EAP101
EAP102

User Manual

Software Release 11.1.1

www.edge-core.com

User Manual

EAP101
EAP102

Cloud-Enabled Enterprise Access Point

E042021-CS-R01

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.

April 2021 Revision

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

Contents

Figures

Figures

Tables

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:

1 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

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

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 14.

For information on using the QR code, see "QR Code Onboarding" on page 19.

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 with192.168.2.x).

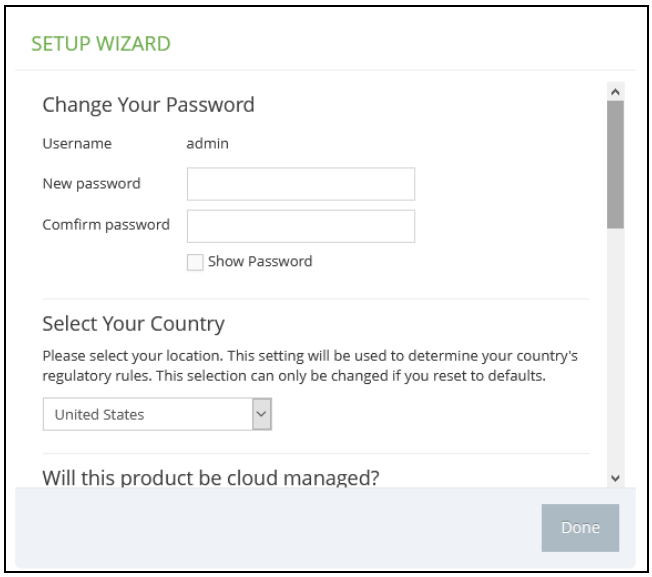
Note: To connect to the web interface using the Uplink(PoE) port, the IP address is automatically assigned through DHCP by default. If a DHCP server is unreachable, the Uplink(PoE) port reverts to a fallback IP address of 192.168.1.10.

To access the AP's web management interface, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.2.1.

   For first-time access, there is no user login and the Setup Wizard starts automatically.

Figure 1: Web Management Login



2. Set a new password for management access and then follow the other steps described in "AP Setup Wizard" on page 14.

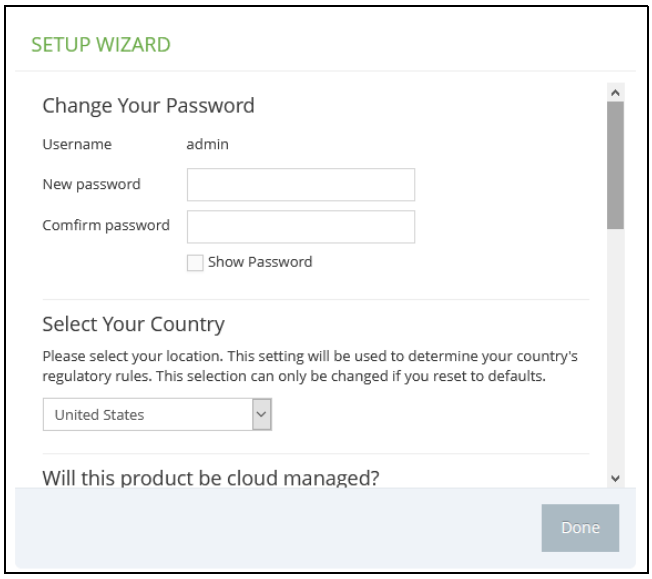
Note: To configure the AP with a different management IP address that is compatible with your network, see "LAN Settings" on page 38.

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 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).

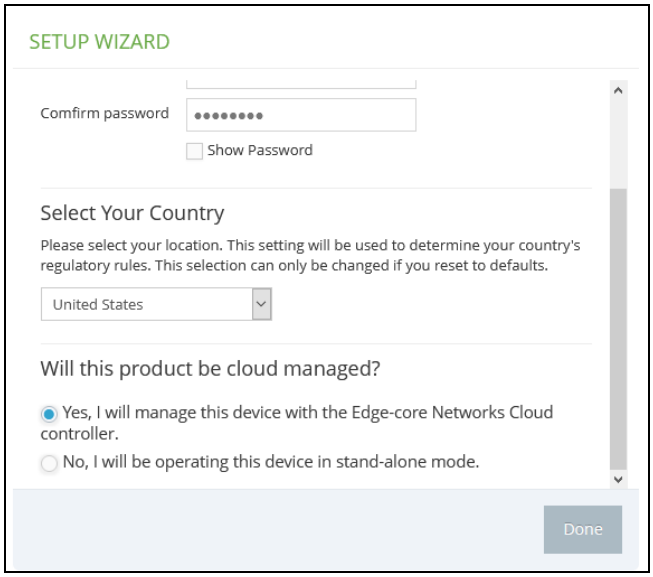
Figure 2: Change Your Password



Note: For information on changing user names and passwords, see "User Accounts" on page 55.

Step 2 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 3: Select Your Country

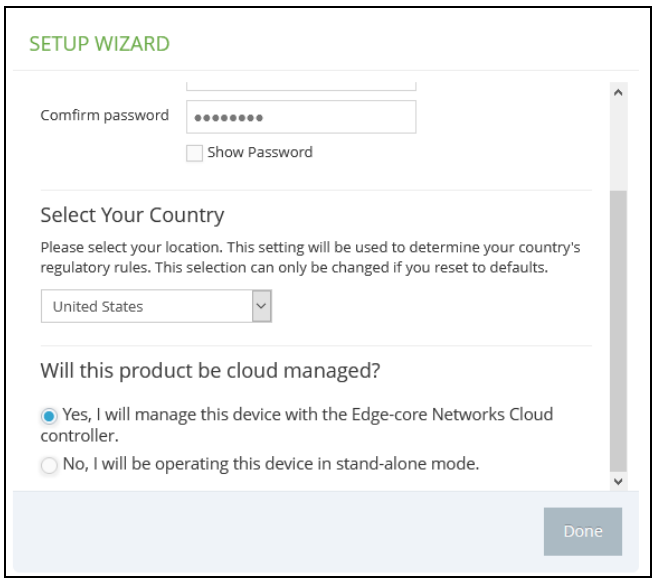


Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.

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 3 Select to Cloud Manage AP or Stand-Alone — To manage the AP using the Edgecore ecCLOUD controller, select "Yes, I will manage this device with the Edge-core Networks Cloud controller," and then click "Done." Otherwise, select "No, I will be operating this device in stand-alone mode" and continue to Step 4.

Figure 4: Select Cloud Managed or Stand-Alone

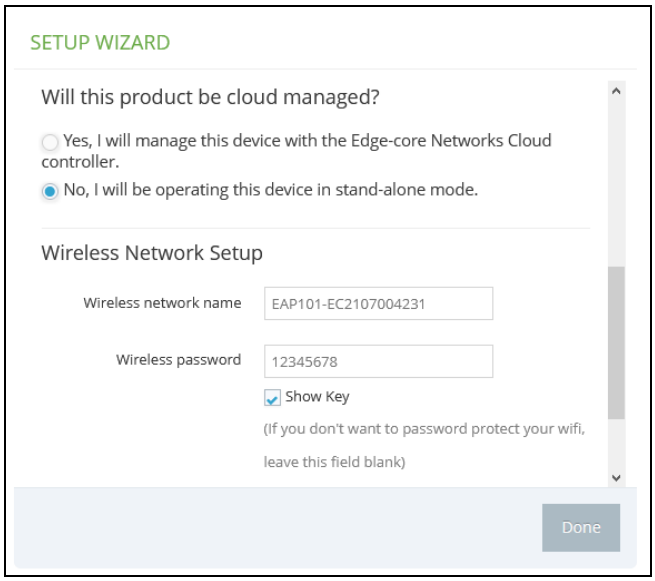


If you select to manage the AP using the Edgecore ecCLOUD controller, go to cloud.ignitenet.com to register your AP. Log in and select Devices from the menu. Click Add Device and enter the AP serial number and MAC address to register the AP with your cloud network. The serial number and MAC address can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

Step 4 Wireless Network Setup — If you select to manage the AP in stand-alone mode, you can continue to configure the default wireless network.

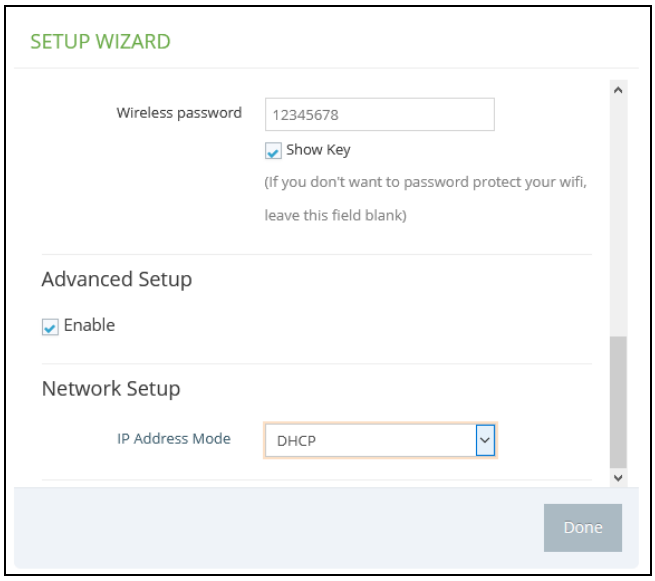
Figure 5: Wireless Network Setup



The default wireless network name 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).

Step 5 Advanced Setup — For AP stand-alone mode, you also have the option to enable the Advanced Setup option and configure the IP address mode used to provide an IP address for the Internet access port.

Figure 6: Advanced Setup



The default IP Address Mode is DHCP and other options include Static IP and PPPoE. For more information, see "Internet Settings" on page 32.

Step 6 After completing the Setup Wizard, click "Done" to continue to the web management main menu.

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 (iPhone) or a barcode app (Android) 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 7: 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 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).

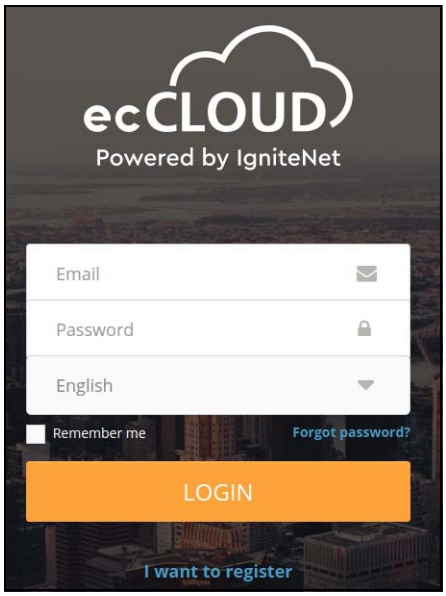
5. Select to manage the AP using the ecCLOUD controller, or to manage the AP in stand-alone mode.

   a. Stand-Alone Mode: Use the default wireless network setting or customize the network name and password. 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. The browser is then redirected to the login page of the AP (see Figure 1 on page 13).

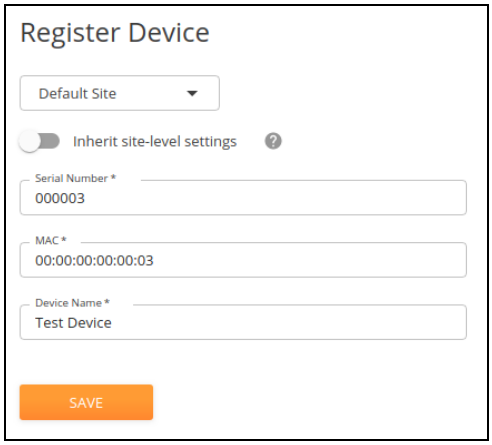
b. Cloud-Managed Mode: Tap "Done" to finish the Setup Wizard and the browser is redirected to the ecCLOUD login page.

Figure 8: 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. After you tap "Save," wait about two minutes for the cloud controller to configure the AP.

Figure 9: ecCLOUD Device Registration



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 two 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.

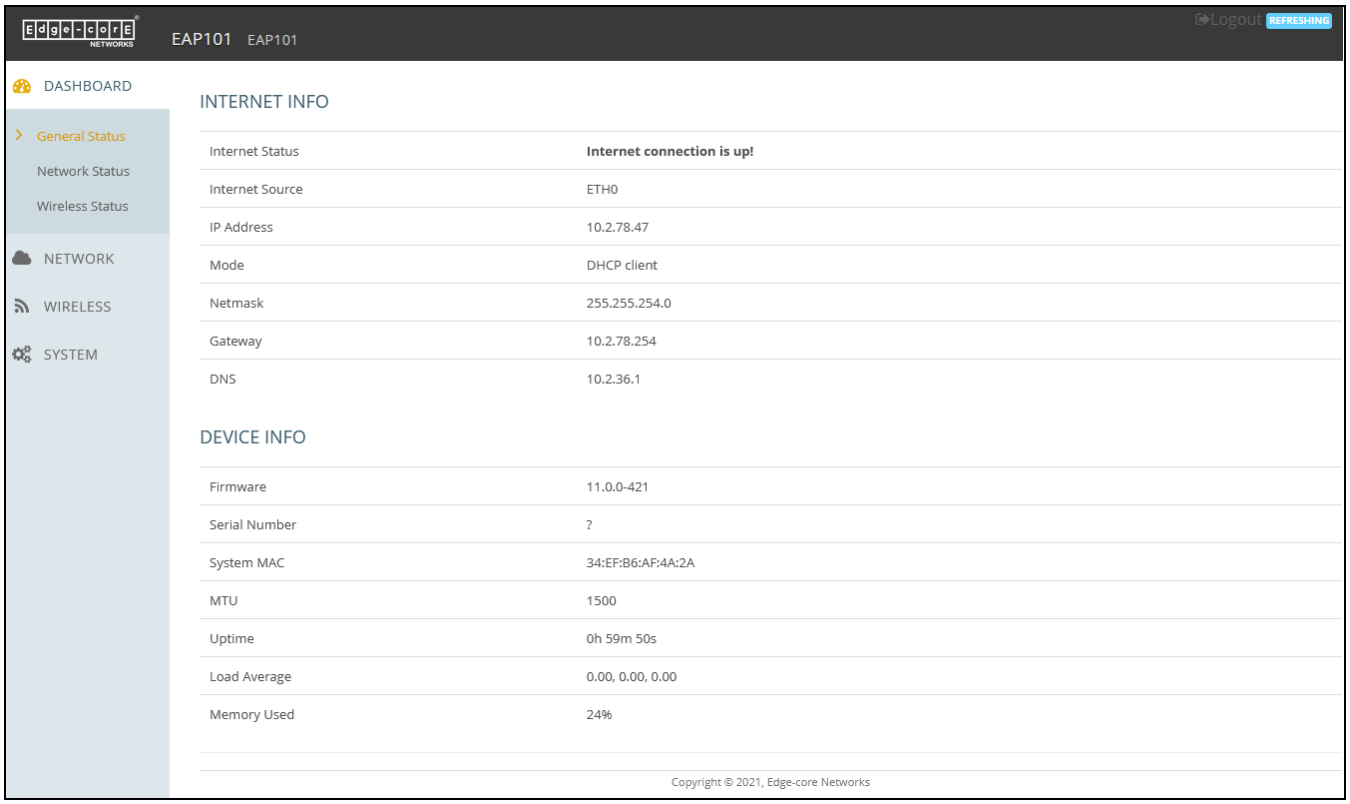
To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Dashboard** — The dashboard shows basic settings for the AP, including general status, local network settings, and wireless radio status. See "Status Information" on page 24.
- **Network** — Configures Internet, Ethernet, and LAN settings. See "Network Settings" on page 31.
- **Wireless** — Configures 5 GHz Radio, 2.4 GHz Radio, and VLAN settings. See "Wireless Settings" on page 40
- **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 10: 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 11: 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:

2 Status Information

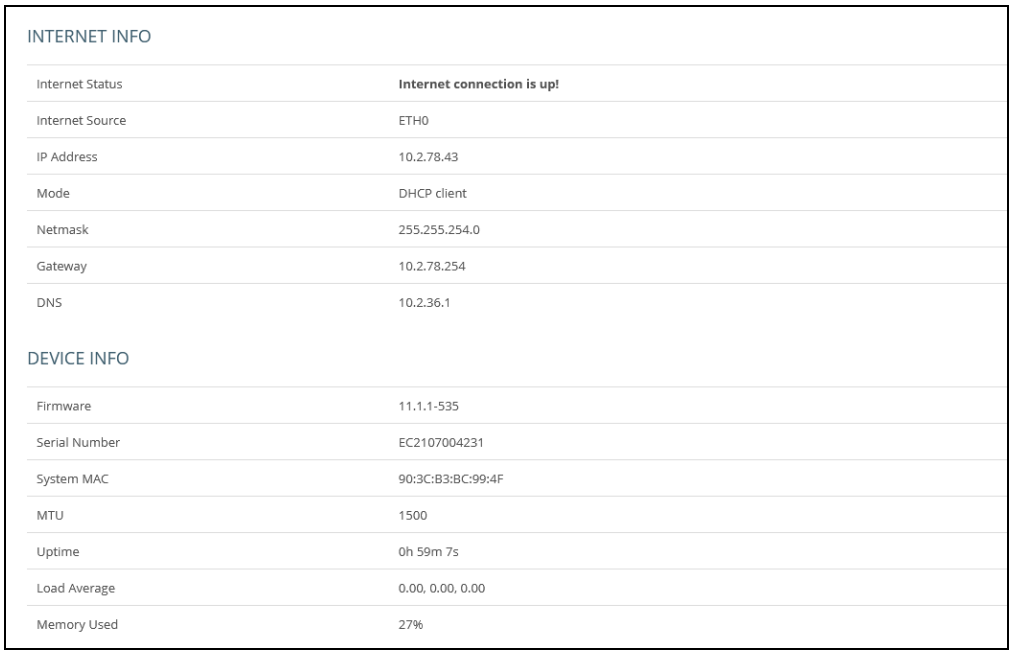
The Dashboard displays information on the current system configuration, including Internet status, local network settings, and wireless radio status.

This chapter includes the following sections:

General Status

The General Status section shows descriptive information about the AP.

Figure 12: General Status Information



INTERNET INFO

Internet Status	**Internet connection is up!**
Internet Source	ETH0
IP Address	10.2.78.43
Mode	DHCP client
Netmask	255.255.254.0
Gateway	10.2.78.254
DNS	10.2.36.1

DEVICE INFO

Firmware	11.1.1-535
Serial Number	EC2107004231
System MAC	90:3C:B3:BC:99:4F
MTU	1500
Uptime	0h 59m 7s
Load Average	0.00, 0.00, 0.00
Memory Used	27%

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.
- **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:

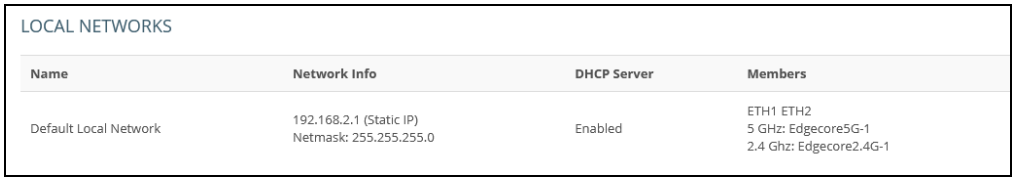
- **Software** — The software version number.

- **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.

Network Status

The Network Status section shows information about local network connections.

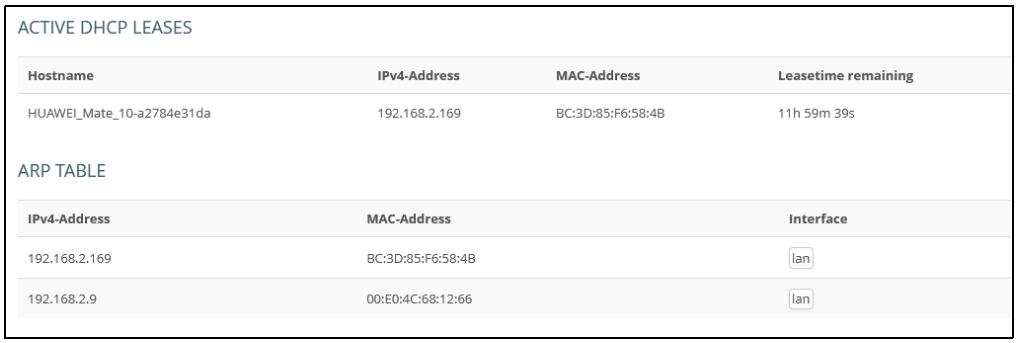
Figure 13: Local Networks



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.)
- **Active DHCP Leases** — Shows DHCP leases.
- **ARP Table** — Shows the ARP cache.

Figure 14: Active DHCP Leases and the ARP Table



ACTIVE DHCP LEASES

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
HUAWEI_Mate_10-a2784e31da	192.168.2.169	BC:3D:85:F6:58:4B	11h 59m 39s

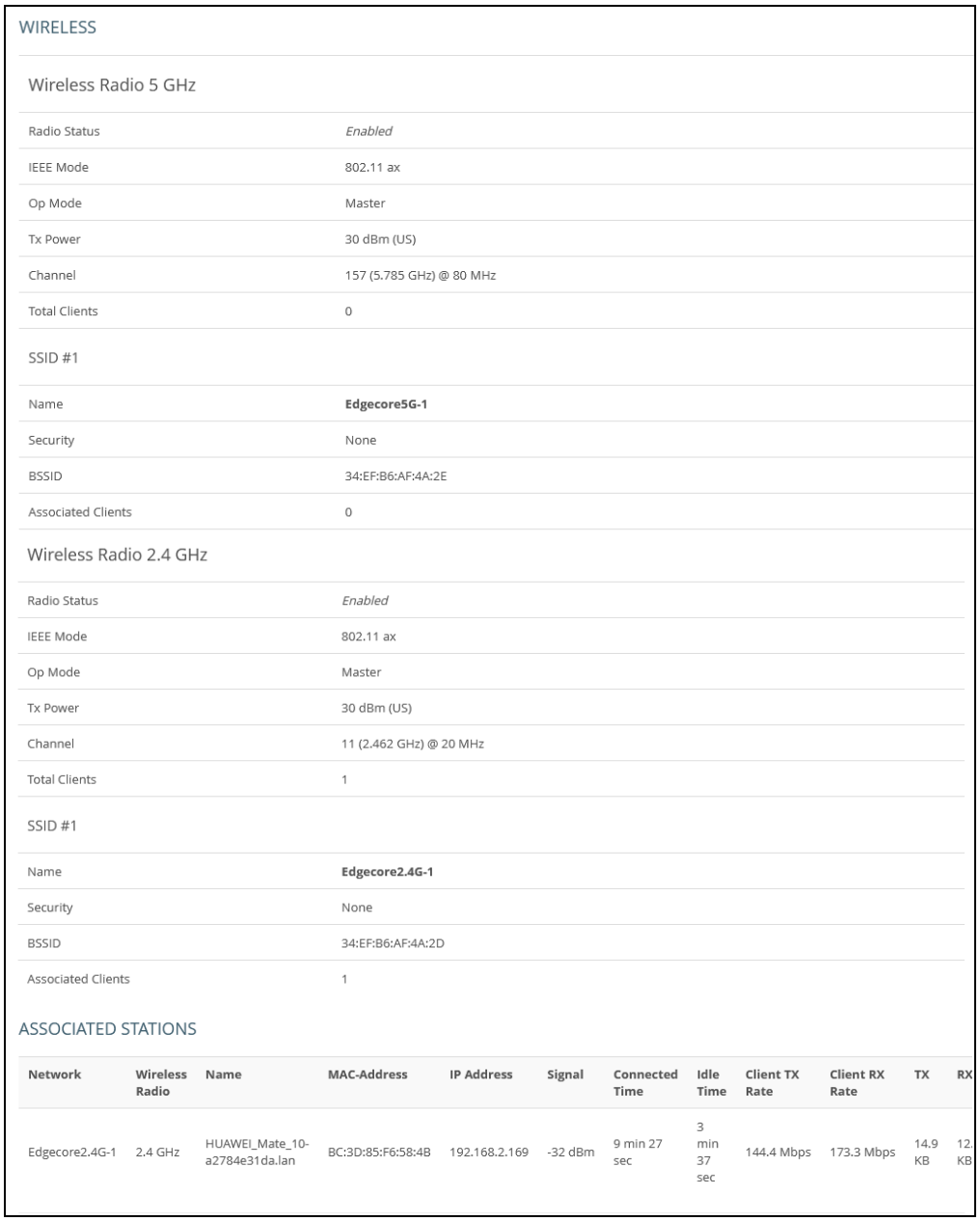
ARP TABLE

IPv4-Address	MAC-Address	Interface
192.168.2.169	BC:3D:85:F6:58:4B	lan
192.168.2.9	00:E0:4C:68:12:66	lan

Wireless Status

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

Figure 15: Wireless Status



WIRELESS

Wireless Radio 5 GHz

Radio Status	*Enabled*
IEEE Mode	802.11 ax
Op Mode	Master
Tx Power	30 dBm (US)
Channel	157 (5.785 GHz) @ 80 MHz
Total Clients	0

SSID #1

Name	**Edgecore5G-1**
Security	None
BSSID	34:EF:B6:AF:4A:2E
Associated Clients	0

Wireless Radio 2.4 GHz

Radio Status	*Enabled*
IEEE Mode	802.11 ax
Op Mode	Master
Tx Power	30 dBm (US)
Channel	11 (2.462 GHz) @ 20 MHz
Total Clients	1

SSID #1

Name	**Edgecore2.4G-1**
Security	None
BSSID	34:EF:B6:AF:4A:2D
Associated Clients	1

ASSOCIATED STATIONS

Network	Wireless Radio	Name	MAC-Address	IP Address	Signal	Connected Time	Idle Time	Client TX Rate	Client RX Rate	TX	RX
Edgecore2.4G-1	2.4 GHz	HUAWEI_Mate_10-a2784e31da.lan	BC:3D:85:F6:58:4B	192.168.2.169	-32 dBm	9 min 27 sec	3 min 37 sec	144.4 Mbps	173.3 Mbps	14.9 KB	12. KB

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** — The number of wireless clients associated to the SSID.

- **Associated Stations** — Shows detailed information about associated wireless clients.
  - **Network** — The SSID name.
  - **Wireless Radio** — Specifies the 5 GHz or 2.4 GHz radio.
  - **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.
  - **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.

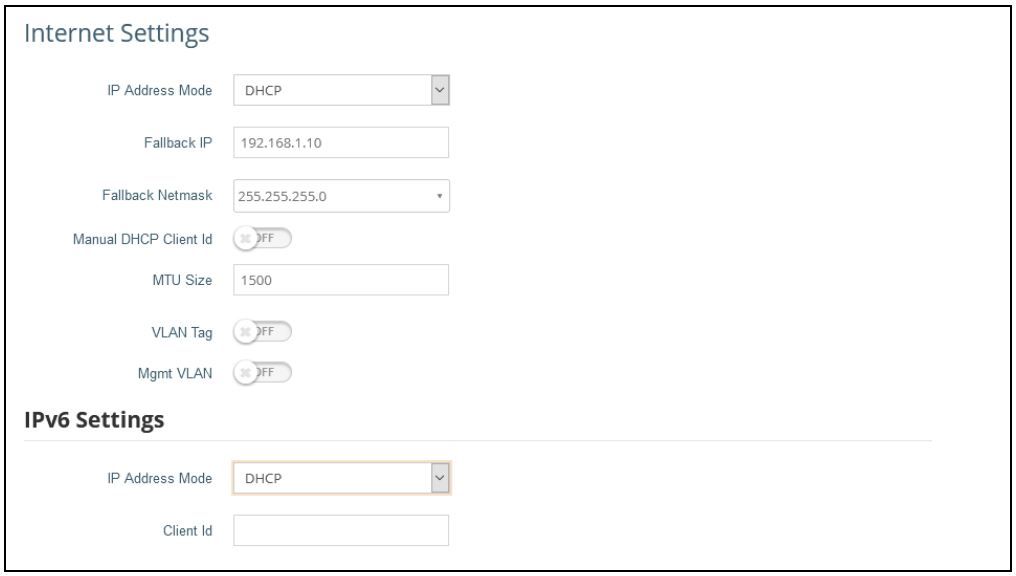
3 Network Settings

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

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 16: Internet Settings



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 16.
    - **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 17: IP Address Mode – Static IP

- **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 18: IP Address Mode – PPPoE

- **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

Figure 19: IPv6 Settings – Static IP

- **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.
  - **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 fields provided.
- **Client Id** — This option to manually enter the client ID for the DHCP client.

Ethernet Settings

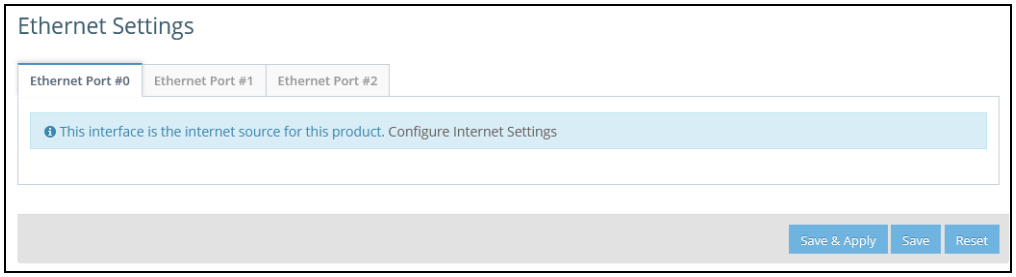
The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection for wireless clients attached to the local network (routed to the Internet), or is bridged directly to the Internet.

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 20: Ethernet Settings – Internet Source

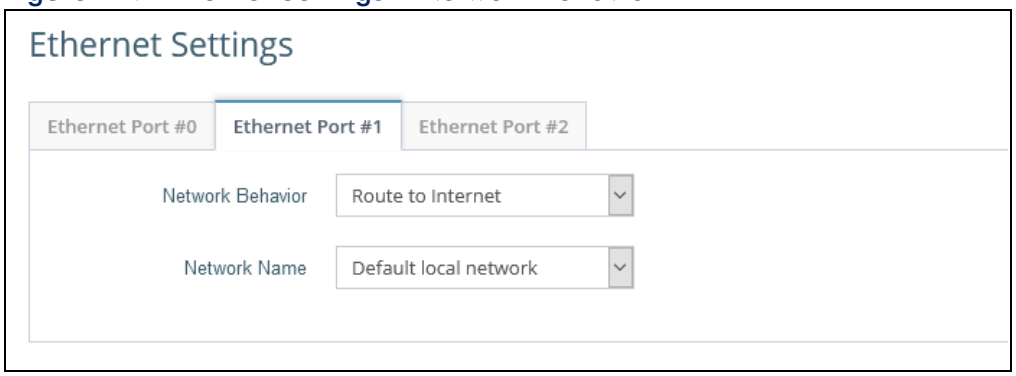


The following status message is displayed if an interface is set as the Internet source:

- "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 21: Ethernet Settings – Network Behavior



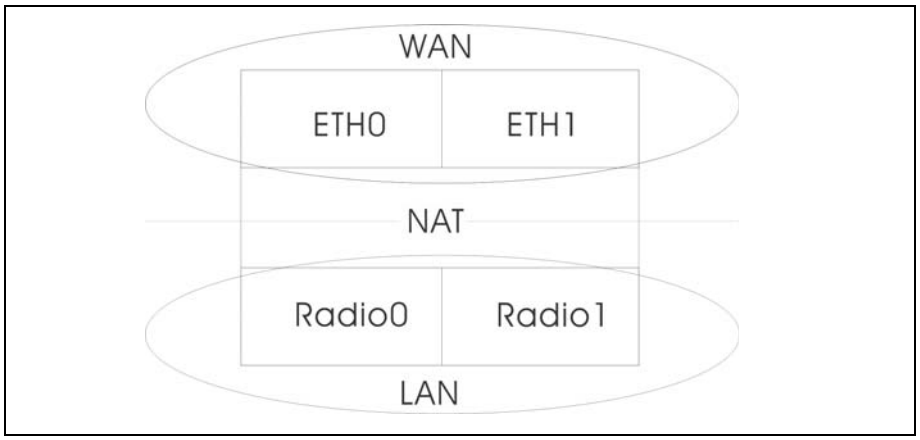
The following items are displayed on this page:

- **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.

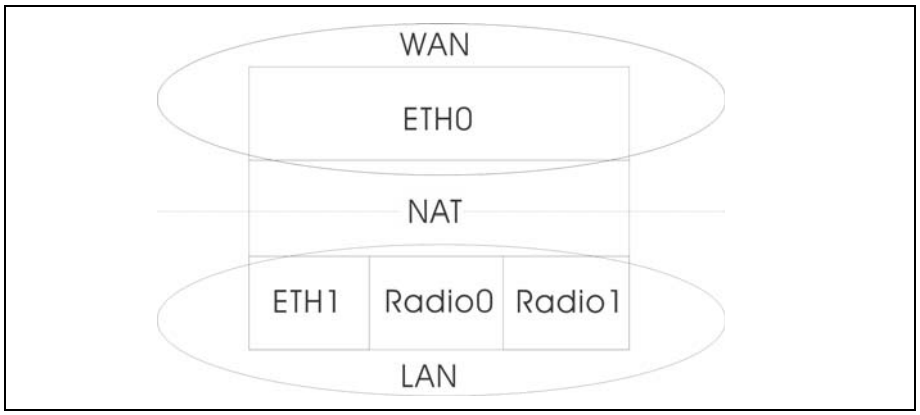
    In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN.

Figure 22: 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 23: Route to Internet



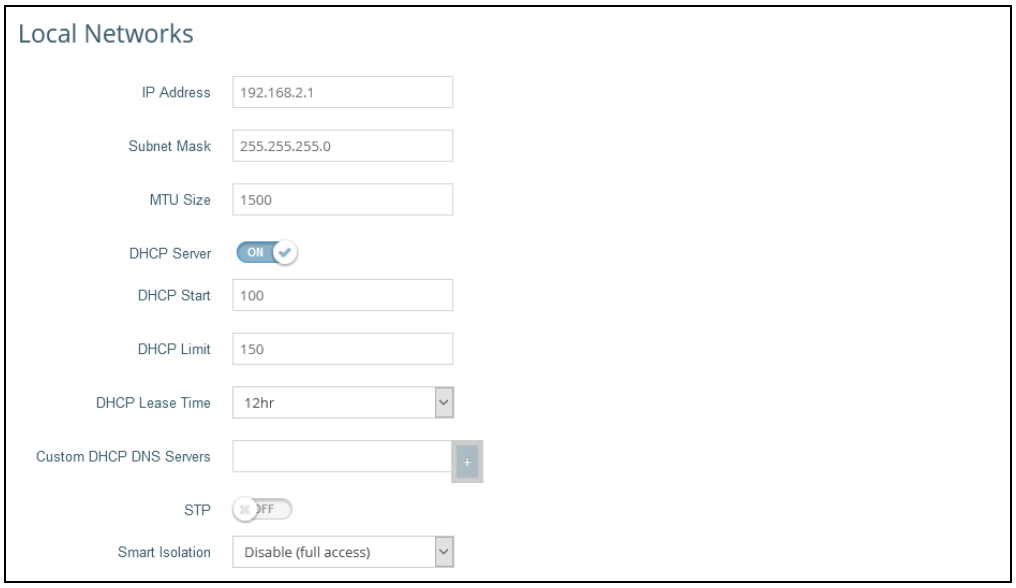
- **VLAN Tag Traffic** — This port transmits tagged traffic from a specified VLAN.

- **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.

LAN Settings

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

Figure 24: Network – LAN Settings



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)

- **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.).

4 Wireless Settings

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

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 25: Physical Settings for Radio 5 GHz

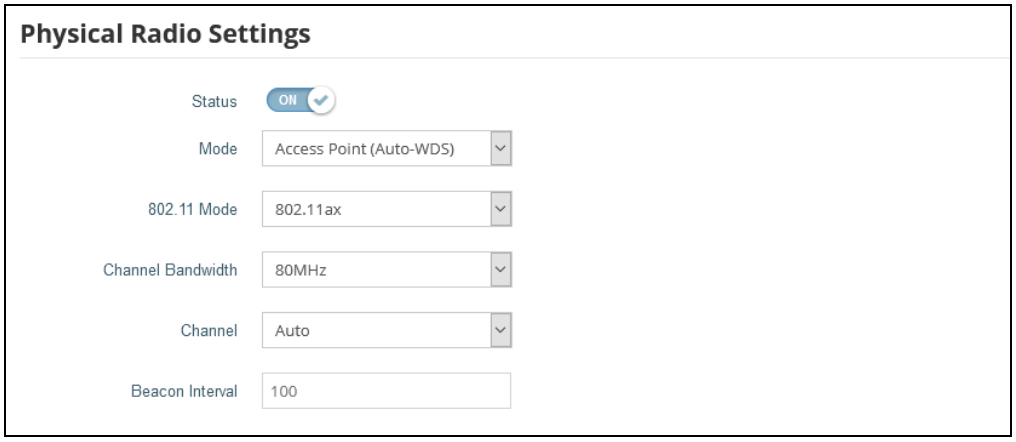
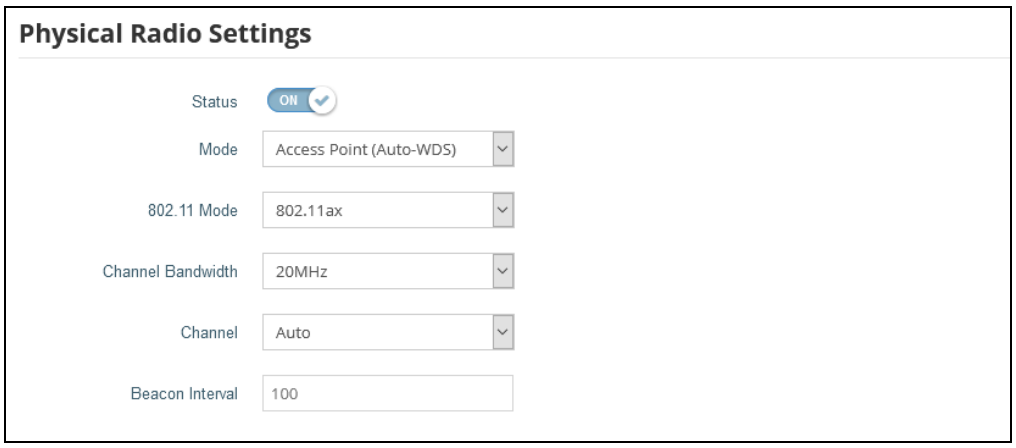


Figure 26: Physical Settings for Radio 2.4 GHz



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 WDS** — The AP operates as a client station in WDS mode, which can connect to other access points in Auto-WDS mode. Connection to another AP can be made automatically by other access points operating in Auto-WDS mode.
- **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)
  - **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

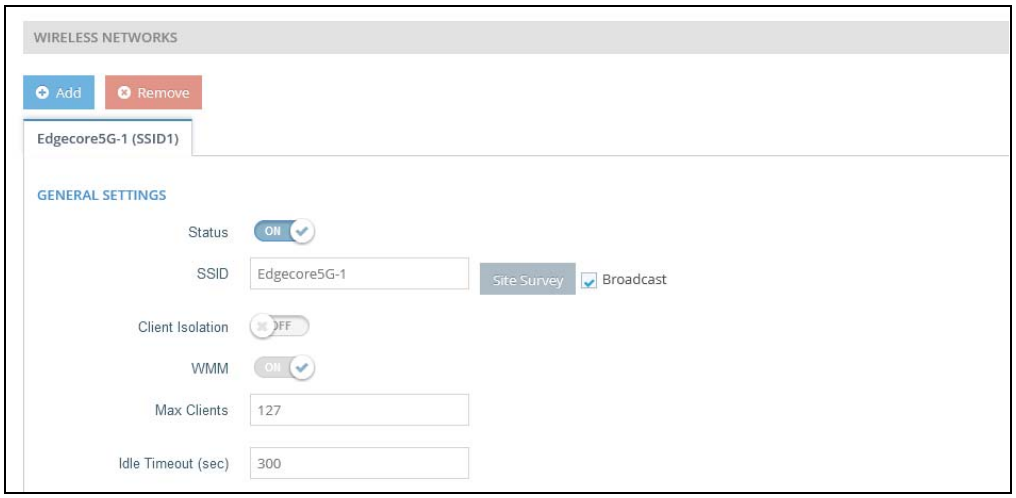
- **Channel** — The radio channel that the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the channel on neighboring access points at least five channels apart to avoid interference with each other. For example, for 11g/n 20 MHz 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)

- **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)

Wireless Networks — General Settings

Figure 27: Radio Settings (General Settings)



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)

- **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)

- **WMM** — Sets the WMM operational mode on the access point. The access point implements QoS using the Wi-Fi Multimedia (WMM) standard. Using WMM, the access point is able to prioritize traffic and optimize performance when multiple applications compete for wireless network bandwidth at the same time.(Default: Enabled)

- **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

Figure 28: Wireless 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: No Security)

  - **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** — 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.

- **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 offers backward compatibility with WPA2 and WPA.

- **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.

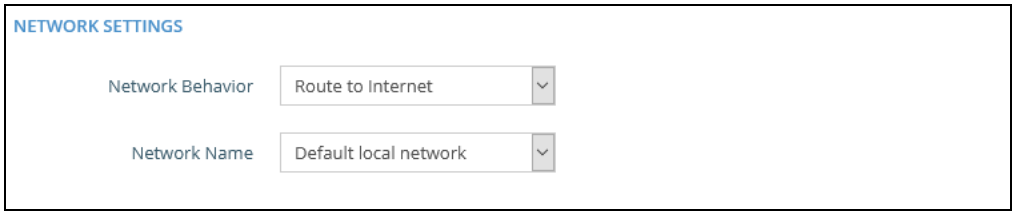
- **Access Control List** — Wireless clients can be authenticated for network access by checking their MAC address against the local database configured on the access point. (Default: OFF)

  - **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 29: Wireless Network Settings



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 22, "Bridge to Internet", on page 37.)
  - **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 23, "Route to Internet", on page 37.)
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.
  - **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 49.
    - **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.

Wireless Networks — Advanced Radio Settings

Figure 30: 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.)

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 31: Configuring VLANs

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.
- **PPPoE Profile** — Enable or disable PPPoE Profile for 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).

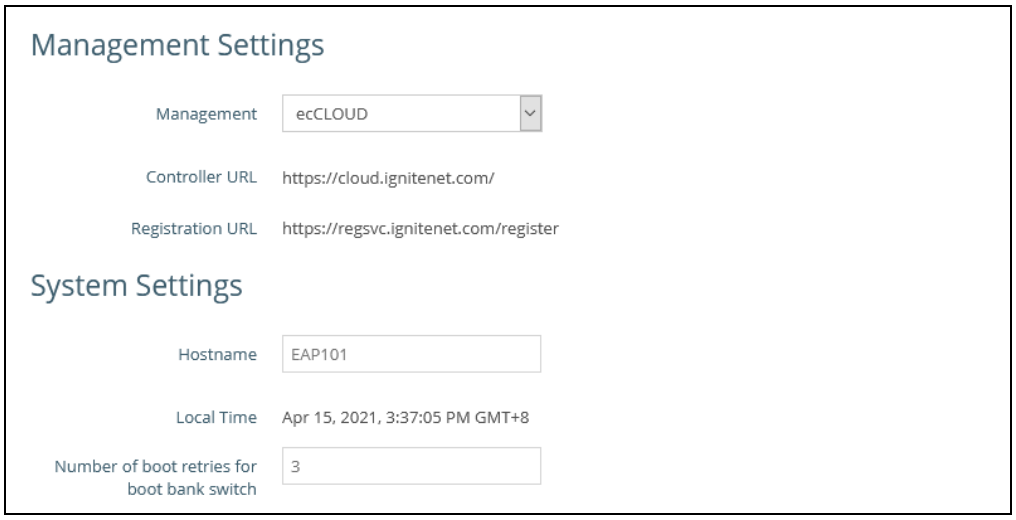
5 System Settings

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

System Settings

The System Settings page can be used to enable the AP to be managed from the Edgecore ecCLOUD controller and configure general descriptive information about the AP, such as the system identification name and local time.

Figure 32: System Settings



The following items are displayed on this page:

- **Management** — Set to "ecCLOUD" to manage this AP from the Edgecore ecCLOUD controller. Set to disable to manage the AP through the web interface in a stand-alone mode.
  - **Controller URL** — Specifies the URL for the Edgecore ecCLOUD controller management site.
  - **Registration URL** — Specifies the URL for device registration.
- **Hostname** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: EAP101; Range: 0-50 characters)
- **Local Time** — The local time, given as day of week, month, time, year.
- **Number of boot retries for boot bank switch** — The maximum number of bootup retries before switching to the next boot bank.
  (Range: 1-254; Default: 3)

Maintenance

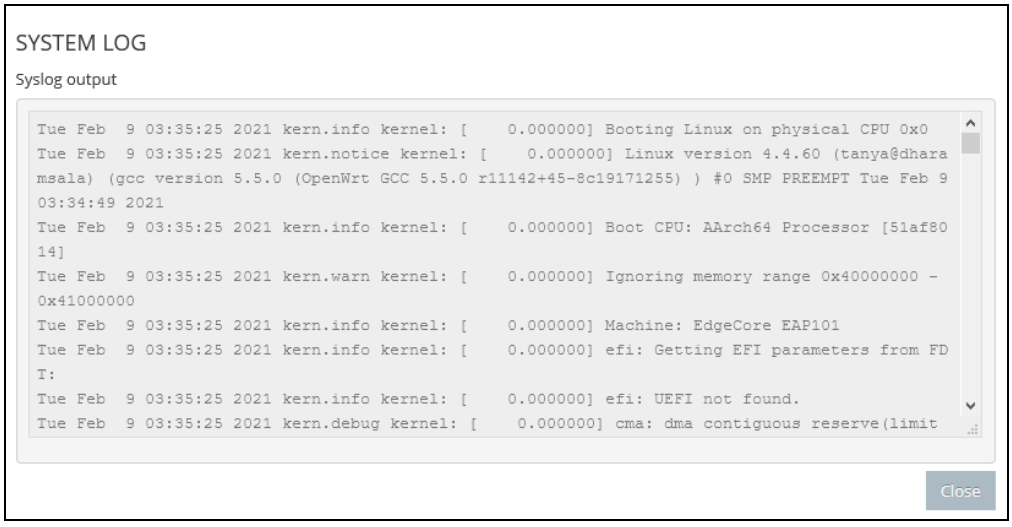
The Maintenance page supports general maintenance tasks including displaying the system log, downloading a diagnostics log, rebooting the device, restoring factory defaults, backing up or restoring configuration settings, and upgrading firmware.

Figure 33: 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 34: System Log



Downloading the Diagnostics Log

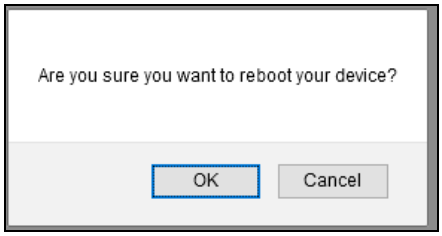
Click "Diagnostics Log" to download the log file to the management workstation. In Windows, a GNU Zip (*.tar.gz) file is stored in the Downloads folder.

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.

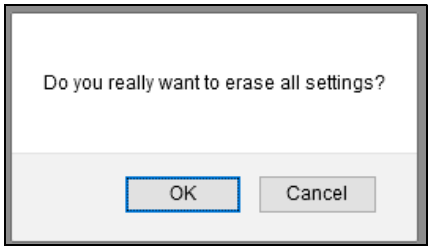
Figure 35: Rebooting the Access Point



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 36: 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.

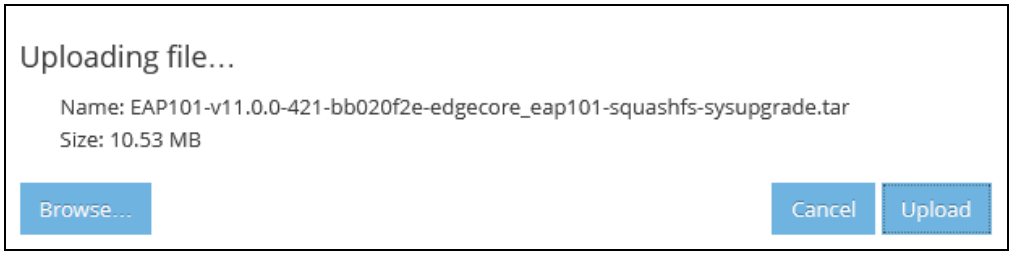
Figure 37: Restoring Configuration Settings

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.

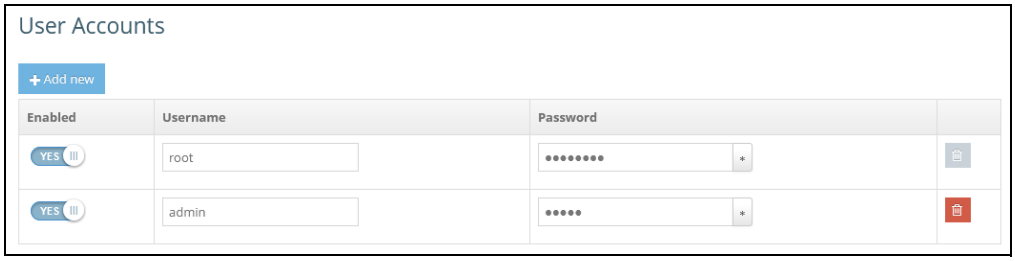
Figure 38: Upgrading Firmware



User Accounts

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

Figure 39: User Accounts



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

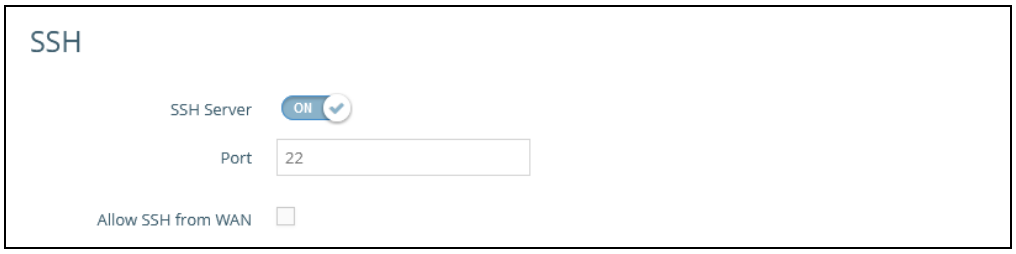
The Services page allows you to control SSH management access to the AP, configure NTP time servers, and configure iBeacon settings.

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 40: SSH Settings



The following items are displayed on this page:

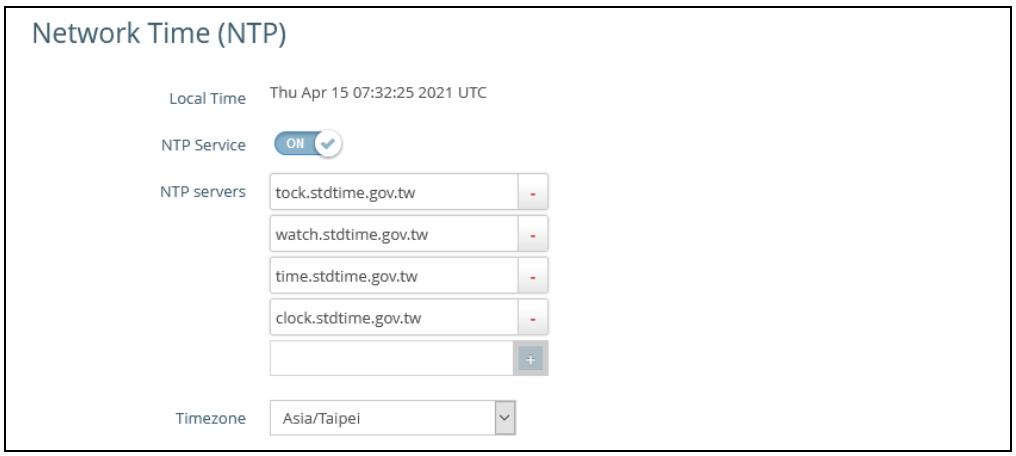
- **SSH Server** — Enables or disables SSH access to the access point. (Default: Enabled)
- **Port** — Sets the TCP port number for the SSH server on the access point. (Range: 1-65535; Default: 22)
- **Allow SSH from WAN** — Allows SSH management access from the WAN.

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 41: NTP Settings



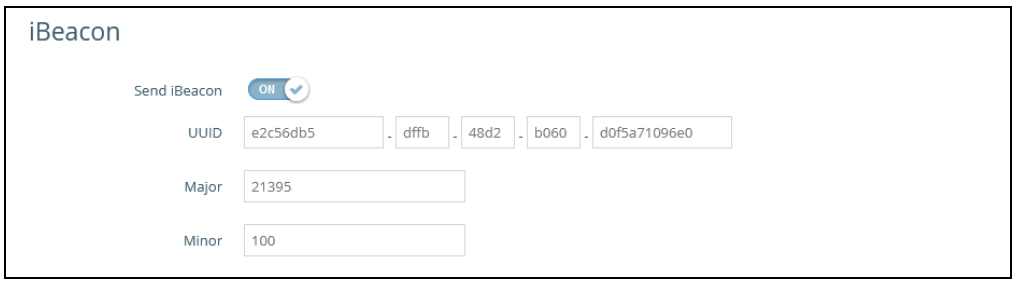
The following items are displayed on this page:

- **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.

iBeacon

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 42: iBeacon 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)

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 43: Network Utilities

Section III

Appendices

This section provides additional information and includes these items:

A Troubleshooting

Problems Accessing the Management Interface

Table 1: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser	◆ 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	◆ 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.