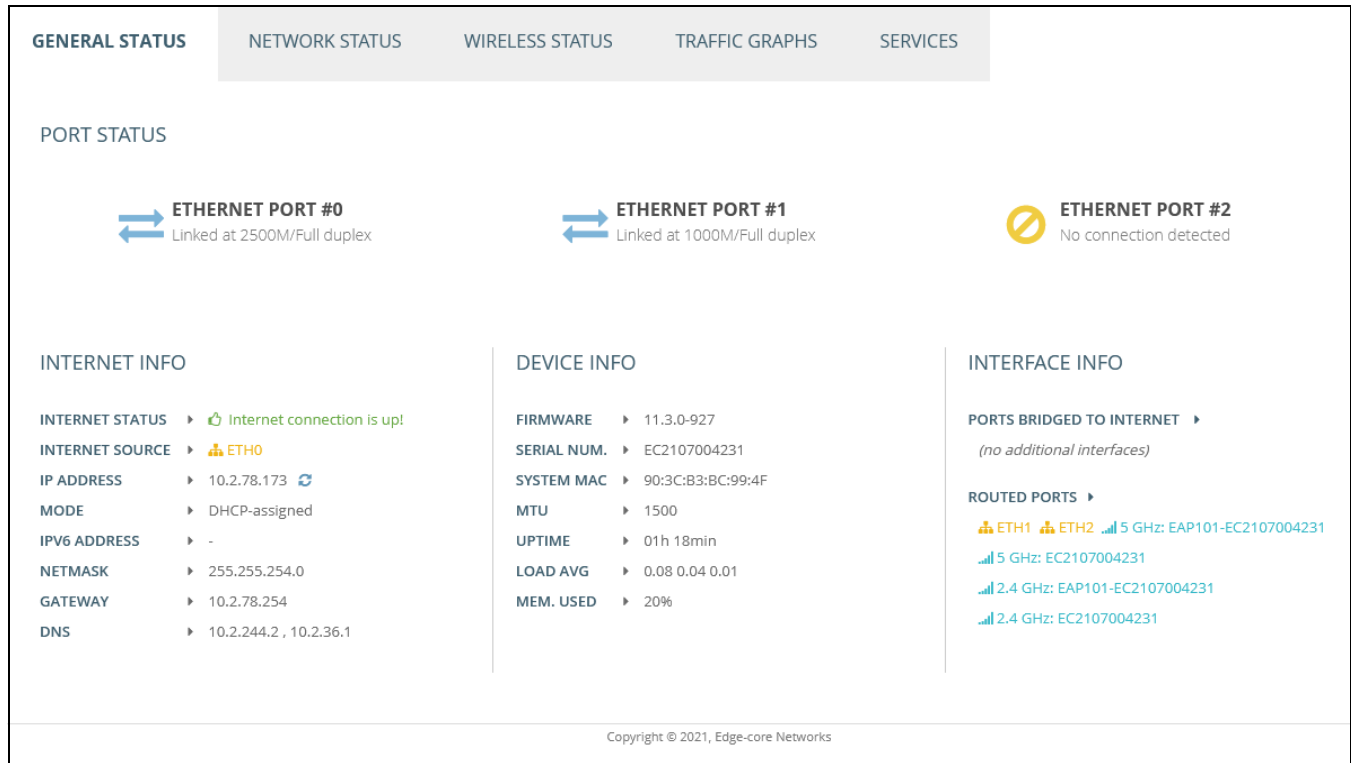
This chapter includes the following sections:

- [“General Status” on page 33](#)
- [“Network Status” on page 35](#)
- [“Wireless Status” on page 37](#)
- [“Traffic Graphs” on page 39](#)
- [“Services” on page 39](#)

General Status

The General Status section shows descriptive information about the AP.

Figure 16: General Status Information



The following items are displayed in the “Port Status” section:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port, including link-up state, speed, and duplex mode.
- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1, including link-up state, speed, and duplex mode.
- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2, including link-up state, speed, and duplex mode.

The following items are displayed in the “Internet Info” section:

- **Internet Status** — Shows whether or not the Internet connection is up.
- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.
- **IP Address** — IP address of the Internet connection.
- **Mode** — Shows if the IP address is a static setting or set by DHCP.

- **IPv6 Address** — The IPv6 address of the Internet connection.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

The following items are displayed in the “Device Info” section:

- **Firmware** — The software version number.
- **Serial Number** — The serial number of the physical access point.
- **System MAC** — The system MAC address of the access point.
- **MTU** — The maximum transmission unit for packets sent on the network.
- **Uptime** — Length of time the management agent has been up.
- **Load Average** — The last 1-minute, 5-minute and 15-minute CPU load average.
- **Memory Used** — The percentage of memory being used.

The following items are displayed in the “Interface Info” section:









- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the WAN (that is, the Internet).
- **Routed Ports** — By default, all interfaces are configured as a member of the LAN. Traffic from these interfaces is routed across the access point through Ethernet Port 0 to the Internet. (This is also called route to Internet.)

Network Status

The Network Status section shows information about local network connections.

Figure 17: Local Networks

LOCAL NETWORKS

NAME	NETWORK INFO	DHCP SERVER	MEMBERS
 Default Local Network	192.168.2.1 (Static IP) Netmask: 255.255.255.0	 Enabled	 ETH1  ETH2  5 GHz: EAP101-EC2107004231  5 GHz: EC2107004231  2.4 GHz: EAP101-EC2107004231  2.4 GHz: EC2107004231
View ARP Table		View DHCP Leases	

Copyright © 2021, Edge-core Networks

The following items are displayed in this section:

- **Name** — Shows information on the name of the local network.
- **Network Info** — Shows whether the local network uses static or dynamic configuration, and the network mask.
- **DHCP Server** — Shows if DHCP service is enabled on this network.
- **Members** — Shows the ports and wireless radios attached to this network. (Click on any of these interfaces to open the corresponding configuration page.)
- **View ARP Table** — Shows the ARP cache.

Figure 18: ARP Table

ARP TABLE			
IP Address	MAC Address	Mask	Device
10.2.78.152	0c:9d:92:5c:b0:6b	*	br-wan
10.2.78.38	8c:84:01:83:62:72	*	br-wan
10.2.78.50	54:e1:ad:51:47:c9	*	br-wan
192.168.2.9	00:e0:4c:68:12:66	*	br-lan
10.2.78.254	ec:9b:8b:c7:b1:81	*	br-wan
10.2.78.79	a8:5e:45:d2:8c:22	*	br-wan
10.2.78.146	d4:5d:64:59:78:9d	*	br-wan
10.2.78.127	20:d1:60:ff:30:c6	*	br-wan
Refresh			

- **View DHCP Leases** — Shows DHCP leases.

Figure 19: Active DHCP Leases

DHCP LEASES

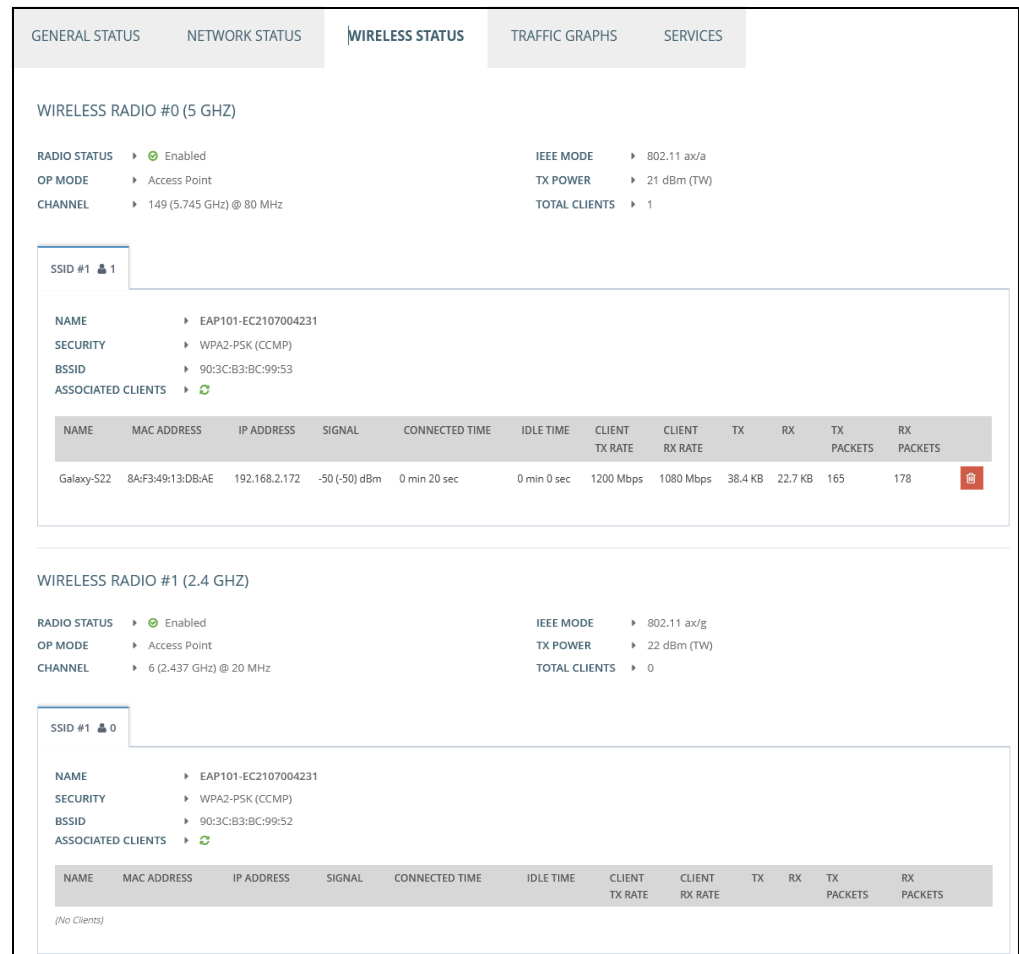
NO.	Expires	MAC Address	IP Address	Client Name	Client Id
1	11h 59m 42s	BC:3D:85:F6:58:4B	192.168.2.181	HUAWEI_Mate_10- a2784e31da	01:BC:3D:85:F6:58:4B

Refresh

Wireless Status

The Wireless Status section shows information about the radio settings and associated clients.

Figure 20: Wireless Status



Note that you can click the red button next to an associated client to force disconnection.

The following items are displayed in this section:

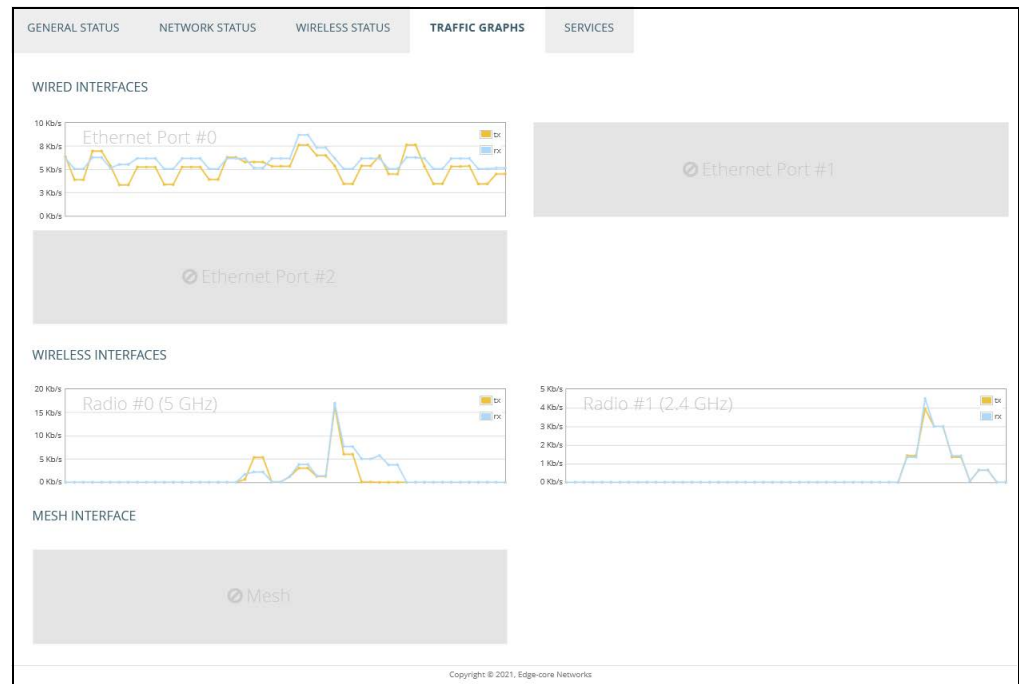
- **Wireless Radio 5 GHz/2.4 GHz** — Indicates the 2.4 GHz or 5 GHz wireless interface.
- **Radio Status** — Shows if the wireless interface is enabled or disabled.
- **IEEE Mode** — The 802.11 wireless LAN standards supported by the AP.
- **Op Mode** — Shows if the wireless interface is configured to operate in an access point mode or client mode.

- **Tx Power** — The power of the radio signals transmitted from the AP.
- **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode, Channel Bandwidth, and Country Code settings.
- **Total Clients** — The total number of clients attached to this interface.
- **SSID #** — Service set identifier. Clients that want to connect to the wireless network through an access point must set their SSIDs to the same as that of the access point.
 - **Name** — A unique identifier for the local wireless network.
 - **Security** — Shows whether or not security has been enabled.
 - **BSSID** — The basic service set identifier. This is the MAC address of the AP generated by combining the 24 bit Organization Unique Identifier (OUI, the manufacturer's identity) and the manufacturer's assigned 24-bit identifier for the radio chipset in the AP.
- **Associated Clients** — Shows detailed information about associated wireless clients.
 - **Name** — Client name.
 - **MAC Address** — The MAC address of the wireless client.
 - **IP Address** — The IP address assigned to the wireless client.
 - **Signal** — The signal strength (TX/RX) in dBm.
 - **Connected Time** — The time the wireless client has been associated.
 - **Idle Time** — The time the wireless client has been inactive.
 - **Client TX Rate** — The data transmit rate to the wireless client.
 - **Client RX Rate** — The data receive rate from the wireless client.
 - **TX** — The number of bytes transmitted to the wireless client.
 - **RX** — The number of bytes received from the wireless client.
 - **TX Packets** — The number of packets transmitted to the wireless client.
 - **RX Packets** — The number of packets received from the wireless client.

Traffic Graphs

The Traffic Graphs section shows the data rate for the Ethernet ports, wireless interfaces, and mesh interface.

Figure 21: Traffic Graphs



Services

The Services section shows the status of the Edgecore cloud management agent.

Figure 22: Services

GENERAL STATUS	NETWORK STATUS	WIRELESS STATUS	TRAFFIC GRAPHS	SERVICES
SERVICES				
NAME	STATUS	MORE INFO		
Edge-core Networks Cloud Agent Status	⊗ Disabled	The cloud agent (mgmtd) is currently disabled. Go to system settings to enable it.		
Hotspot (Chilli)	⊗ Disabled	The hotspot service is currently disabled. Included interfaces: <i>(no interfaces)</i>		
Edge-core Networks EWS-Series Controller	⊗ Disabled	The capwap service is currently disabled. Go to system settings to enable it.		

- **Edge-core Networks Cloud Agent Status** — Shows whether or not the agent for the cloud controller is enabled.

- **Hotspot (Chilli)** — Shows whether or not hotspot services are enabled. Click on this field to open the Hotspot Settings menu.
- **Edge-core Networks EWS-Series Controller** — Shows if the CAPWAP service is enabled for management of the AP through an EWS-Series controller.

3

Network Settings

This chapter describes basic network settings on the access point. It includes the following sections:

- [“Internet Settings” on page 42](#)
- [“Ethernet Settings” on page 45](#)
- [“LAN Settings” on page 48](#)
- [“Firewall Rules” on page 50](#)
- [“Port Forwarding” on page 51](#)
- [“Hotspot Settings” on page 52](#)
- [“DHCP Snooping” on page 57](#)
- [“ARP Inspection” on page 58](#)
- [“DHCP Relay” on page 59](#)

Internet Settings

The Internet Settings page configures the basic Internet settings for the AP, such as the source port, IP aliases, as well as the host name and maximum MTU size.

Figure 23: Internet Settings

Internet Settings

IP Address Mode: DHCP

MTU Size: 1500

Fallback IP: 192.168.1.10

Fallback Netmask: 255.255.255.0

Manual DHCP Client Id: YES

Hostname: Edge-core

VLAN Tag: OFF

Mgmt VLAN: OFF

The following items are displayed on this page:

- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP, PPPoE)
- **DHCP** — Configuration options displayed for DHCP are shown in [Figure 23](#).
 - **Fallback IP** — This IP address is used if the DHCP service is unavailable or fails. (Default: 192.168.1.10)
 - **Fallback Netmask** — The network mask associated with the fallback IP address. (Default: 255.255.255.0)
 - **Manual DHCP Client Id** — An option to manually enter the hostname for the DHCP client.

Figure 24: IP Address Mode – Static IP

The screenshot shows the 'Internet Settings' configuration page. At the top, the title 'Internet Settings' is displayed. Below it, the 'IP Address Mode' is set to 'Static IP' via a dropdown menu. The 'MTU Size' is set to 1500. The 'IP Address' field contains '192.168.1.1'. The 'Subnet Mask' is set to '255.255.255.0' via a dropdown menu. The 'Default Gateway' field contains '192.168.1.254'. The 'DNS Servers' field contains '8.8.8.8'. At the bottom, there are two toggle switches: 'VLAN Tag' and 'Mgmt VLAN', both of which are currently turned off (labeled 'OFF').

- **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.
 - **IP Address** — Specifies an IP address for the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
 - **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
 - **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

If you have management stations, DNS, RADIUS, or other network servers located on another subnet, type the IP address of the default gateway router in the text field provided.
 - **DNS Servers** — The IP address of Domain Name Servers on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

If you have a DNS servers located on the local network, type the IP address in the text fields provided.

Figure 25: IP Address Mode – PPPoE

The screenshot shows the 'Internet Settings' configuration page. At the top, the title 'Internet Settings' is displayed. Below it, the 'IP Address Mode' is set to 'PPPoE' in a dropdown menu. The 'MTU Size' is set to '1500' in a text input field. The 'Service Name' is an empty text input field. The 'Username' is an empty text input field. The 'Password' is an empty text input field with an eye icon for toggling visibility. The 'VLAN Tag' is a toggle switch set to 'OFF'. The 'Mgmt VLAN' is a toggle switch set to 'OFF'.

- **PPPoE** — To obtain an IP address for the selected Ethernet interface using PPPoE, the following items must be specified.
 - **Service Name** — The service name assigned for the PPPoE connection. The service name is normally optional, but may be required by some service providers. (Range: 1-32 alphanumeric characters)
 - **User Name** — The user name specified by the service provider. (Range: 1-32 characters)
 - **Password** — The password specified by the service provider. (Range: 1-32 characters)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)
- **VLAN Tag** — Enable to activate tagging on this port and choose a tagging ID value between 2 and 4094, inclusive.
- **Mgmt VLAN** — Select this option to enable a management VLAN on this device. Once you enable this option, you will no longer be able to access this device on any of built-in the local networks (like 192.168.2.1 for example). You will only be able to access the device from the specified VLAN network. If this device's IP mode is set to DHCP, it will also request a new IP address in the subnet range assigned to the VLAN network.

IPv6 Settings Enables you to configure the method used to provide an IPv6 address for the Internet access port.

Figure 26: IPv6 Settings



The following items are displayed on this section of the page:

- **IP Address Mode** — The method used to provide an IPv6 address for the Internet access port. (Default: DHCP; Options: DHCP, Static IP)
 - **DHCP** — If you configure DHCP, the Client Id must be specified.
 - **Client Id** — Manually enter the client ID for the DHCP client.
- **Static IP** — To configure a static IPv6 address for the Internet access port, the following items must be specified.
 - **IP Address** — Specifies an IPv6 address for the access point. An IPv6 address must be configured according to RFC 2373 using 8 colon separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
 - **Default Gateway** — The IPv6 address of the default gateway, which is used if the requested destination address is not on the local subnet.
 - **DNS** — The IPv6 address of Domain Name Servers on the network. A DNS maps numerical IPv6 addresses to domain names and can be used to identify network hosts by familiar names instead of the IPv6 addresses. If you have a DNS server located on the local network, type the IPv6 address in the text field provided.

Ethernet Settings

The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection for wireless clients attached to the local network (routed to the Internet), or is bridged directly to the Internet.

The following items are common for all pages under Ethernet Settings:

- **Ethernet Port #0** — Shows the status of the WAN Ethernet port.
- **Ethernet Port #1** — Shows the status of the LAN Ethernet port 1.

- **Ethernet Port #2** — Shows the status of the LAN Ethernet port 2.

Figure 27: Ethernet Settings – Internet Source

Ethernet Settings

Ethernet Port #0 Ethernet Port #1 Ethernet Port #2

i This interface is the internet source for this product. Configure Internet Settings

Save & Apply Save Reset

The following status message is displayed if an interface is set as the Internet source:

- “This interface is the internet source for this product. [Configure Internet Settings](#)”

If more than one interface is connected to the Internet, only the last configured interface is used.

Figure 28: Ethernet Settings – Network Behavior

Ethernet Settings

Ethernet Port #0 Ethernet Port #1 Ethernet Port #2

Network Behavior Route to Internet

Network Name Default local network

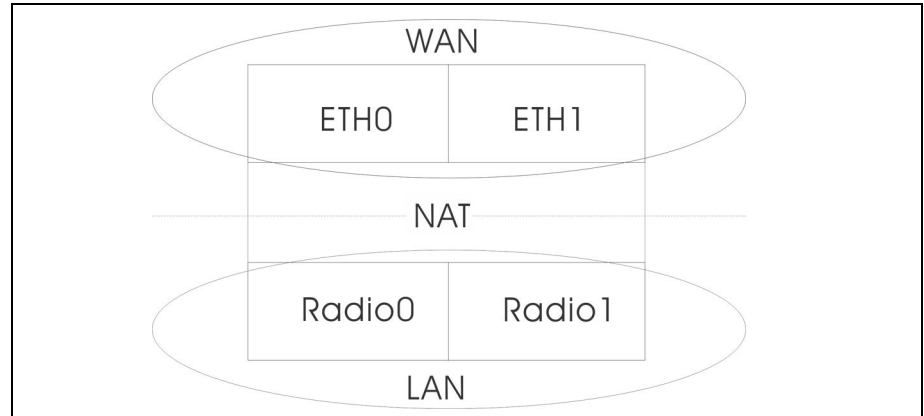
CAPWAP Tunnel Interface Disable

The following items are displayed on this page:

- **Network Behavior** — For the Ethernet port which is not providing Internet access, one of the following connection methods must be specified. (Default: Route to Internet)
 - **Bridge to Internet** — Configures an interface to be attached to the WAN. Traffic from this interface is directly bridged into the Internet. If an Ethernet port is bridged to the Internet, management access cannot be made by a direct connection to this port. However, if another Ethernet port or radio interface is within the LAN (routed to the Internet) the access point can be managed through this interface by a PC which is configured with an IP address in the same subnet.

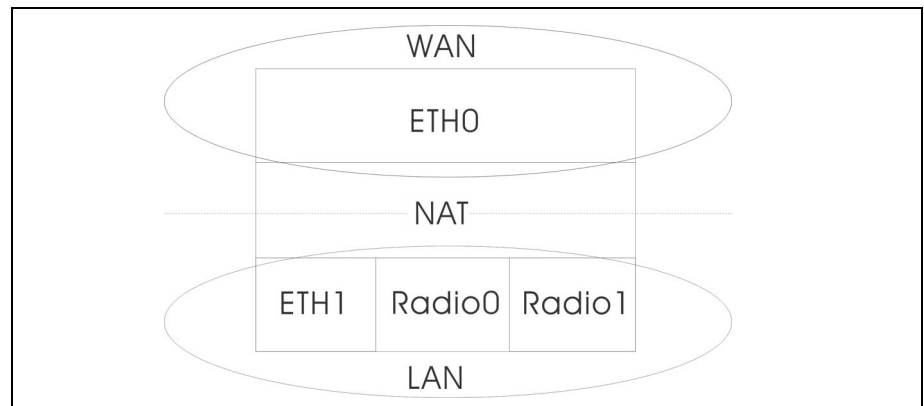
In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN.

Figure 29: Bridge to Internet



- **Route to Internet** — Configures an interface to be a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged directly to the Internet. By default, Ethernet Port 1 is routed to Internet, allowing management access via a direct connection to a PC configured with an address in the same subnet.

Figure 30: Route to Internet



- **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.
- **Add to Guest Network** — This port can only support the guest network.
- **Hotspot Controlled** — This port can only access hotspot services. Click the link to open the Hotspot Settings page. See ["Hotspot Settings" on page 52](#).
- **VLAN Tag Traffic** — This port transmits tagged traffic from a specified VLAN. Select the VLAN ID from the configured list, or click the link to open the Wireless VLAN Settings page and create a VLAN ID. See ["VLAN Settings" on page 76](#).

- **PoE Out** — (EAP104 only) Enables the PoE Out feature when the PoE source is detected as 802.3at, otherwise the PoE Out feature is disabled. When set to “Off,” PoE Out is always disabled. (Default: On)
- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see [“System Settings” on page 79](#)), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured for the Ethernet port from the controller template. The options are “Disable” or “Complete.” A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. (Default: Disable)

LAN Settings

The LAN Settings page configures the LAN settings for the local and guest networks, including IP interface setting, DHCP server settings, and STP administrative status.

Figure 31: Network – LAN Settings

The screenshot displays the 'LAN Settings' page with two main sections: 'Default Local Network' and 'Default Guest Network'. Both sections have an 'ON' toggle in the top right corner.

Default Local Network:

- Members:** ETH1, ETH2, 5 GHz: EAP101-EC2107004231, 5 GHz: EC2107004231, 2.4 GHz: EAP101-EC2107004231, 2.4 GHz: EC2107004231
- IP Address:** 192.168.2.1
- Subnet Mask:** 255.255.255.0
- MTU Size:** 1500
- DHCP Server:** ON
- DHCP Start:** 100
- DHCP Limit:** 150
- DHCP Lease Time:** 12hr
- Custom DHCP DNS Servers:** (Empty field)
- STP:** OFF
- UPnP:** OFF
- Smart Isolation:** Disable (full access) v

Default Guest Network:

- Members:** (None)
- IP Address:** 192.168.3.1
- Subnet Mask:** 255.255.255.0
- MTU Size:** 1500
- DHCP Server:** ON
- DHCP Start:** 100
- DHCP Limit:** 150
- DHCP Lease Time:** 12hr
- Custom DHCP DNS Servers:** (Empty field)
- STP:** OFF
- UPnP:** OFF
- Smart Isolation:** Internet access only v

The following items are displayed on this page:

- **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network. (Range: 1400-1500 bytes; Default 1500 bytes)
- **DHCP Server** — Enables/disables DHCP on this network. (Default: Enabled)
 - **DHCP Start** — First address in the address pool. (Range: 1-256; Default: x.x.x.100)
 - **DHCP Limit** — Maximum number of addresses in the address pool. (Range: 1-254; Default: 150)
 - **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client.
 - **Custom DHCP DNS Servers** — Specify the addresses or hostnames of custom DNS servers to be used.
- **STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- **UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- **Smart Isolation** — Enables network traffic to be restricted to the specified network:
 - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN.
 - **Internet access only** — Traffic from this network can only be routed to and from the Internet.
 - **LAN access only** — Traffic from this network is restricted to local LAN devices only.
 - **Internet access strict** — Traffic from this network can only be routed to and from the Internet, but with the additional restriction that users cannot access resources or devices on any private network (such as 192.168.0.0, 172.16.0.0, 10.0.0.0 etc.).
- **Add Custom LAN** — Click this button to create additional networks with their own custom settings. You can create up to 5 custom LANs.

Firewall Rules

Firewall filtering restricts connection parameters to limit the risk of intrusion. The firewall settings allow you to define a sequential list of rules that filter traffic based on source and destination IP addresses and ports. Ingress packets are tested against the filter rules one by one. As soon as a packet matches a rule, the configured target action is implemented.

One rule, “Allow-Ping,” is pre-configured to allow Ping packets from the Internet. You can enable or disable this rule, but it cannot be modified or deleted. Click the “Add new” button to add a new firewall rule.

Figure 32: Firewall Rules

Firewall Rules

+ Add new

Enabled	Name	Target	Family	Source	Source IP	Source port	Protocol	Destination	Destination IP	Destination port	
<input checked="" type="checkbox"/>	Allow-Ping	ACCEPT	IPv4	Internet			ICMP	Any			

Save & Apply Save Reset

The following items are displayed on this page:

- **Enabled** — Enables or disables the rule.
- **Name** — A user-defined name for the filtering rule. (Range: 1-30 characters)
- **Target** — The action to take when a packet is matched. (Options: Accept, Reject, Drop, Mark, Notrack; Default: Accept)
 - **Accept** — Accepts matching packets.
 - **Reject** — Drops matching packets and returns an error packet in response.
 - **Drop** — Drops matching packets.
 - **Mark** — Matched packets are associated with a mark value for specific processing or routing by the AP.
 - **Notrack** — Disables connection tracking for packets matching the rule. Disabling packet tracking conserves resources within the AP.
- **Family** — The IP address family. (Options: Any, IPv4; Default: Any)
- **Source** — The source interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)

- **Source IP** — The source IPv4 address in CIDR notation. Includes an IPv4 address followed by a slash (/) and a decimal number to define the network mask.
- **Source port** — The source protocol port. (Range: 0-65535)
- **Protocol** — The protocol type. (Options: Any, TCP+UDP, TCP, UDP, ICMP; Default: TCP+UDP)
- **Destination** — The destination interface. (Options: Guest Network, Hotspot Network, Default Local Network, Internet, Any)
- **Destination IP** — The destination IP address.
- **Destination port** — The destination protocol port. (Range: 0-65535)

Port Forwarding

Port Forwarding can be used to map an inbound protocol type (TCP/UDP) and port to an "internal" IP address and port. The internal (local) IP addresses are the IP addresses assigned to local devices at the edge of a network, and the external IP address is the IP address assigned to the AP interface. This allows remote users to access different servers on your local network using your single public IP address.

Remote users accessing services such as web or FTP at your local site through your public IP address, are redirected (mapped) to other local server IP addresses and TCP/UDP port numbers. For example, if you set Type/Public Port to TCP/80 (HTTP or web) and the Private IP/Port to 192.168.3.9/80, then all HTTP requests from outside users are forwarded to 192.168.3.9 on port 80. Therefore, by just using your external IP address provided by your ISP, Internet users can access the services they need at the local addresses to which you redirect them.

Figure 33: Port Forwarding

Port forwarding

[+ Add new](#)

Enabled	Name	Protocol	External port	Internal IP address	Internal port	
<input checked="" type="checkbox"/>	web service	TCP	80	192.168.3.9	80	

[Save & Apply](#) [Save](#) [Reset](#)

The following items are displayed on this page:

- **Enabled** — Enables port forwarding.
- **Name** — User defined name. (Range: 1-30 characters)

- **Protocol** — Set the protocol to which port forwarding is applied. (Options: TCP, UDP, TCP+UDP)
- **External Port** — The TCP/UDP port number. (Range: 1-65535)

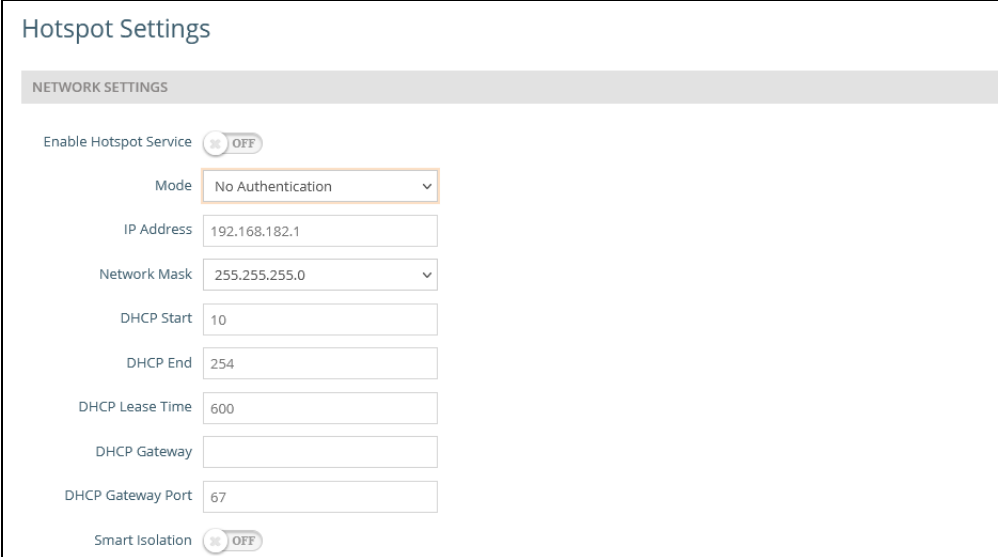
The more common TCP service port numbers include: HTTP: 80, FTP: 21, Telnet: 23, and POP3: 110.
- **Internal IP address** — The internal destination IP address.
- **Internal Port** — The internal destination protocol port. (Range: 1-65535)

Hotspot Settings

The Hotspot Settings page can configure Internet access to the general public in places such as coffee houses, libraries and hospitals. Specific access rights may also be defined through a RADIUS server.

Network Settings This section includes the option to enable or disable hotspot service, hotspot mode options, and network settings.

Figure 34: Hotspot Settings (Network Settings)



Hotspot Settings

NETWORK SETTINGS

Enable Hotspot Service ☐ OFF

Mode

IP Address

Network Mask

DHCP Start

DHCP End

DHCP Lease Time

DHCP Gateway

DHCP Gateway Port

Smart Isolation ☐ OFF

The following items are displayed on this page:

- **Enable Hotspot Service** — Enables or disables hotspot service. A hotspot is a physical location where people may obtain Internet access, typically using Wi-Fi technology, via a wireless local area network using a router connected to an Internet service provider.

- **Mode** — Hotspot service types include the following options:
 - **External Captive Portal Service** — This option will show the hotspot guest an externally hosted captive portal splash page and may prompt them to login, depending on how you've configured your service settings. Choose this option if you've signed up with a third-party captive portal service provider such as Cloud4Wi or HotSpotSystem.
 - **No Authentication** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will not require the guest to login before accessing the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.
 - **Simple Password-Only Splash Page** — This option will show the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a simple password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.
 - **Local Spash Page with External RADIUS** — This option shows the hotspot guest your customized, locally hosted captive portal splash page, and will require them to enter a valid RADIUS username and password to login and access the Internet. If you fill out the (optional) terms of service text, the guest will be required to accept these before they can access the Internet.
- **Network IP** — Specifies the IP address for the hotspot. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)

If your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.

- **Network Mask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)
- **DHCP End** — Ending number of (last numeric field) in address pool. (Range: 1-254; Default: 254)
- **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 600 seconds)
- **DHCP Gateway** — Configure the DHCP gate IP address if you want to use an external DHCP server instead of the internal one.

- **DHCP Gateway Port** — The listening port used by the DHCP gateway.
- **Smart Isolation** — Activate to prevent Hotspot users to possibly access WAN resources.

RADIUS Server

If you click set the mode to External Captive Portal Service or Local Splash page with External RADIUS, the following section is displayed.

Figure 35: Hotspot Settings (RADIUS Settings)

RADIUS SETTINGS

Enable RADIUS Auth ☒

RADIUS Server 1

RADIUS Server 2

RADIUS Shared Secret

RADIUS Auth Port

RADIUS Acct Port

Enable RadSec ☐

RADIUS Auth Method

Local ID

Local Name

NAS ID

The following items are displayed on this page:

- **Enable RADIUS Auth** — Enables or disables client authentication via a RADIUS server.
- **RADIUS Server 1** — IP address or host name of the primary RADIUS server.
- **RADIUS Server 2** — IP address or host name of the secondary RADIUS server.
- **RADIUS Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- **RADIUS Auth Port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- **RADIUS Acct Port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- **Enable RadSec** — An authentication and authorization protocol for transporting RADIUS datagrams over TCP and TLS. RadSec replaces UDP used

in the initial RADIUS design, providing a reliable transport protocol and more extensive security for the packet payload.

- **RADIUS Auth Method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MSCHAPv2. The encryption method must match that used by the RADIUS server.
- **Local ID** — Local RADIUS server identifier.
- **Local Name** — Local RADIUS server name
- **NAS ID** — Local RADIUS server operation identifier.

Captive Portal Settings

The following section is displayed for all hotspot mode options.

Figure 36: Hotspot Settings (Captive Portal Settings)

CAPTIVE PORTAL SETTINGS

HTTPS ON

HTTPS Domain

Captive Portal URL

Captive Portal Secret

Session Timeout

Idle Timeout

Landing URL

Swap Octets OFF

Walled Garden

Enter a list of space or newline-delimited hostnames and IPs.
Example: 203.211.150.204 66.235.128.0/17 www.paypal.com

Auth White List

Enter a list of space or newline-delimited MAC addresses.
Example: 00:11:22:33:44:55 55:44:33:22:11:00

The following items are displayed on this page:

- **HTTPS** — Enables HTTPS for the captive portal. (Default: Disabled)



Note: To upload a unique security certificate from a trusted certification authority for the HTTPS captive portal, see [“Upload Certificate” on page 84](#).

- **HTTPS Domain** — The domain name of the HTTPS captive portal.

- **Captive Portal URL** — Host name of Internet service portal for the hotspot.

The captive portal forces a hotspot client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.

- **Captive Portal Secret** — The password used for logging into the hotspot.
- **Customize Splash Page** — This option is shown for all hotspot service options other than External Captive Portal Service. If enabled, fill in information for the title, background color, logo image file, and optional terms and conditions.
- **Session Timeout** — The maximum time a client can stay attached to the hotspot. (Range: 0-86400 seconds)
- **Idle Timeout** — The maximum a connection can remain inactive before it is closed. (Range: 0-86400 seconds)
- **Landing URL** — Indicates the URL to which the user is directed after logging in to the captive portal.
- **Swap Octets** — Swap the values of the reported “input octets” and “output octets.” This option only appears under External Captive Portal Service.
- **Walled Garden** — A list of web sites to which unauthenticated users are allowed to navigate.
- **Auth White List** — A list of MAC addresses that are allowed to bypass the captive portal to access the Internet.

DHCP Snooping

DHCP snooping is used to validate and filter DHCP messages received by the AP. When DHCP snooping is enabled, DHCP messages received from a device not listed in the DHCP snooping table are dropped.

You can add known and trusted DHCP servers to the table by specifying their MAC and IP addresses.

Figure 37: DHCP Snooping

Trust DHCP Server MAC	Trust DHCP Server IP	Remark
0:11:22:33:44:55	10.1.2.3	

The following items are displayed on this page:

- **Enable DHCP Snooping** — Enables DHCP Snooping on the AP.
- **Trust DHCP Server MAC** — The MAC address of a known and trusted DHCP server.
- **Trust DHCP Server IP** — The IP address of a known and trusted DHCP server.
- **Remark** — A comment relating to the DHCP server configured.

ARP Inspection

ARP Inspection is a security feature that validates the MAC Address bindings for Address Resolution Protocol packets. It provides protection against ARP traffic with invalid MAC-to-IP address bindings, which forms the basis for certain “man-in-the middle” attacks. This is accomplished by intercepting all ARP requests and responses and verifying each of these packets before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

Figure 38: ARP Inspection

ARP Inspection

ARP Inspection ☒

Force DHCP ☒

Trust List Broadcast ☒

Static Trust List ☒

+ Add new

MAC	IP	State
00:11:22:33:44:55	10.2.3.4	YES (II)

Save & Apply Save Reset

The following items are displayed on this page:

- **ARP Inspection** — When enabled, ARP packets are validated against ARP spoofing.
- **Force DHCP** — Allows the AP to only learn MAC/IP pair information through DHCP packets. Since devices configured with static IP address do not send DHCP traffic, any clients with static IP addresses will be blocked by the AP unless their MAC/IP pair is listed and enabled in the Static Trust List.
- **Trust List Broadcast** — Lets other APs learn the trusted MAC/IP pairs to issue ARP requests.
- **Static Trust List** — Adds the MAC or MAC/IP pairs of devices that are trusted to issue ARP requests. Other network nodes can still send their ARP requests, but if their IP appears in the static list with a different MAC, their ARP requests will be dropped.

DHCP Relay

When DHCP relay is enabled, the AP acts as an agent for all clients and sends all broadcast DHCP requests directly to a specified DHCP server. The DHCP server IP address and port must be configured, and optionally a backup server.

With DHCP relay enabled, the circuit ID can be set on the VLAN settings or LAN settings page. IP addresses of clients are then obtained by the DHCP relay server and the IP range is determined by the remote ID and circuit ID.

Figure 39: DHCP Relay



DHCP Relay

Enable DHCP Relay ☒ ON

DHCP Relay Server

DHCP Relay Port

Backup DHCP Relay ☐ OFF

Remote ID

The following items are displayed on this page:

- **Enable DHCP Relay** — Enables the DHCP relay feature on the AP.
- **DHCP Relay Server** — Specifies the IP address of the DHCP server.
- **DHCP Relay Port** — Specifies the port of the DHCP server.
- **Backup DHCP Relay** — Optionally specifies a backup DHCP server IP address and port to use if there is no response from the primary server.
- **Remote ID** — Use the hostname as the remote ID, or manually configure a text string as the remote ID.

4

Wireless Settings

This chapter describes the wireless settings on the access point. It includes the following sections:

- [“Radio Settings” on page 61](#)
- [“VLAN Settings” on page 76](#)

Radio Settings

The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

The access point can operate in several radio modes, 802.11b+g+n/ax (2.4 GHz) or 802.11a/a+n/ac+a+n/ax (5 GHz). Note that the dual-band access points can operate at 2.4 GHz and 5 GHz at the same time. The web interface identifies the radio configuration pages as:

- **Radio 5 GHz** — the 5 GHz 802.11a/n/ac/ax radio interface
- **Radio 2.4 GHz** — the 2.4 GHz 802.11b/g/n/ax radio interface

Each radio supports 16 virtual access point (VAP) interfaces based on the SSIDs, referred to as SSID1 ~ SSID16. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. However, most radio signal parameters apply to all VAP interfaces. Traffic to specific VAPs can be segregated based on user groups or application traffic. The clients associate with each VAP in the same way as they would with separate physical access points.

Physical Radio Settings **Figure 40: Physical Settings for Radio 5 GHz**

PHYSICAL RADIO SETTINGS

Status: ☒ ON

Mode: Access Point (Auto-WDS)

802.11 Mode: 802.11ax

Channel Bandwidth: 80MHz

Channel: Auto

WME Configure: Configure

Beacon Interval: 100

Bandsteering: ☐ OFF

Airtime Fairness: ☐ OFF

Minimum signal allowed: 30

BSS coloring: 64

Interference Detection: 0

OFDMA: ☒ ON

Target Wake Time: ☐ OFF

Multicast/Broadcast Rate: 6M

Figure 41: Physical Settings for Radio 2.4 GHz

PHYSICAL RADIO SETTINGS

Status ☒ ON

Mode

802.11 Mode

Channel Bandwidth

Channel

WME Configure

Beacon Interval

Bandsteering ☐ OFF

Airtime Fairness ☐ OFF

Minimum signal allowed

BSS coloring

Interference Detection

OFDMA ☒ ON

Target Wake Time ☐ OFF

Multicast/Broadcast Rate

The following items are displayed on this page:

- **Status** — Enables or disables the wireless service on this interface.
- **Mode** — Selects the mode in which the AP will function.
 - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)

In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.
 - **Client** — The AP can provide a wireless connection to another AP, as well as pass information from or to locally wired hosts and wireless clients.
- **802.11 Mode** — Defines the radio operation mode.
 - **Radio 5 GHz** — Default: 11ax; Options: 11a, 11a+n, 11ac+a+n, 11ax
 - **Radio 2.4 GHz** — Default: 11ax; Options: 11b+g+n/ax

- **Channel Bandwidth** — The AP options for channel bandwidth include 20, 40 and 80 MHz. The available channel bandwidth is dependent on the 802.11 Mode. (Default: 20 MHz on 2.4 GHz Radio, 80 MHz on 5 GHz Radio; Options: 20 MHz, 40 MHz, 80MHz, 160MHz)
 - **20MHz** — For 802.11b+g+n and 802.11ax
 - **40MHz** — For 802.11b+g+n, 802.11a, 802.11a+n, 802.11ac+a+n and 802.11ax
 - **80MHz** — For 802.11ac+a+n and 802.11ax
 - **160MHz** — (Supported on EAP104 5 GHz radio only) For 802.11ac+a+n and 802.11ax
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, for 11g/n 20 MHz mode you can deploy up to three access points in the same area using channels 1, 6, 11. Note that wireless clients automatically set the channel to the same as that used by the access point to which it is linked. (The available channels are dependent on the 802.11 Mode, Channel Bandwidth, and Country Code settings.)
Selecting Auto enables the access point to automatically select an unoccupied radio channel. (Default: Auto)
- **WME Configuration** — Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM), is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features for IEEE 802.11 networks. Access priority can be configured for four “Access Category”(AC) types using the following parameters:
 - **CW Min (Minimum Contention Window)** – The initial upper limit of the random backoff wait time before wireless medium access can be attempted. The initial wait time is a random value between zero and the CWMin value. Specify the CWMin value in the range 0-15 microseconds. Note that the CWMin value must be equal or less than the CWMax value.
 - **CW Max (Maximum Contention Window)** – The maximum upper limit of the random backoff wait time before wireless medium access can be attempted. The contention window is doubled after each detected collision up to the CWMax value. Specify the CWMax value in the range 0-15 microseconds. Note that the CWMax value must be greater or equal to the CWMin value.
 - **AIFS (Arbitration Inter-Frame Space)** – The minimum amount of wait time before the next data transmission attempt. Specify the AIFS value in the range 0-15 microseconds.

- **TXOP Limit (Transmit Opportunity Limit)** — The maximum time an AC transmit queue has access to the wireless medium. When an AC queue is granted a transmit opportunity, it can transmit data for a time up to the TXOP Limit. This data bursting greatly improves the efficiency for high data-rate traffic. Specify a value in the range 0-8192 microseconds.
- **Beacon Interval** — The rate at which beacon signals are transmitted from the access point. The beacon signals allow wireless clients to maintain contact with the access point. They also carry power-management and other information. (Range: 100-1024 TUs; Default: 100 TUs)
- **Bandsteering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs and security settings that match for this feature to fully operate. (Default: Off)
- **Airtime Fairness** — Enabling this feature improves the overall performance of the wireless network. (Default: Disabled)
- **Minimum signal allowed** — Only allows clients to connect to the radio interface if their signal strength (SNR) is equal or greater than the specified value. Setting the value to zero disables this feature. (Range: 0-99; Default: 30)
- **BSS coloring** — In 802.11ax (Wi-Fi 6) mode, BSS coloring allows nearby APs operating at the same frequency to identify traffic belonging to their own Basic Service Set (BSS). The BSS coloring enables Wi-Fi 6 networks to operate more efficiently in high-density environments where neighboring AP and client transmissions overlap. Assign a color value (a number from 1 to 63) to identify the radio BSS, or enter value 64 to allow the AP to randomly select a color value. (Range: 1-63, 64 random; Default: 64)
- **Interference Detection** — When the utilization in current channel reaches the configured threshold (as a percentage), the AP switches to a different channel. (Range: 0 - 100%; Default: 0, disabled)
- **OFDMA** — The 802.11ax (Wi-Fi 6) mode supports Orthogonal Frequency Division Multiple Access (OFDMA) and this cannot be disabled.
- **Target Wake Time** — In 802.11ax (Wi-Fi 6) mode, the AP can allow clients to request a specific Target-Wakeup Time (TWT) to transmit or receive frames, rather than rely on periodic beacons. This feature enables client devices to have much longer sleep states and results in significant power savings. In addition, the AP can control and schedule client TWTs to both manage contention in the network and accommodate delay-sensitive traffic. (Default: Disabled)
- **Multicast/Broadcast Rate** — Allows a limit to be placed on the wireless bandwidth consumed by multicast and broadcast packets.

- **Radio 5 Ghz** — Options: 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 6M
- **Radio 2.4 Ghz** — Options: 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; Default: 5.5M

Wireless Networks — **Figure 42: Radio Settings (General Settings)**
General Settings

The screenshot displays the 'WIRELESS NETWORKS' section with an 'Add' button. Below it, two tabs are visible: 'EAP101-EC2107004231 (SSID1)' and 'EC2107004231 (SSID2)'. The 'GENERAL SETTINGS' section includes the following controls:

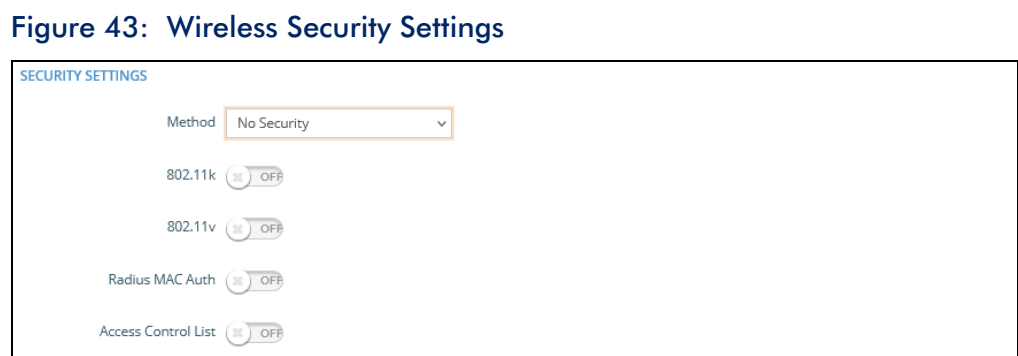
- Status:** A toggle switch set to 'ON'.
- SSID:** A text field containing 'EAP101-EC2107004231'.
- Site Survey:** A toggle switch set to 'ON'.
- Broadcast:** A checkbox that is checked.
- Local Configurable:** A toggle switch set to 'OFF'.
- Client Isolation:** A toggle switch set to 'OFF'.
- Multicast-to-Unicast Conversion:** A toggle switch set to 'ON'.
- WMM:** A toggle switch set to 'ON'.
- Max Clients:** A text field containing '127'.
- Idle Timeout (sec):** A text field containing '300'.

The following items are displayed in this section of the Wireless Settings page:

- **Status** — Enables or disables the wireless service on this VAP.
- **SSID** — The name of the basic service set provided by a Virtual Access Point (VAP) interface. Clients that want to connect to the network through the access point must set their SSID to the same as that of the access point's VAP interface. (Default: Edgecore5G-# (where # is 1-16) for 5 GHz, Edgecore2.4G-# (where # is 1-16) for 2.4 GHz; Range: 1-32 characters)
- **Site Survey** — Scans for all wireless networks that are broadcasting their SSID.
- **Broadcast** — The SSID can be broadcast at regular intervals so that wireless stations searching for a network connection can discover it. This allows wireless clients to dynamically discover and roam between WLANs. This feature also makes it easier for hackers to break into your home network. Because SSIDs are not encrypted, it is easy to grab one by snooping the WLAN looking for SSID broadcast messages coming from the AP. (Default: Enabled)
- **Local Configurable** — Enables the SSID to be user configurable when the system is operating in MSP mode (see ["System Settings" on page 79](#)). (Default: Disabled)

- **Client Isolation** — When enabled, wireless clients can talk to the LAN, and reach the Internet if such connection is available, but they cannot communicate with one another. (Default: Disabled)
- **Multicast-to-Unicast Conversion** — When enabled, the AP converts multicast traffic to unicast traffic and sends it to each associated client. This feature provides a network throughput enhancement, since the AP transmits multicast traffic at a low basic rate, whereas unicast traffic can be transmitted at HT, VHT, or HE rates.
- **Max Clients** — The maximum number of clients that can associate to this SSID at the same time. (Default: 127; Range: 1-256)
- **Idle Timeout (sec)** — The AP disconnects a client when there is no activity for the configured amount of time. (Default: 300 seconds; Range: 60-60000 seconds)

Wireless Networks — Security Settings



The following items are displayed in this section of the Wireless Settings page:

- **Method** — Sets the wireless security method for each VAP, including association mode, encryption, and authentication. (Default: WPA2-PSK)
 - **No Security** — The VAP broadcasts a beacon signal including the configured SSID. Wireless clients with an SSID setting of “any” can read the SSID from the beacon and automatically set their SSID to allow immediate connection.
 - **WPA-PSK** — For enterprise deployment, WPA requires a RADIUS authentication server to be configured on the wired network. However, for small office networks that may not have the resources to configure and maintain a RADIUS server, WPA provides a simple operating mode that uses just a pre-shared password for network access. The Pre-Shared Key mode uses a common password for user authentication that is manually entered on the access point and all wireless clients. The PSK mode uses the same TKIP packet encryption and key management as WPA in the enterprise, providing a robust and manageable alternative for small networks.

- **Encryption** — Data encryption uses one of the following methods:
 - **CCMP (AES)** — AES-CCMP is used as the multicast encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2. (This is the default setting.)
 - **Auto: TKIP + CCMP (AES)** — The encryption method used by the client is discovered by the access point.
- **Key Method** — Uses one of the following PSK methods:
 - **Single PSK** — Enables the entry of a single PSK key.

- **Key** — WPA is used to encrypt data transmitted between wireless clients and the VAP. WPA uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually distributed to all clients that want to use the network.

String length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.

- **Multiple PSK** — Enables the entry of multiple PSK keys.
 - **Multiple Keys** — Enter multiple keys, one per line. Entering a key with a specific MAC address limits the key for use by a single client. Entering a key without a MAC address enables the key to be used by all clients.

Multiple keys are supported for WPA-PSK, WPA2-PSK, and WPA3 Personal Transition security.

- **Dynamic PSK** — Enables the use of dynamic PSK keys that are periodically generated and updated by a RADIUS authentication server. The RADIUS server IP address, UDP port, and secret text string must be specified. (See “RADIUS Settings” below for details.)

Dynamic keys are supported only for WPA2-PSK security.

- **WPA2-PSK** — Clients using WPA2 with a Pre-shared Key are accepted for authentication.

WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

Refer to WPA-PSK for a description of encryption methods and the key.

- **WPA-EAP** — WPA employs a combination of several technologies to provide an enhanced security solution for 802.11 wireless networks. A RADIUS server is used for authentication, and can also be used for accounting.

Refer to WPA-PSK for a description of encryption methods.

- **RADIUS Settings** — A RADIUS server must be specified for the access point to implement IEEE 802.1X network access control and Wi-Fi Protected Access (WPA) wireless security.

In addition, you can configure a RADIUS Accounting server to receive user-session accounting information from the access point. RADIUS Accounting can be used to provide valuable information on user activity in the network.



Note: This guide assumes that you have already configured RADIUS server(s) to support the access point. Configuration of RADIUS server software is beyond the scope of this guide, refer to the documentation provided with the RADIUS server software.

- **Radius Auth Server** — Specifies the IP address or host name of the RADIUS authentication server.
- **Radius Auth Port** — The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 255 characters)
- **Backup Radius Auth** — Enables the support of a backup RADIUS authentication server.
 - **Radius Auth Server** — Specifies the IP address or host name of the backup RADIUS authentication server.
 - **Radius Auth Port** — The UDP port number used by the backup RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
 - **Radius Auth Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the backup RADIUS authentication server. Do not use blank spaces in the string. (Maximum length: 200 characters)
- **Use Radius Accounting** — Enables the support of a RADIUS accounting server.

- **Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.
- **Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)
- **Acct Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS accounting server. Do not use blank spaces in the string. (Maximum length: 200 characters)
- **Acct Interim Interval** — The time (in seconds) between each accounting update sent to the server. (Range: 60-600 seconds; Default: 60 seconds)
- **WPA2-EAP** — WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward compatibility with WPA. Therefore, WPA2 includes the same 802.1X and PSK modes of operation and support for TKIP encryption.

A RADIUS server is used for authentication, and can also be used to accounting.

Refer to WPA-PSK for a description of encryption methods.

Refer to WPA-EAP for a information on configuring the RADIUS server.

- **WPA3 Personal** — Clients using WPA3 with Simultaneous Authentication of Equals (SAE) are accepted for authentication.

WPA3 provides more robust password-based authentication called Simultaneous Authentication of Equals (SAE), which replaces Pre-Share Key (PSK) in WPA2-Personal. This technology prevents offline dictionary attacks so that data traffic can be transmitted securely.

- **WPA3 Personal Transition** — Clients using WPA3 with SAE or clients using WPA2 with PSK are accepted for authentication. The AP negotiates the supported authentication and encryption with each client before allowing access to the network.
- **WPA3 Enterprise** — An enhanced version of WPA2-EAP security that uses more robust encryption. Clients must support one of the stronger WPA3 encryption options and use Protected Management Frames (PMF) to be able to access the network. The use of IEEE 802.1X network access control and a RADIUS server is required.

Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise Transition** — Allows WPA3 and WPA2 clients to access the network. Encryption options and the use of Protected Management Frames (PMF) are negotiated with each client before allowing access to the network.

Refer to RADIUS Settings above for information on RADIUS configuration.

- **WPA3 Enterprise 192-bit** — WPA3 Enterprise security uses a standard 128-bit encryption. For a network handling more sensitive data, there is an option to use 192-bit encryption for additional protection.

Refer to RADIUS Settings above for information on RADIUS configuration.

- **OWE** — Opportunistic Wireless Encryption (OWE) is the WPA3 open network security that allows users of public Wi-Fi networks to gain secure access without using a password. OWE provides individual encryption of data communications between the AP and each client, but does not provide authentication of user identities.
- **PMF** — Protected Management Frames (PMF) provide WPA2/WPA3 security for unicast and multicast management frames between the AP and clients. The “Optional” setting allows clients that do not support PMF to access the network. The “Mandatory” setting allows only clients that support PMF to access the network. (Default: Optional)
- **802.11k** — Provides clients with information on neighbor APs when roaming. As a client is about to roam from an AP, it sends a request for a “Neighbor Report” that includes a list of available APs and associated information. The client can then quickly identify the best AP to which it can roam without having to scan all channels. (Default: Disabled)
- **802.11r** — Provides a method for fast transition roaming between APs. Before clients roam to a new AP, the initial handshake and encryption calculations are performed in advance, which results in a fast hand off without the need for re-authentication. (Default: Disabled)
- **802.11v** — Provides information to associated clients that facilitates the overall improvement of the wireless network. Also helps clients to improve battery life by setting the idle period. (Default: Disabled)
- **Radius MAC Auth** — The MAC address of the associating station is sent to a configured RADIUS server for authentication. (Default: Disabled)
- **Dynamic Authorization** — The Dynamic Authorization Extensions (DAE) to RADIUS enable a server to disconnect or change the authorization of clients that are already connected to the network. (Default: Disabled)
- **DAE Port** — The UDP port number to use for DAE messages. (Default: 3799)

- **DAE Client** — Specifies the IPv4 address of the RADIUS server.
- **DAE Secret** — The shared text string used to encrypt DAE messages between the access point and the RADIUS server.
- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)
- **Policy** — The MAC list can be configured to either allow or deny network access to specified clients. (Default: Allow all MACs on list)
- **Filtered MACs** — List of client MAC addresses.

Wireless Networks — Network Settings **Figure 44: Wireless Network Settings**

The screenshot shows the 'NETWORK SETTINGS' section of a configuration interface. It includes the following settings:

- Network Behavior:** A dropdown menu currently showing 'Bridge to Internet'.
- CAPWAP Tunnel Interface:** A dropdown menu currently showing 'Disable'.
- Proxy ARP:** A toggle switch currently turned 'ON'.
- Limit Upload:** A toggle switch currently turned 'OFF'.
- Limit Download:** A toggle switch currently turned 'OFF'.
- Authentication:** A toggle switch currently turned 'OFF'.

The following items are displayed in this section of the Wireless Settings page:

- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
 - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See [Figure 29, “Bridge to Internet”, on page 47.](#))
 - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See [Figure 30, “Route to Internet”, on page 47.](#))
 - **Network Name** — The network to be routed. The default is “Default local network” as displayed under LAN Settings – Local Network.
- **Add to Guest Network** — This interface can only support the guest network.
- **Hotspot Controlled** — This interface can only support hotspot services.

- **Configure Hotspot** — Opens Hotspot Settings page.
- **Walled Garden** — Configures the Walled Garden list on the Hotspot Settings page.
- **VLAN Tag Traffic** — Tags any packets passing from this VAP (virtual access point) to the associated Ethernet port with a VLAN ID configured under [“VLAN Settings” on page 76](#).
- **VLAN Id** — Selects the configured VLAN ID with which to tag the VAP traffic.
- **VLAN Settings** — Opens the VLAN Settings page.
- **Dynamic VLAN** — The RADIUS server provides the access point with the user VLAN information. The access point assigns the associated user to the related VLAN.
- **CAPWAP Tunnel Interface** — When the AP system management is set to EWS-Series Controller mode (see [“System Settings” on page 79](#)), the CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode can be configured. The options are “Disable,” “Complete,” or “Split.” A Complete tunnel sends all management, authentication, and data traffic from the AP back to the controller. A Split tunnel only sends the management and authentication traffic to the controller. (Default: Disable)
- **Proxy ARP** — When Proxy ARP is enabled, the AP maintains its own ARP lookup table and replies to ARP requests on behalf of downstream stations, avoiding network inefficiencies. This feature is automatically enabled when client isolation is disabled, and disabled when client isolation is enabled. The feature cannot be configured manually. Proxy ARP is supported when the network behavior is “Bridge to Internet” or “VLAN Tag Traffic.”
- **Limit Upload** — Enables rate limiting of traffic from the VAP interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)
- **Limit Download** — Enables rate limiting of traffic from the wired network as it is passed to the VAP interface. You can set a maximum rate in kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)
- **Authentication** — When the AP system management is set to ecCLOUD mode (see [“System Settings” on page 79](#)), this options authenticates the AP communications with the ecCLOUD controller. (Default: Disabled)
- **Hotspot 2.0** — Available when WPA2-EAP security is selected, Hotspot 2.0, also known as Wi-Fi Certified Passpoint, provides a standard for public-access Wi-Fi networks to support seamless roaming between wireless networks. A Hotspot 2.0 AP advertises its public Wi-Fi capabilities and services so that clients can decide if they want to connect to the network. (Default: Disabled)

- **Internet Access** — Enable if this network provides access to the Internet.
- **Access Network Type** — Select one from the predefined list.
 - **Private network** — Home and enterprise networks that unauthorized users cannot access.
 - **Private network with guest access** — A private network that provides for guest access. A typical example would be an enterprise network that offers guest access.
 - **Chargeable public network** — A network that is available to all users, but requires a fee.
 - **Free Public Network** — A network that is available to all users without any fees.
 - **Personal device network** — A network for peripheral connectivity in an ad-hoc mode. For example, a camera that connects to a printer.
 - **Emergency services only network** — A network that is dedicated for access to emergency services only.
 - **Test or experimental** — A network for tests or experimental work.
 - **Wildcard** — When selected, the AP will reply to clients regardless of the network type requested by the client query.
- **HESSID** — The Homogenous Extended Service Set Identifier (HESSID) for the Hotspot2.0 network. When configured, the HESSID (a MAC address) uniquely identifies all APs belonging to the same network.
- **Venue Group** — Identifies the general class of the venue. Select from the predefined list.
- **Venue Type** — Identifies the specific type of venue within each group.
- **Venue Name** — The name of the network venue. Multiple names can be added to the list.
- **Venue URL** — Specifies a URL that provides additional venue information to users.
- **Network Auth Type** — Specifies the authentication required for the network. Select an option from the predefined list. (Default: "Acceptance of terms and conditions")
- **Roaming Consortium List** — A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Each roaming consortium is identified by an organization

identifier (OI) that is assigned by the IEEE. An OI is often 24 bits in length, but can also be 36 bits.

- **IPv4 Address Type** — Specifies the IPv4 address type available from the network.
- **IPv6 Address Type** — Specifies the IPv6 address type available from the network
- **NAI Realm List** — The network access identifier (NAI) realm list identifies those service provider or other networks that are accessible through the AP. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred network.
- **Domain Name List** — Lists one or more domain names for the entity operating the AP. This is critical for Hotspot 2.0 network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home hotspot or a visited hotspot.
- **Cellular Network Information List (PLMN)** — Identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator.
- **Operator Friendly Name** — The name of the Hotspot 2.0 operator (in English only).
- **Operating Class** — A standard index (based on IEEE Std 802.11-2012 Annex E) that specifies the AP supported operating channels.

Wireless Networks — Open Mesh Settings

Open Mesh is a network of interconnected node APs, of which only one has a wired connection to the network (and the Internet). The other AP nodes provide wireless links to each other and some support connections to wireless clients. The mesh network not only extends wireless connectivity over a greater distance, but also provides backup links should one node in the network fail.

When setting up an AP to be a node in a mesh network, select one radio interface (2.4 GHz or 5 GHz) and configure it to operate on a specific channel (do not select Auto). Set up other AP nodes to operate on the same radio interface, channel, and with the same SSID.

Figure 45: Open Mesh Settings

The following items are displayed in this section of the Wireless Settings page:

- **Mesh Point** — Enables Open Mesh support on the SSID interface.
- **Mesh ID** — Name of the mesh network.
- **Method** — Security applied on Open Mesh links.
 - **No Security** — None.
 - **WPA3-Personal** — Uses WPA3 with Simultaneous Authentication of Equals (SAE) on mesh links to other APs.
- **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
 - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See [Figure 29, “Bridge to Internet”, on page 47.](#))
 - **Route to Internet** — Configures an interface as a member of the LAN. Traffic from this interface is routed across the access point and out through an interface which is bridged to the Internet. (See [Figure 30, “Route to Internet”, on page 47.](#))
 - **Network Name** — The network to be routed. The default is “Default local network” as displayed under LAN Settings – Local Network.

Wireless Networks — **Figure 46: Advanced Radio Settings**
Advanced Radio Settings

The following items are displayed in this section of the Wireless Settings page:

- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range.

Power selection is not just a trade off between coverage area and maximum supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model and the Country setting.)

- **SGI** — Enables the Short Guard Interval (SGI) in the following 802.11 modes:
5 GHz radio; 802.11a, 802.11a+ n, 802.11ac+a+n.
2.4 GHz radio; 802.11 b g+ n.

The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling SGI sets it to 400ns. (Default: Disabled)

VLAN Settings

VLANs (virtual local area networks) are turned off by default. If turned on they will automatically tag any packets passed to the LAN port from the relevant VAP (virtual access point).

The access point can employ VLAN tagging to control access to network resources and increase security. VLANs separate traffic passing between the access point, associated clients, and the wired network. You can create up to 16 VLAN tagged networks.

Note the following points about the access point's VLAN support:

- If an Ethernet LAN port on the access point is assigned a VLAN ID, any traffic entering that port must be also tagged with the same VLAN ID.
- Wireless clients associated to the access point can be assigned to a VLAN. Wireless clients are assigned to the VLAN for the VAP interface with which they are associated. The access point only allows traffic tagged with correct VLAN IDs to be forwarded to associated clients on each VAP interface.
- When VLAN support is enabled on the access point, traffic passed to the wired network is tagged with the appropriate VLAN ID. When an Ethernet port on the access point is configured as a VLAN member, traffic received from the wired network must also be tagged with the same VLAN ID. Received traffic that has an unknown VLAN ID or no VLAN tag is dropped.
- When VLAN support is disabled, the access point does not tag traffic passed to the wired network and ignores the VLAN tags on any received frames.
- Network IP range conflict detection and resolution — The AP has two built-in local networks - one "main" network, and the more secure "guest" network. By

default, the subnet ranges of these networks is set to 192.168.2.1 and 192.168.3.1, respectively.

If your network is already configured to use one of these subnets, when you plug in your network cable to the WAN port of your AP, there would normally be an IP conflict in the local AP's network and your upstream network.

However, if your WAN subnet conflicts with any of the local networks (even the custom ones you create), the AP will automatically change the subnet of the local network.



Note: Before enabling VLAN tagging on the access point, be sure to configure the attached network switch port to support tagged VLAN frames for the VLAN IDs configured on the access point. Otherwise, connectivity to the access point will be lost when you enable the VLAN feature.

Figure 47: Configuring VLANs

Wireless VLAN Settings

Create up to 16 VLAN-tagged networks.

[+ Add new](#)

VLAN Id	Ports	Members	
33	<input type="checkbox"/> Ethernet Port #0 <input type="checkbox"/> Ethernet Port #1 <input checked="" type="checkbox"/> Ethernet Port #2	(None)	Delete

[Save & Apply](#)
[Save](#)
[Reset](#)

The following items are displayed on this page:

- **VLAN ID** — A VLAN identifier to be assigned. (Range: 2-4094) (VLANs 1 is reserved for internal use.)
- **Ports** — The Ethernet ports assigned to the specified VLAN.
- **Members** — The SSID of a VAP configured to be a member of the specified VLAN. This option is configured under Radio Settings (Network Settings – Network Behavior).

5

System Settings

This chapter describes maintenance settings on the access point. It includes the following sections:

- [“System Settings” on page 79](#)
- [“Maintenance” on page 81](#)
- [“Upload Certificate” on page 84](#)
- [“User Accounts” on page 84](#)
- [“Services” on page 85](#)
- [“Diagnostics” on page 92](#)
- [“Device Discovery” on page 93](#)

System Settings

The System Settings page can be used to enable the AP to be managed from the Edgecore ecCLOUD controller or EWS-Series Controller, and configure general descriptive information about the AP.

Figure 48: System Settings

The screenshot displays the 'System Settings' page. It is divided into two main sections: 'Management Settings' and 'System Settings'. In the 'Management Settings' section, there is a 'Management' dropdown menu currently set to 'Disable'. The 'System Settings' section includes a 'Hostname' text field with 'EAP101' entered. Below this is a toggle for 'Enable reset button' which is turned 'ON'. A 'Local Time' display shows 'Thu Jun 30 14:54:29 2022 UTC' with a link to 'Configure Network Time'. There is a 'Number of boot retries' text field set to '3'. An 'MSP mode' toggle is turned 'OFF'. Finally, a 'Led Enable' toggle is turned 'ON'.

The following items are displayed on this page:

- **Management** — Set to “ecCLOUD” to manage this AP from the Edgecore ecCLOUD controller. Set to “EWS-Series Controller” to manage this AP from an Edgecore EWS-Series controller in the local network. Set to disable to manage the AP through the web interface in a stand-alone mode.
 - **ecCLOUD** — When selected, the following parameters are displayed:
 - **Controller URL** — Provides a URL link to the Edgecore ecCLOUD controller management site.
 - **Enable agent** — Enables the AP to be managed from the ecCLOUD controller.
 - **Registration URL** — Specifies the URL for device registration.
 - **EWS-Series Controller** — When selected, the following parameters are displayed:
 - **CAPWAP** — Enables CAPWAP (Control And Provisioning of Wireless Access Points) protocol tunnel mode.
 - **DNS SRV Discovery** — The AP uses DNS server records to discover the EWS controller to which it can send a CAPWAP join request.

- **Domain Name Suffix** — Specifies the domain suffix of the controller.
- **DHCP Option Discovery** — The AP uses the DHCP server to obtain an IP address in the same subnet as the EWS controller, which it can then discover and send a CAPWAP join request.
- **Broadcast Discovery** — The AP sends broadcast requests to discover the EWS controller in the same subnet.
- **Multicast Discovery** — The AP sends multicast discover packets across the network to find the EWS controller. This option requires routing paths to be properly configured in the network.
- **Static Discovery** — Provides a manual method to reach an EWS controller by entering IP addresses that the AP uses to send a CAPWAP join request.
- **Hostname** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: EAP101; Range: 0-50 characters)
- **Enable Reset Button** — Enables the AP's hardware reset button. (Default: Enabled)
- **Local Time** — The local time, given as day of week, month, time, year.
- **Number of boot retries** — The maximum number of bootup retries before switching to the next boot bank. (Range: 1-254; Default: 3)
- **MSP Mode** — Enables the Managed Service Provider (MSP) mode that prevents end-users from accessing and modifying most device settings from user-defined user accounts. Management access from "root" and "admin" accounts still provide full access to all device settings. (Default: Disabled)

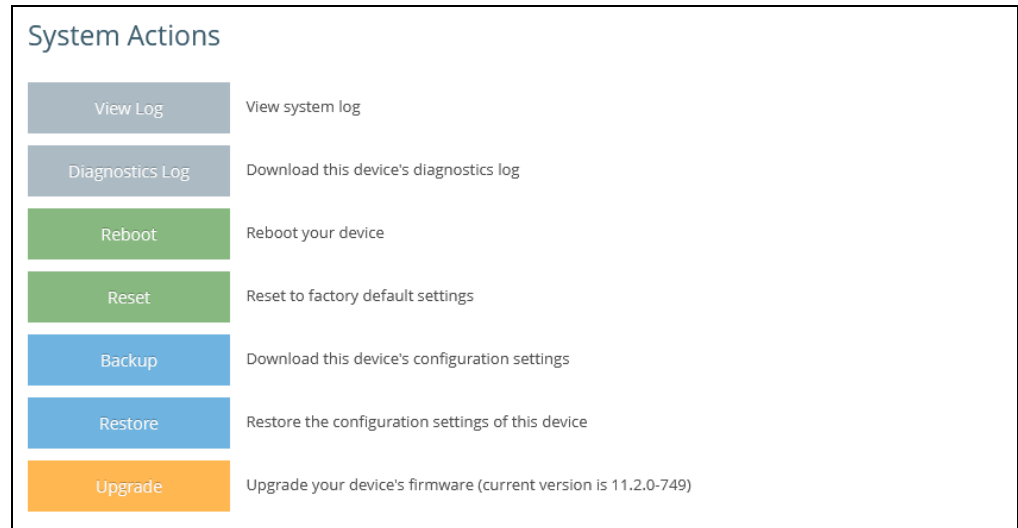
With MSP mode enabled, service providers have the option of making specific wireless SSID settings available for user configuration by enabling the "Local Configurable" setting. See ["Wireless Networks — General Settings" on page 65](#).

- **LED Enable** — Enables the LED indicators on the AP. (Default: Enabled)

Maintenance

The Maintenance page supports general maintenance tasks including displaying the system log, downloading a diagnostics log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

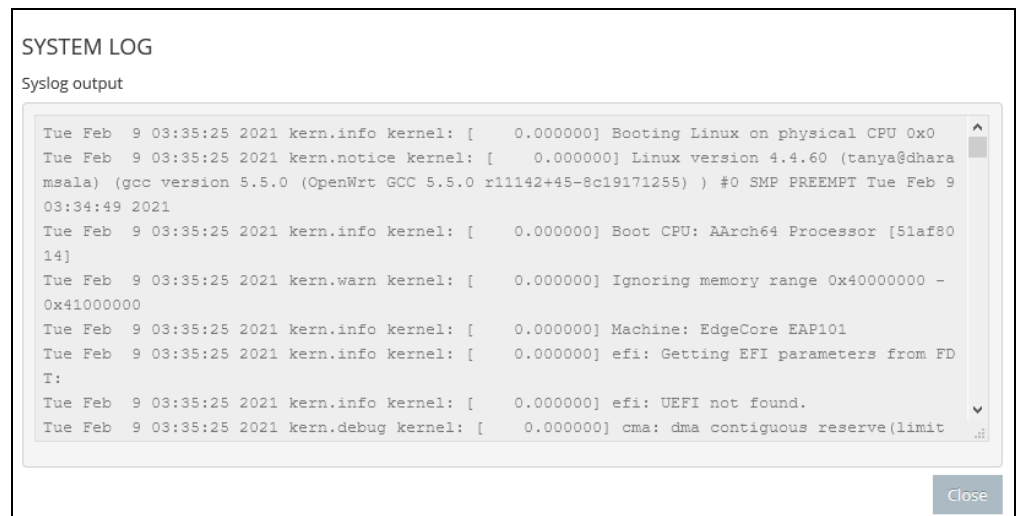
Figure 49: Maintenance



Displaying System Logs

The access point saves event and error messages to a local system log database. The log messages include the date and time, device name, message type, and message details.

Figure 50: System Log

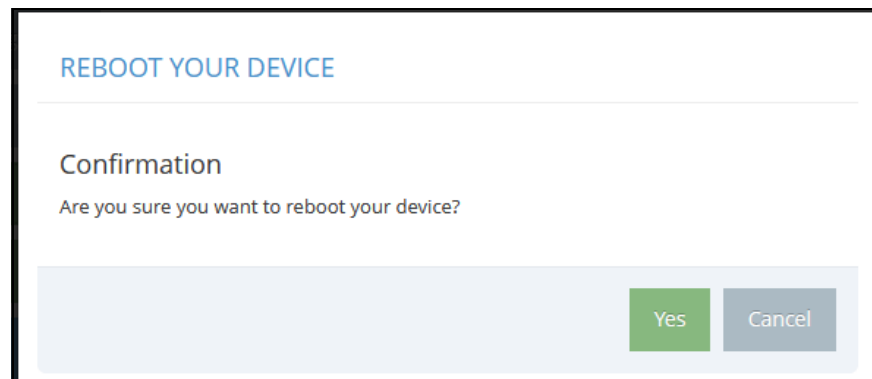


Downloading the Diagnostics Log Click “Diagnostics Log” to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder.

The diagnostics log file contains information that can help Edgecore resolve technical issues with the AP.

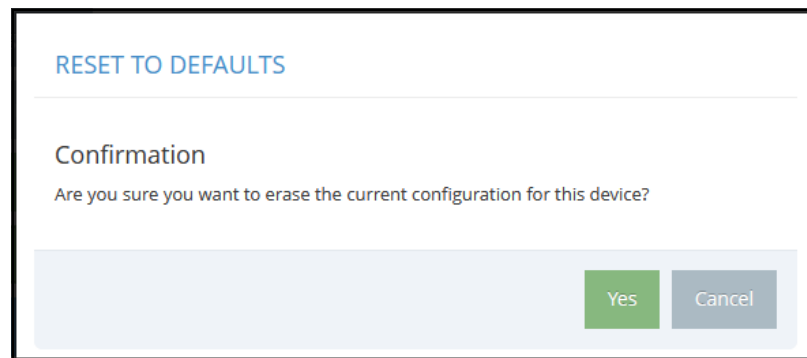
Rebooting the Access Point The Reboot page allows you to reboot the access point.

Figure 51: Rebooting the Access Point



Resetting the Access Point The Reset page allows you to reset the access point to the factory defaults. Note that all user configured information will be lost. You will have to re-enter the default user name and password to re-gain management access to this device.

Figure 52: Resetting to Defaults



Note: It is also possible to reboot or reset the access point by inserting a pin in the pin hole labeled “Reset” on the connector panel of the access point and:

- give a quick press to reboot the access point;
- press and hold for 5 seconds to reset the access point to factory defaults.

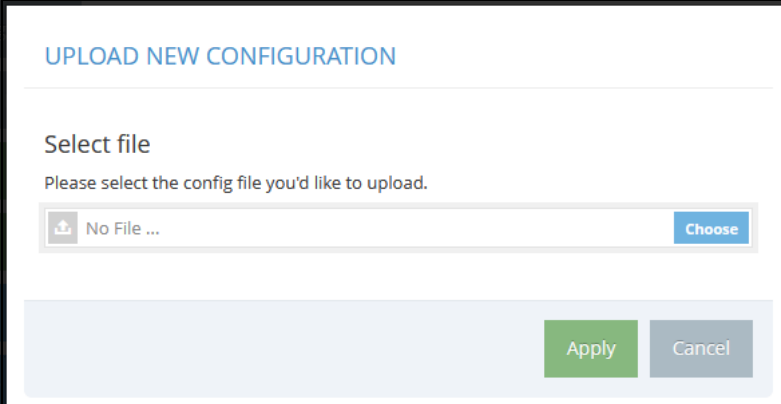
**Backing Up
Configuration
Settings**

The Backup function allows you to back up the access point's configuration to a management workstation. In Windows, a GNU Zip (*.tar.gz) file will be stored in the Downloads folder. This is a sample file name: backup-EAP101-2021-02-09.tar.gz

**Restoring
Configuration
Settings**

The Restore page allows you to upload configuration settings from a management workstation. The specified file must be one that was previously backed up from the access point.

Figure 53: Restoring Configuration Settings



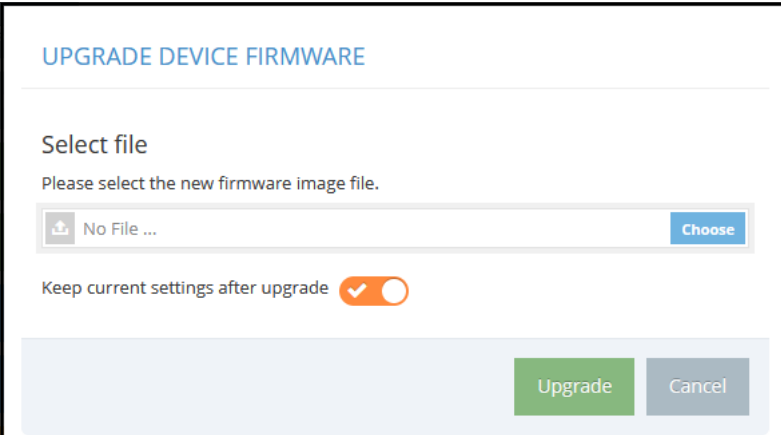
The screenshot shows a web interface titled "UPLOAD NEW CONFIGURATION". Below the title is a "Select file" section with the instruction "Please select the config file you'd like to upload." There is a file selection area with a "No File ..." button and a "Choose" button. At the bottom right, there are "Apply" and "Cancel" buttons.

Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation. New software may be provided periodically from Edgecore.

After upgrading new software, you must reboot the access point to implement the new code. Until a reboot occurs, the access point will continue to run the software it was using before the upgrade started. The access point supports dual software images, so if newly loaded software is corrupted, the alternate image will be used on the next reboot. Configuration settings are stored separately from the software, so the current settings will always be used for any new software. However, note that if the current configuration settings are corrupted, the system defaults will be used.

Figure 54: Upgrading Firmware



The screenshot shows a web interface titled "UPGRADE DEVICE FIRMWARE". Below the title is a "Select file" section with the instruction "Please select the new firmware image file." There is a file selection area with a "No File ..." button and a "Choose" button. Below this is a toggle switch labeled "Keep current settings after upgrade" which is currently turned on. At the bottom right, there are "Upgrade" and "Cancel" buttons.

Upload Certificate

The Upload Certificate page allows you to upload a unique security certificate from a trusted certification authority for secure access (an encrypted connection) to a configured HTTPS captive portal. Alternatively, you can also reset to use the default certificate.

Figure 55: Upload Certificate

The screenshot shows the 'Upload Certificate' page. At the top, there are two buttons: a green 'Upload Certificate' button with the text 'Upload Certificate of this device' and an orange 'Use Default Certificate' button with the text 'Reset to default Certificate'. Below these buttons, a text line states: 'The following table shows properties of your current Trusted Root CA Certificate.' Below this text is a table with two columns: a property name and its value.

COUNTRY	▶ TW
LOCALITY	▶ Hsinchu
ORGANIZATION	▶ Accton
VERSION	▶ 3
SERIAL NUMBER	▶ AC9A7B3ED6341BFC
SIGNATURE ALGORITHM	▶ sha1WithRSAEncryption
VALID FROM	▶ Feb 26 07:01:56 2014 GMT
VALID UNTIL	▶ Nov 13 07:01:56 2033 GMT
SUBJECT KEY IDENTIFIER	▶ C0:78:AC:2D:8B:F4:00:7B:94:EF:A3:9C:6E:2E:2E:BB:8B:03:DE:AA
IS CERTIFICATE AUTHORITY	▶ TRUE

The following items are displayed on this page:

- **Upload Certificate** — Click to upload a security certificate and private key from a trusted certification authority.
- **Use Default Certificate** — Click to reset to use the AP's default certificate.

User Accounts

The User Accounts page allows you to control management access to the AP based on manually configured user names and passwords.

Figure 56: User Accounts

The screenshot shows the 'User Accounts' page. At the top left, there is a blue button labeled '+ Add new'. Below this is a table with four columns: 'Enabled', 'Username', 'Password', and an action column. The table contains two rows of user accounts.

Enabled	Username	Password	
<input checked="" type="checkbox"/>	root	*****	
<input checked="" type="checkbox"/>	admin	*****	

The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 1-32 ASCII characters, no special characters)
- **Password** — The user password. (Range: 6-20 ASCII characters, case sensitive, no special characters)

Services

The Services page allows you to control SSH management access to the AP, configure NTP time servers, and configure iBeacon settings.

SSH The Secure Shell (SSH) can act as a secure replacement for Telnet. The SSH protocol uses generated public keys to encrypt all data transfers passing between the access point and SSH-enabled management station clients and ensures that data traveling over the network arrives unaltered. Clients can then securely use the local user name and password for access authentication.

Note that SSH client software needs to be installed on the management station to access the access point for management via the SSH protocol.

Figure 57: SSH Settings



SSH

SSH Server ☒

Port

Allow SSH from WAN ☐

The following items are displayed on this page:

- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

Telnet Telnet is a remote management tool that can be used to configure the access point from anywhere in the network. However, note that Telnet is not secure from hostile attacks.

Figure 58: Telnet Server Settings

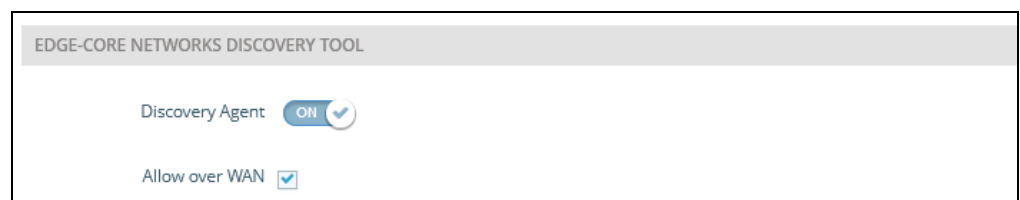


The following items are displayed on this page:

- **Telnet Server** — Enables or disables Telnet access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the Telnet server on the access point. (Range: 1-65535; Default: 23)
- **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

Edgecore Networks Discovery Tool The Discovery Tool agent enables the AP to find other Edgecore devices in the same Layer 2 network. See [“Device Discovery” on page 93](#) to scan the network for devices.

Figure 59: Discovery Agent Settings



The following items are displayed on this page section:

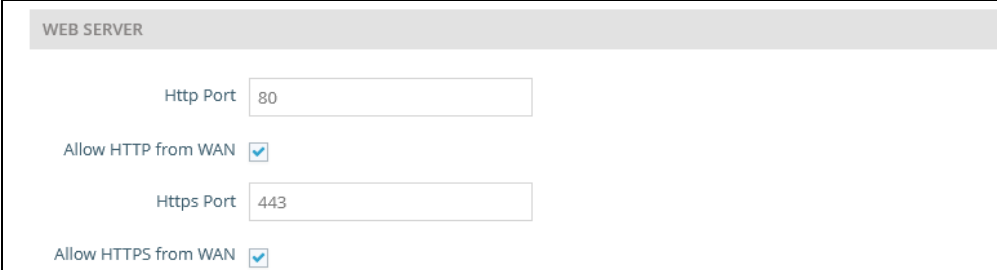
- **Discovery Agent** — Enables the discovery agent. (Default: Enabled)
- **Allow over WAN** — Enables the discovery agent to operate over the port connected to the Internet source. (Default: Enabled)

Web Server A Web browser provides the primary method of managing the access point. Both HTTP and HTTPS service can be accessed independently. If you enable HTTPS, you must indicate this in the URL: https://device:port_number]

When you start HTTPS, the connection is established in this way:

- The client authenticates the server using the server's digital certificate.
- The client and server negotiate a set of security protocols to use for the connection.
- The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.
- A padlock icon should appear in the status bar for most browsers.

Figure 60: Web Server Settings



WEB SERVER

Http Port

Allow HTTP from WAN ☒

Https Port

Allow HTTPS from WAN ☒

The following items are displayed on this page:

- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **Allow HTTP from WAN** — Allows HTTP management access from the WAN.
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)
- **Allow HTTPS from WAN** — Allows HTTPS management access from the WAN.

Remote System Log Setup Use this feature to send log messages to a Syslog server.

Figure 61: Remote System Log Settings



The screenshot shows the 'REMOTE SYSTEM LOG SETUP' configuration page. It includes a toggle for 'Remote Syslog' which is currently turned 'ON' with a checkmark icon. Below this are three input fields: 'Server IP', 'Server Port', and 'Log Prefix', each with a red border indicating they are required or active. At the bottom, there is a 'Track Connections' toggle which is currently turned 'OFF' with a minus icon.

The following items are displayed on this page:

- **Remote Syslog** — Enables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Server IP** — Specifies the IP address of a remote Syslog server that will be sent log messages.
- **Server Port** — Specifies the UDP port number used by the remote Syslog server. (Range: 1-65535)
- **Log Prefix** — Sets a prefix string for log messages sent to the specified server. The prefix can help with sorting messages on the server.
- **Track Connections** — Enables the inclusion of connection information such as source IP and port, destination IP and port in log messages.

Network Time Network Time Protocol (NTP) allows the access point to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the access point enables the system log to record meaningful dates and times for event entries. If the clock is not set, the access point will only record the time from the factory default set at the last bootup.

The access point acts as an NTP client, periodically sending time synchronization requests to specified time servers. The access point will attempt to poll each server in the configured sequence to receive a time update.

Figure 62: NTP Settings

NETWORK TIME (NTP)

Local Time Wed Oct 13 07:00:04 2021 UTC

NTP Service ☒

NTP servers tock.stdtime.gov.tw
watch.stdtime.gov.tw
time.stdtime.gov.tw
clock.stdtime.gov.tw

+

Timezone UTC

The following items are displayed on this page:

- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)
- **NTP Servers** — Sets the host names for time servers. The switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence. To configure additional servers, click the “+” button to open a new edit field.
- **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

SNMP Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. It is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Figure 63: SNMP Settings

SNMP

SNMP Server ☒

Read Community public

Write Community private

IPv6 Read Community public6

IPv6 Write Community private6

Trap ☒

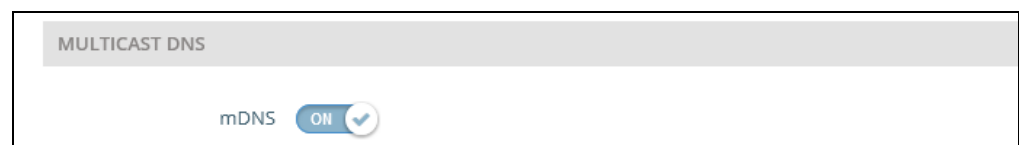
Server IP 10.1.2.3

The following items are displayed on this page:

- **SNMP Server** — Enables or disables SNMP on the access point.
(Default: Enabled)
- **Read Community** — A community string that acts like a password and permits read access to the access point's Management Information Base (MIB).
(Range: 1-32 characters, case sensitive; Default: public)
- **Write Community** — A community string that acts like a password and permits write access to the access point's Management Information Base (MIB).
(Range: 1-32 characters, case sensitive; Default: private)
- **IPv6 Read Community** — A community string for IPv6 read access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: public6)
- **IPv6 Write Community** — A community string for IPv6 write access to the access point's Management Information (MIB) database. (Range: 1-32 characters, case sensitive; Default: private6)
- **Trap** — Enables the sending of SNMP trap messages to a specified server. The access point sends the following trap messages: cold start, warm start, link up, and link down. (Default: Disabled)
 - **Server IP** — Specifies the IP address of the SNMP trap server that will be sent trap messages.

Multicast DNS The multicast DNS (mDNS) protocol is a zero-configuration service to facilitate connections within a local networks.

Figure 64: Multicast DNS Settings



The following items are displayed on this page:

- **mDNS** — Enables or disables Multicast DNS on the access point.
(Default: Enabled)

LLDP Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices in a network. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device.

Figure 65: LLDP Settings

The following items are displayed on this page:

- **Send LLDP** — Enables the sending of LLDP advertisements about the AP to neighboring devices in the network. (Default: Disabled)
- **Tx Interval (seconds)** — Sets the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)
- **Tx Hold (time(s))** — Configures a time-to-live (TTL) value sent in the LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 4)

The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending device if it does not transmit updates in a timely manner.

The TTL in seconds is based on the following rule:
minimum value ((Tx Interval * Tx Hold), or 65535)
Therefore, the default TTL is $4 * 30 = 120$ seconds.

BLE The AP supports the iBeacon standard based on Bluetooth Low Energy (BLE). Devices with BLE Beacons can provide location-based services to BLE clients, such as phones, that can recognize the beacon advertisements, extract the provided information, and then take actions based on the content.

Figure 66: BLE Settings

The following items are displayed on this page:

- **Send iBeacon** — Enables iBeacon support on the AP. (Default: Enabled)
- **UUID** — The iBeacon Universally Unique Identifier that advertises the beacon service. The UUID contains 32 hexadecimal digits in five groups, separated by hyphens.
- **Major** — The iBeacon value that is used to identify a beacon group. (Range: 0-65535)
- **Minor** — The iBeacon value that is used to identify individual beacons within a group. (Range: 0-65535)
- **Tx Power** — Sets the BLE radio transmit power (supported only on EAP101 and EAP104). (Range: 5 dBm to -20 dBm; Default: 5 dBm)
- **BLE Scan** — (EAP101 and EAP104 only) Scans for all BLE devices, including these four types: EddyStone-UUID, EddyStone-URL, EddyStone-TLM, and ibeacon.

Figure 67: BLE Scan



The screenshot shows a web interface titled "BLE SCAN" with a "BLE Scan Now" button and a close icon. Below is a table with three columns: "MAC Address", "Signal", and "Type". The table contains six rows of data.

MAC Address	Signal	Type
51:F2:DE:6F:5F:5A	-74dBm	ibeacon
52:3A:8D:30:CF:64	-75dBm	EddyStone-UUID
56:62:39:B2:7B:DB	-73dBm	EddyStone-URL
6E:A3:1A:DA:CA:DF	-81dBm	EddyStone-TLM
79:2C:9F:37:EC:8A	-84dBm	EddyStone-UUID
7E:67:D5:E9:78:C7	-74dBm	ibeacon

Diagnostics

The Diagnostics page provides Ping, Traceroute, and Nslookup tools for troubleshooting connectivity problems.

Enter a hostname or IP address and click to run the tool.

Figure 68: Network Utilities

The screenshot shows the 'Diagnostics' section of a system settings interface. Under the 'NETWORK UTILITIES' header, there are three input fields, each followed by a button: 'Ping', 'Traceroute', and 'Nslookup'.

Device Discovery

The Device Discovery Tool provides a method for finding other Edgecore APs within the same Layer 2 network. To function, the Discovery Agent must be enabled (see [“Edgecore Networks Discovery Tool”](#) on page 86).

Click the Scan Network button to scan for devices.

Figure 69: Device Discovery Tool

The screenshot shows the 'Device Discovery Tool' interface. At the top, there are two buttons: 'Scan Network' and 'Clear'. Below these is a table with the following data:

Device Model	Hostname	MAC Address	Device IP Address
Edge-core Wave2	EAP101	90:3cb3:bc99:4f	192.168.1.10

Section III

Appendices

This section provides additional information and includes these items:

- [“Troubleshooting” on page 95](#)

A

Troubleshooting

Problems Accessing the Management Interface

Table 1: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	<ul style="list-style-type: none">■ Be sure the AP is powered up.■ Check network cabling between the management station and the AP.■ Check that you have a valid network connection to the AP and that intermediate switch ports have not been disabled.■ Be sure you have configured the AP with a valid IP address, subnet mask and default gateway.■ Be sure the management station has an IP address in the same subnet as the AP's IP.■ If you are trying to connect to the AP using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.■ If you cannot connect using SSH, you may have exceeded the maximum number of concurrent SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	<ul style="list-style-type: none">■ Reset the AP to factory defaults using its Reset button.

Using System Logs

If a fault does occur, refer to the *Quick Start Guide* to ensure that the problem you encountered is actually caused by the AP. If the problem appears to be caused by the AP, follow these steps:

1. Repeat the sequence of commands or other actions that lead up to the error.
2. Make a list of the commands or circumstances that led to the fault. Also, make a list of any error messages displayed.
3. Record all relevant system settings.
4. Display the log file through the System > Maintenance page, and copy the information from the log file.
5. Download the Diagnostics Log to a file from the System > Maintenance page.

6. Contact Edgecore and send a detailed description of the problem, along with all of the information mentioned in the above steps.

