Edge-corE®

IEEE 802.11a/ac/b/g/n Wireless Access Point

ECW5212

Software Release v2.1.1.36r197

Management Guide

www.edge-core.com

Management Guide

ECW5212 Wireless Access Point

IEEE 802.11a/ac/b/g/n Dual-Band Access Point
with one 1000BASE-T (RJ-45 PoE-Input) Port,
and an Adaptive-MIMO Smart Antenna Array

15020000xxxxA
E052016-CS-R01

How to Use This Guide

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

How This Guide is Organized

The organization of this guide is based on the AP's main management interfaces. The web management interface is described in separate sections that follow the web menu. 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 the AP. For specific information on how to install the AP, see the following guide:

Quick Start Guide

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

Quick Start Guide
Safety and Regulatory Information

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.

Warning: Alerts you to a potential hazard that could cause personal injury.

Revision History

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

May 2016 Revision

This is the first revision of this guide. It is valid for software release v2.1.1.36r197.

Contents

Figures

Tables

Section I

Getting Started

This section describes the basic settings required to access the AP’s 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.

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 such as Internet Explorer 9.x, Mozilla Firefox 35, and Google Chrome 39, or later versions. The AP's web management interface can be accessed from any computer attached to the network.

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 and statistics

Network Connections

Prior to accessing the AP's management agent through a network connection, you must first configure it with a valid IP address, subnet mask, and default gateway using the web interface or DHCP protocol.

The AP has a static default management address of 192.168.1.1 and a subnet mask of 255.255.255.0. If the AP's default IP address is not compatible with your network or a DHCP server is not available, the AP's IP address must be configured manually through the web interface.

First directly connect a PC to the AP's LAN port and log in to the web interface, as described in "Connecting to the Web Interface" on page 14. Follow the steps described in the "Setup Wizard" on page 15 to configure the basic settings. Then configure the AP with an IP address that is compatible with your network as described under "LAN Settings" on page 27.

Once the AP's IP settings are configured for your network, you can access the AP's management agent from anywhere within the attached network. The AP can be managed by any computer using a web browser.

Connecting to the Web Interface

The AP offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer 9.x, Mozilla Firefox 35 or later, and Google Chrome 39, or later versions.

You may want to make initial configuration changes by connecting a PC directly to the AP's LAN port. The AP has a default management IP address of 192.168.1.1 and a subnet mask of 255.255.255.0. 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 with192.168.1.x).

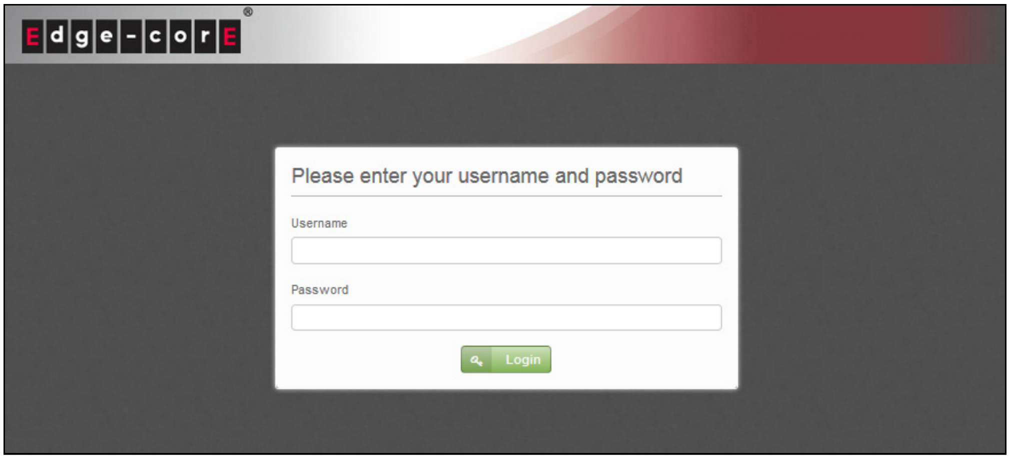
To access the AP's web management interface, follow these steps:

1. Use your web browser to connect to the management interface using the default IP address of 192.168.1.1.

2. Log in to the interface by entering the default user name "root" with the password "admin123," and then click Login.

Note: It is strongly recommended to change the default password the first time you access the web interface. For information on changing the user password, see "Password" on page 37.

Figure 1: Login Page



Please enter your username and password

Username

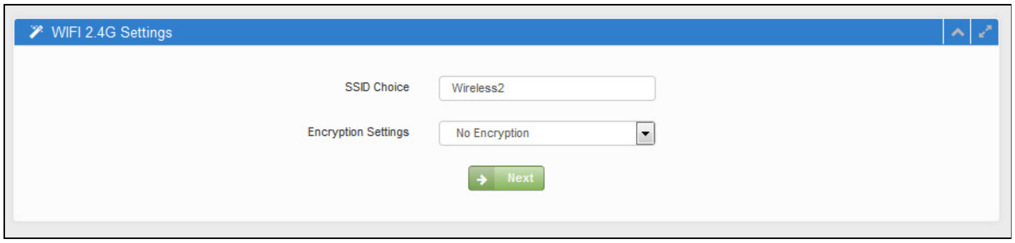
Password

Setup Wizard

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

Step 1 **Setting WIFI 2.4G** — Click Wizard on the main menu, and then set the SSID and encryption method for the 2.4 GHz wireless band.

Figure 2: Setting WIFI 2.4G



WIFI 2.4G Settings

SSID Choice: Wireless2

Encryption Settings: No Encryption

This page includes the following items:

SSID Choice – The name of the basic service set provided by a Virtual Access Point (VAP) interface. Clients who want to connect to the network through the access point must set their SSID to the same as that of the AP's VAP interface. Note that each radio supports 8 virtual access point (VAP) interfaces based on the SSIDs, referred to as VAP 0 ~ VAP 7, and are named Wireless2 - Wireless2.7 by default.

Encryption Settings – The wireless security method used for this VAP, including association mode, encryption, and authentication. (Default: No Encryption)

The following security options are supported:

- **No Encryption** – 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.

- **WEP Open System** – 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.

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

    WEP is the security protocol initially specified in the IEEE 802.11 standard for wireless communications. Unfortunately, WEP has been found to be seriously flawed and cannot be recommended for a high level of network security. For more robust wireless security, the access point provides Wi-Fi Protected Access (WPA) and WPA2 for improved data encryption and user authentication.

    Be sure that the WEP shared keys are the same for each client in the wireless network. All clients share the same keys, which are used for data encryption.

    For 64-bit WEP, string length must be 5 ASCII characters (letters and numbers) or 10 hexadecimal digits. For 128-bit WEP, string length must be 13 ASCII characters (letters and numbers) or 26 hexadecimal digits.

- **WEP Shared Key** – 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 if the WEP keys set by the client matches those set on the AP. When using this encryption option, the WEP keys are used both to authenticate the client and to encrypt the data transmitted.

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

    Be sure that the WEP shared keys are the same for each client in the wireless network. All clients share the same keys, which are used for authentication and data encryption.

    For 64-bit WEP, string length must be 5 ASCII characters (letters and numbers) or 10 hexadecimal digits. For 128-bit WEP, string length must be 13 ASCII characters (letters and numbers) or 26 hexadecimal digits.

- **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.

- **Cipher** – Data encryption uses one of the following methods:
  - **AES (CCMP)** – This method is used as the unicst encryption cipher. AES-CCMP is the standard encryption cipher required for WPA2.
  - **TKIP** – TKIP is used as the unicast encryption cipher.
  - **AES/TKIP Mixed** – This option of WPA with **"**TKIP or AES**"** allows you to run a mixed network: Those devices that support WPA2 with AES will use that system, less advanced devices that only support WPA will use WPA with TKIP. (This is the default setting.)
- **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-PSK / WPA2-PSK Mixed Mode** – The TKIP/AES type is the only encryption available for mixed WPA/WPA2 security. In mixed mode, the unicast encryption (TKIP or AES) is negotiated for each client as they associate with the network.

- **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.

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 Authentication Server** – Specifies the IP address or host name of the RADIUS authentication server.
- **Radius Authentication Port** – The UDP port number used by the RADIUS server for authentication messages. (Range: 1024-65535; Default: 1812)
- **Radius Authentication Secret** — A shared text string used to encrypt messages be sent tween 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)

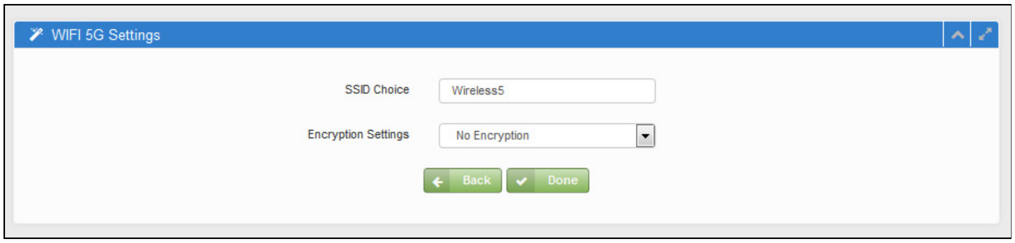
◆ **WPA2-EAP** —WPA was introduced as an interim solution for the vulnerability of WEP pending the ratification of the IEEE 802.11i wireless security standard. In effect, the WPA security features are a subset of the 802.11i standard. WPA2 includes the now ratified 802.11i standard, but also offers backward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

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

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

Step 2 **Setting WIFI 5G** — Click Next, and set the SSID and encryption method for the 5 GHz wireless band.

Figure 3: Setting WIFI 5G


WIFI 5G Settings

SSID Choice: Wireless5

Encryption Settings: No Encryption

Refer to Setting WIFI 2.4G for a description of the configuration options.

Main Menu

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

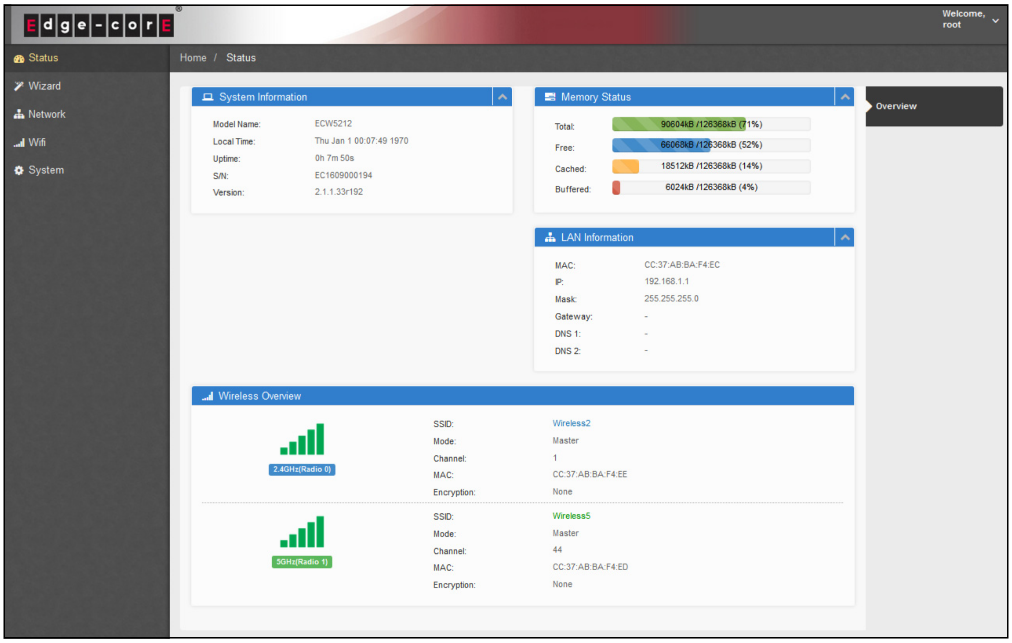
To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **Status** — The status page shows basic settings for the AP, including a description of the system, memory usage, local network settings, and wireless radio settings. See "Status Information" on page 23.
- **Network** — Configures Ethernet LAN and SSH access settings. See "Network Settings" on page 27.
- **WIFI** — Configures 5 GHz Radio and 2.4 GHz Radio settings. See "Wireless Settings" on page 29.
- **System** — Displays the system log, configures the system time, user accounts, and Maintenance (such as firmware upgrade, and reset). See "System Settings" on page 35.

Status

After logging in to the web interface, the status page displays. This page shows basic settings for the AP, including Internet status, local network settings, wireless radio status, client connections, and traffic graphs.

Figure 4: Status Overview



System Information

Model Name: ECW5212
Local Time: Thu Jan 1 00:07:49 1970
Uptime: 0h 7m 50s
S/N: EC1609000194
Version: 2.1.1.33r192

Memory Status

Total: 90604kB /126368kB (71%)
Free: 66068kB /126368kB (52%)
Cached: 18512kB /126368kB (14%)
Buffered: 6024kB /126368kB (4%)

LAN Information

MAC: CC:37:AB:BA:F4:EC
IP: 192.168.1.1
Mask: 255.255.255.0
Gateway: -
DNS 1: -
DNS 2: -

Wireless Overview

2.4GHz(Radio 0)
SSID: Wireless2
Mode: Master
Channel: 1
MAC: CC:37:AB:BA:F4:EE
Encryption: None

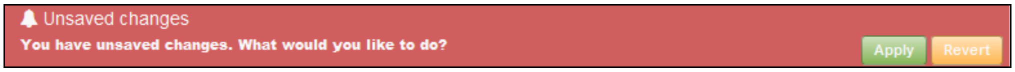
5GHz(Radio 1)
SSID: Wireless5
Mode: Master
Channel: 44
MAC: CC:37:AB:BA:F4:ED
Encryption: None

Common Web Page Buttons

The list below describes common buttons found on most 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 "Apply" button.

Figure 5: Set Configuration Changes



Unsaved changes

You have unsaved changes. What would you like to do?

- **Apply** – Saves the current configuration so that it is retained after a restart.

- **Revert** – Cancels the newly entered settings and restores the originals.

- **Welcome > Logout** – Open the Welcome list and click Logout to end 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 23
- "Network Settings" on page 27
- "Wireless Settings" on page 29
- "System Settings" on page 35

2

Status Information

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

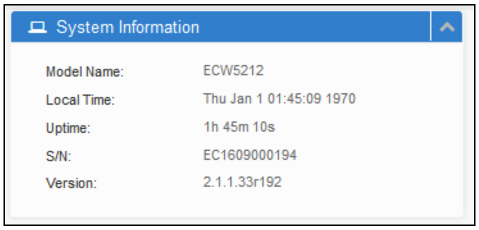
Status Information includes the following sections:

- "System Information" on page 23
- "Memory Status" on page 24
- "LAN Information" on page 24
- "Wireless Overview" on page 25

System Information

The System Information section shows descriptive information about the AP.

Figure 6: System Information



Model Name:	ECW5212
Local Time:	Thu Jan 1 01:45:09 1970
Uptime:	1h 45m 10s
S/N:	EC1609000194
Version:	2.1.1.33r192

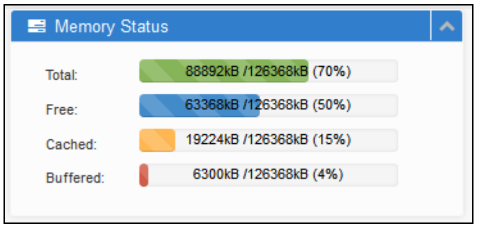
The following items are displayed in this section:

- **Model Name** — The model number of the unit.
- **Local Time** — The current system date and time.
- **Uptime** — Length of time the management agent has been up.
- **S/N** — The serial number of the physical access point.
- **Version** — The software version number.

Memory Status

The Memory Status section shows information about memory usage.

Figure 7: Memory Status



Memory Status

Total:	88892kB /126368kB (70%)
Free:	63368kB /126368kB (50%)
Cached:	19224kB /126368kB (15%)
Buffered:	6300kB /126368kB (4%)

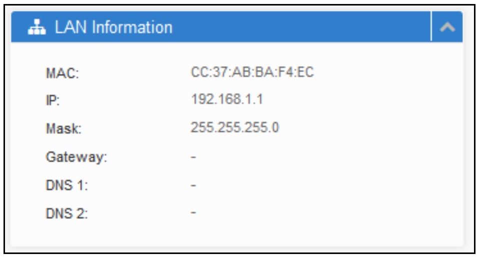
The following items are displayed in this section:

- **Total** — The total amount of memory space, and the percentage in use.
- **Free** — The amount of free memory.
- **Cached** — The amount of cached memory in use.
- **Buffered** — The amount of buffered memory in use.

LAN Information

The LAN Information section shows information about the local network connection.

Figure 8: LAN Information



LAN Information

MAC:	CC:37:AB:BA:F4:EC
IP:	192.168.1.1
Mask:	255.255.255.0
Gateway:	-
DNS 1:	-
DNS 2:	-

The following items are displayed in this section:

- **MAC** — MAC address assigned to the LAN port interface.
- **IP** — The IP address of the AP.
- **Mask** — Network mask for the IP subnet. This mask identifies the host address bits used for routing to specific subnets.

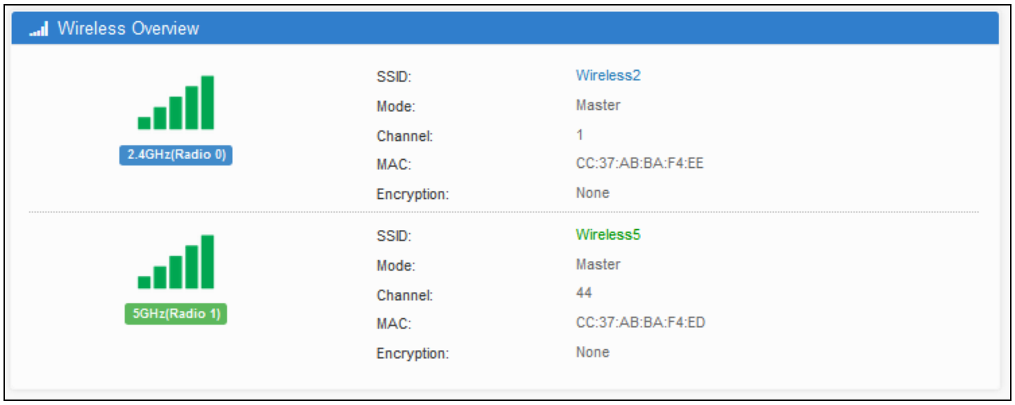
- **Gateway** — The IP address of the default gateway router that is used when a destination address is not on the local subnet.

- **DNS 1 / DNS 2** — Shows configured Domain Name Server IP addresses.

Wireless Overview

The Wireless Overview section shows information about the radio settings.

Figure 9: Wireless Overview



SSID: Wireless2
Mode: Master
Channel: 1
MAC: CC:37:AB:BA:F4:EE
Encryption: None

SSID: Wireless5
Mode: Master
Channel: 44
MAC: CC:37:AB:BA:F4:ED
Encryption: None

The following items are displayed in this section:

- **Radio #** — Indicates the 5 GHz (Radio 0) or 2.4 GHz (Radio 1) wireless interface.

- **SSID** — Service set identifier. Clients that want to connect to the wireless network must set their SSIDs to the same as that of the access point.

- **Mode** — Indicates Master (Access Point) or Client.

- **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode[1], Channel Bandwidth, and Country Code settings[2].

- **MAC** — MAC address assigned to this AP interface.

- **Encryption** — The encryption method configured on this interface.

[1] See "Basic Settings" on page 29.

[2] See "Setup Wizard" on page 15.

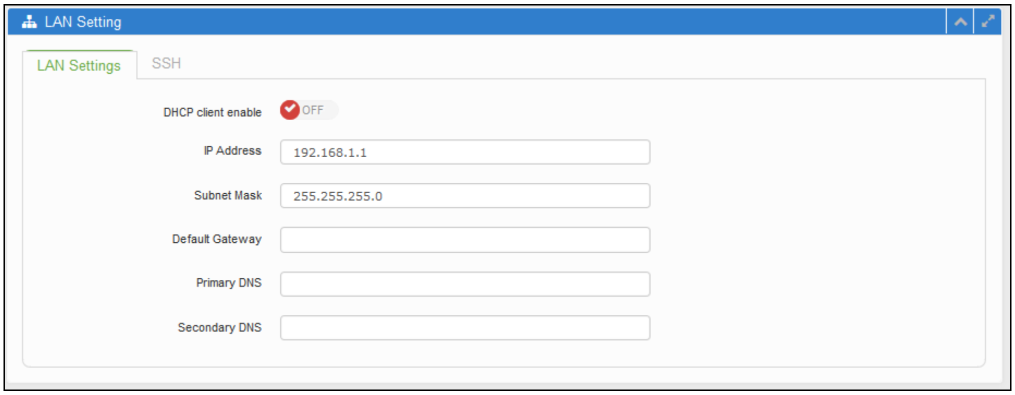
3 Network Settings

This chapter describes LAN and SSH settings. It includes the following sections:

LAN Settings

The LAN Setting fields configure the basic Internet settings for the AP.

Figure 10: LAN Settings



LAN Setting

LAN Settings | SSH

DHCP client enable	OFF
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS	
Secondary DNS	

The following items are displayed in this menu:

- **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, enter the IP address of the default gateway router in the text field provided.
- **Primary DNS Server** — The IP addresses of the primary domain name server.

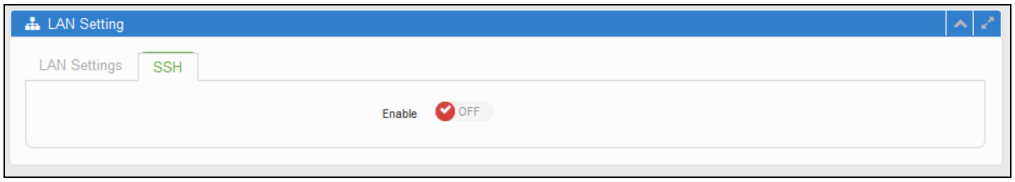
- **Secondary DNS Server** — The IP addresses of the secondary domain name server.

SSH Setting

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 11: SSH Setting



Enable ✓ OFF

4

Wireless Settings

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

- "Basic Settings" on page 29
- "Advanced Settings" on page 32

Basic Settings

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

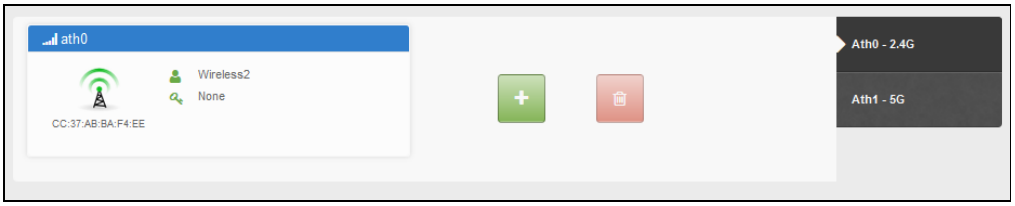
The access point can operate in several radio modes, 802.11a/n/ac (5 GHz) or 802.11b/g/n (2.4 GHz). Note that dual-band access points can operate at 2.4 GHz and 5 GHz at the same time. The web interface identifies the radio configuration pages as:

- **Ath0 - 2.4G** — the 2.4 GHz 802.11b/g/n radio interface
- **Ath1 - 5G** — the 5 GHz 802.11a/ac/n radio interface

Each radio supports 8 virtual access point (VAP) interfaces based on the SSIDs, referred to as VAP 0 ~ VAP 7. Each VAP functions as a separate access point, and can be configured with its own Service Set Identification (SSID) and security settings. 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. The AP supports up to a total of 127 wireless clients across all VAP interfaces per radio.

The basic configuration settings for the radios are shown on the Basic page. To select 5G and 2.4G radios, click the Ath0 - 2.4G or Ath1 - 5G tab.

Figure 12: Basic Radio Configuration Status



ath0

Wireless2

None

CC:37:AB:BA:F4:EE

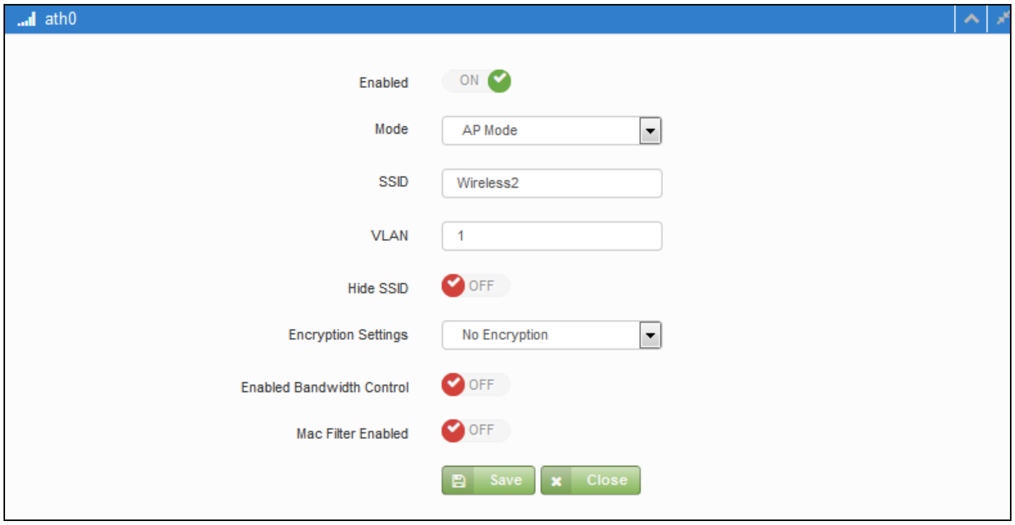
The following items are displayed on this page:

WLAN radio status for each VAP.

- **Enabled** — Shows if the wireless service on this VAP is enabled.
- **SSID** — The name of the basic service set used by a VAP interface.
- **Encryption** — Shows the type of encryption used on this interface.

Click on the box for any of the VAPs to open the configuration dialog box for basic radio settings

Figure 13: Basic Radio Configuration Dialog Box


ath0

Enabled: ON

Mode: AP Mode

SSID: Wireless2

VLAN: 1

Hide SSID: OFF

Encryption Settings: No Encryption

Enabled Bandwidth Control: OFF

Mac Filter Enabled: OFF

The following items are displayed on this page:

- **Enabled** — Enables or disables the wireless service on this interface.
- **Mode** — This setting determines how the VAP interface operates. The AP supports the following options:
  - **AP Mode** — In this mode, the VAP provides services to wireless clients as a normal access point. (This is the default setting.)
  - **AP WDS Mode** — The VAP operates as an access point in WDS mode, which accepts connections from access points in Client WDS Mode. WDS is used to automatically search for and connect to other access points using the same SSID and security settings.
  - **Client WDS Mode** — The VAP operates as a client station in WDS mode, which can connect to other access points in AP WDS Mode.

- **SSID** — The name of the basic service set used by a 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: ACN0.# (where # is 0-7) for 5 GHz, ACN1.# (where # is 0-7) for 2.4 GHz; Range: 1-32 characters)

- **VLAN** — Wireless clients are assigned to the VLAN for the VAP interface to 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. (Default: 1; Range: 1-4095)

Note: 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.

- **Hide SSID** — Removes the SSID from beacon frames. Also known as network cloaking, this security measure is less effective than using WPA or WPA2. There are many tools that allow you to "find" the supposedly "hidden" network name. (Default: Off)

- **Encryption Settings** — The encryption options are described under Step 1 in the Introduction. (Default: No Encryption)

- **Enable Bandwidth Control** — Enables rate limiting of traffic to and from the VAP interface as it is passed to and from the wired network. You can set a maximum rate in Kbytes per second. (Range: 0 (unlimited) or 512-1024000 Kbytes per second; Default: OFF)

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

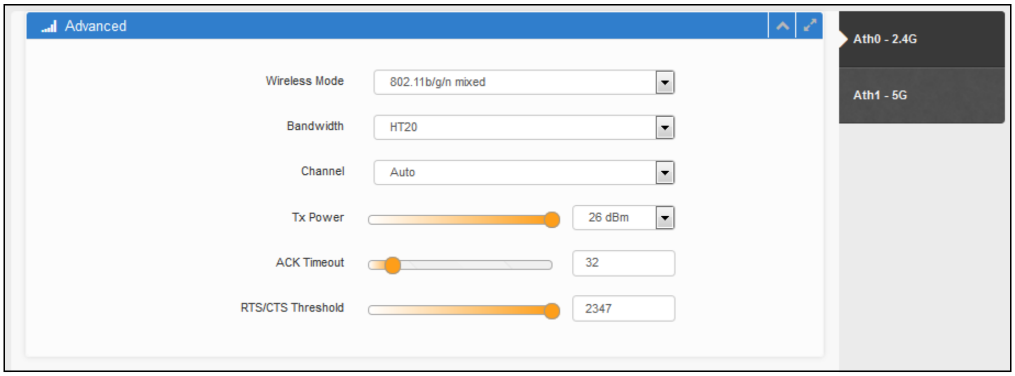
  - **MAC Filter Rule** — The MAC list can be configured to either accept or deny network access to specified clients. (Default: Deny)

  - **MAC Filter Address** — Enter a physical address for each client. Enter six pairs of hexadecimal digits separated by colons. For example, 00:90:D1:12:AB:89.

Advanced Settings

This section includes configuration settings for the radio operating mode and related parameters.

Figure 14: Advanced Radio Configuration Dialog Box



Wireless Mode: 802.11b/g/n mixed

Bandwidth: HT20

Channel: Auto

Tx Power: 26 dBm

ACK Timeout: 32

RTS/CTS Threshold: 2347

The following items are displayed on this page:

- **Wireless Mode** — Defines the radio operation mode.
  - **Radio 0** (2.4 GHz Radio) — Default: 802.11b/g/n mixed; Options: 802.11b, 802.11g.
  - **Radio 1** (5 GHz Radio) — Default: 802.11a/n/ac mixed; Options: 802.11a/n mixed, 802.11a.
- **Bandwidth** — The channel bandwidth of the radio interface:
  - **Radio 0** (2.4 GHz Radio) — The radio interface provides a channel bandwidth of 20 MHz by default, which ensures backward compatibility for slower 802.11b devices. Setting the channel bandwidth to 40 MHz increases connection speed by bonding two 20 MHz channels together. You can select to bond either the channel immediately above or below the current channel. (Default: HT20; Options: HT40 channel below, HT40 channel above)
  - **Radio 1** (5 GHz Radio) — The radio interface provides a channel bandwidth of 80 MHz (referred to as Very High Throughput mode) by default. To ensure backward compatibility or to reduce channel interference, you can also select slower 20 MHz or 40 MHz channel bandwidths. (Default: VHT80; Options: HT20, HT40 channel below, HT40 channel above)
- **Channel** — The radio channel the access point uses to communicate with wireless clients. When multiple access points are deployed in the same area, set the 2.4 GHz 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 and channel bandwidth settings. A setting of "Auto" lets the access point set an available channel with the least interference. (Default: Radio 0 - Auto, Radio 1 - Auto)

Table 1: Radio Channels

Radio 0 (2.4 GHz)		Radio 1 (5 GHz)	
Radio Channels	Frequency (GHz)	Radio Channels*	Frequency (GHz)
1	2.412	36	5.180
2	2.417	40	5.200
3	2.422	44	5.220
4	2.427	48	5.240
5	2.432	149	5.745
6	2.437	153	5.765
7	2.442	157	5.785
8	2.447	161	5.805
9	2.452		
10	2.457		
11	2.462		

* Supported channels depend on the 802.11 mode and channel bandwidth.

- **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 about coverage area, 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 regulatory limitations for the radio band.)

- **ACK Timeout** — Sets the acknowledgement timeout, which is used primarily for long-distance connections. This timeout is used to make an adjustment for link distance. It is based on the amount of time, in microseconds, that it should take to transmit a frame to the other end of the link, be processed by the receiving device, and have the ACK frame created and returned to the sending device. (Range: 0-255 microseconds; Default: 32 microseconds)

- **Fragmentation Threshold** (802.11b/g modes only) — Sets the maximum frame size above which packets are fragmented. Using a lower threshold reduces the time required to transmit the frame, and therefore reduces the probability that it will be corrupted (at the cost of more data overhead). (Range: 256-2346 bytes; Default: 2346 bytes)

- **RTS/CTS Threshold** (2.4 GHz radio only) — Sets the packet size threshold at which a Request to Send (RTS) frame must be sent to a receiving station prior to the sending station starting communications. The access point sends CTS (clear to send) frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the access point sends a CTS frame to notify the sending station that it can start sending data.

  If the RTS threshold is set to 0, the access point always sends RTS signals. If set to 2347, the access point never sends RTS signals. If set to any other value, and the packet size equals or exceeds the RTS threshold, the RTS/CTS (Request to Send / Clear to Send) mechanism is enabled.

  The access points contending for the medium may not be aware of each other. The RTS/CTS mechanism can solve this "Hidden Node Problem." (Range: 0-2347 bytes: Default: 2347 bytes)

5

System Settings

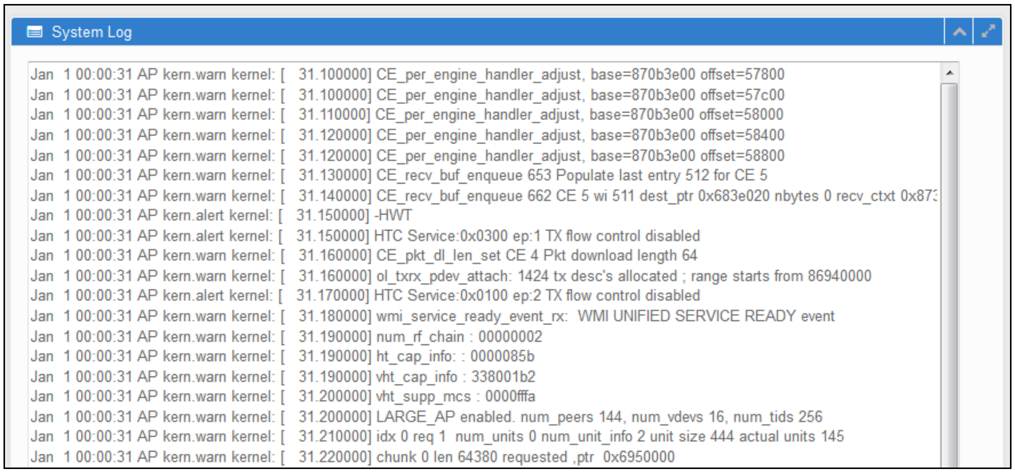
This chapter describes maintenance settings on the access point. It includes the following sections:

- "System Log" on page 35
- "NTP" on page 36
- "Password" on page 37
- "Maintenance" on page 38

System Log

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

Figure 15: System Log



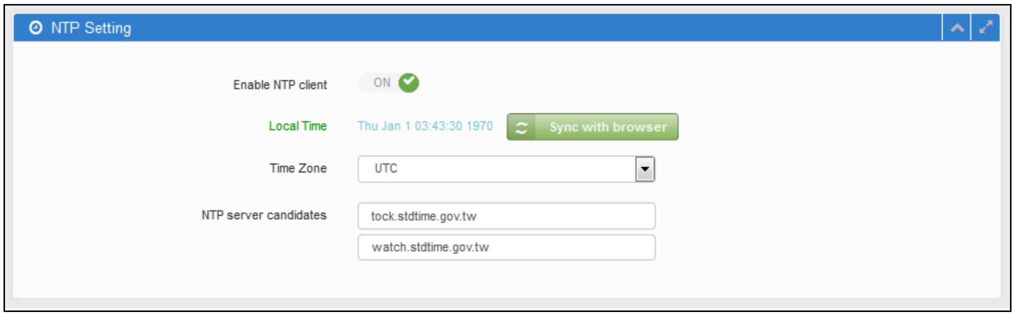
```
Jan  1 00:00:31 AP kern.warn kernel: [   31.100000] CE_per_engine_handler_adjust, base=870b3e00 offset=57800
Jan  1 00:00:31 AP kern.warn kernel: [   31.100000] CE_per_engine_handler_adjust, base=870b3e00 offset=57c00
Jan  1 00:00:31 AP kern.warn kernel: [   31.110000] CE_per_engine_handler_adjust, base=870b3e00 offset=58000
Jan  1 00:00:31 AP kern.warn kernel: [   31.120000] CE_per_engine_handler_adjust, base=870b3e00 offset=58400
Jan  1 00:00:31 AP kern.warn kernel: [   31.120000] CE_per_engine_handler_adjust, base=870b3e00 offset=58800
Jan  1 00:00:31 AP kern.warn kernel: [   31.130000] CE_recv_buf_enqueue 653 Populate last entry 512 for CE 5
Jan  1 00:00:31 AP kern.warn kernel: [   31.140000] CE_recv_buf_enqueue 662 CE 5 wi 511 dest_ptr 0x683e020 nbytes 0 recv_ctxt 0x873
Jan  1 00:00:31 AP kern.alert kernel: [   31.150000] -HWT
Jan  1 00:00:31 AP kern.alert kernel: [   31.150000] HTC Service:0x0300 ep:1 TX flow control disabled
Jan  1 00:00:31 AP kern.warn kernel: [   31.160000] CE_pkt_dl_len_set CE 4 Pkt download length 64
Jan  1 00:00:31 AP kern.warn kernel: [   31.160000] ol_txrx_pdev_attach: 1424 tx desc's allocated ; range starts from 86940000
Jan  1 00:00:31 AP kern.alert kernel: [   31.170000] HTC Service:0x0100 ep:2 TX flow control disabled
Jan  1 00:00:31 AP kern.warn kernel: [   31.180000] wmi_service_ready_event_rx:  WMI UNIFIED SERVICE READY event
Jan  1 00:00:31 AP kern.warn kernel: [   31.190000] num_rf_chain : 00000002
Jan  1 00:00:31 AP kern.warn kernel: [   31.190000] ht_cap_info: : 0000085b
Jan  1 00:00:31 AP kern.warn kernel: [   31.190000] vht_cap_info : 338001b2
Jan  1 00:00:31 AP kern.warn kernel: [   31.200000] vht_supp_mcs : 0000fffa
Jan  1 00:00:31 AP kern.warn kernel: [   31.200000] LARGE_AP enabled. num_peers 144, num_vdevs 16, num_tids 256
Jan  1 00:00:31 AP kern.warn kernel: [   31.210000] idx 0 req 1  num_units 0 num_unit_info 2 unit size 444 actual units 145
Jan  1 00:00:31 AP kern.warn kernel: [   31.220000] chunk 0 len 64380 requested ,ptr  0x6950000
```

NTP

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 16: NTP



Enable NTP client: ON ✓

Local Time: Thu Jan 1 03:43:30 1970

Time Zone: UTC

NTP server candidates: tock.stdtime.gov.tw
watch.stdtime.gov.tw

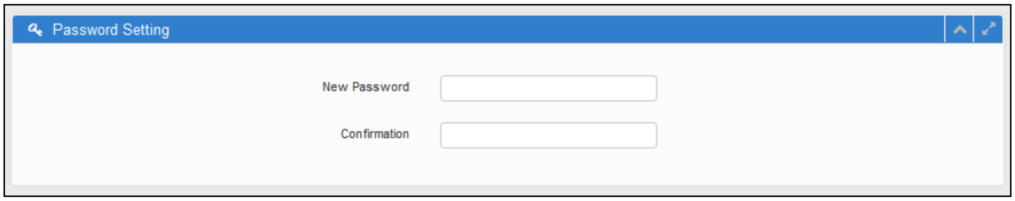
The following items are displayed on this page:

- **Enable NTP Client** — Enables or disables sending of requests for time updates. (Default: Enabled)
- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **Sync with browser** — Click to update the system time based on the management computer hosting the browser session.
- **Time Zone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.
- **NTP Server Candidates** — 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.

Password

The Password page sets the password for the system administrator.

Figure 17: Password



Password Setting

New Password

Confirmation

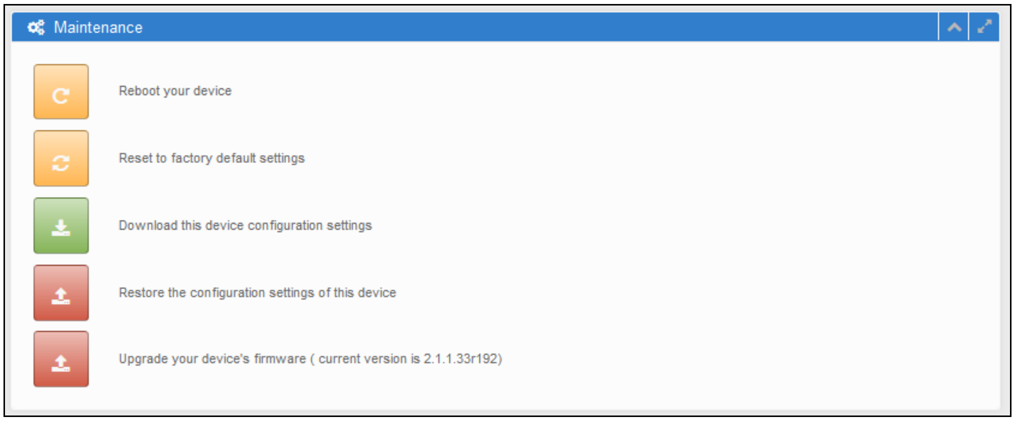
The following items are displayed on this page:

- **New Password** — The system administrator's password. (Range: 3-15 ASCII characters, case sensitive, no special characters; Default: admin123)
- **Confirmation** — Enter the password again for verification.

Maintenance

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

Figure 18: Maintenance



Maintenance

Reboot your device

Reset to factory default settings

Download this device configuration settings

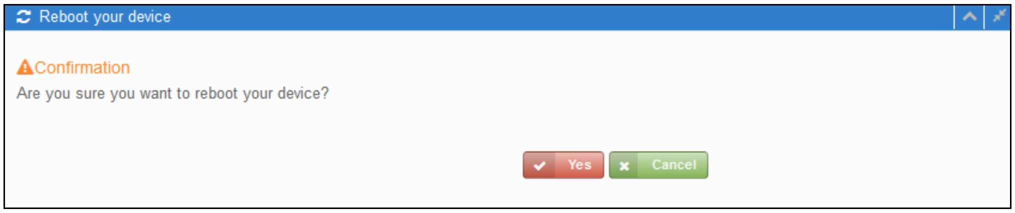
Restore the configuration settings of this device

Upgrade your device's firmware (current version is 2.1.1.33r192)

Rebooting the Access Point

The “Reboot your device” page allows you to reboot the access point.

Figure 19: Reboot your device



Reboot your device

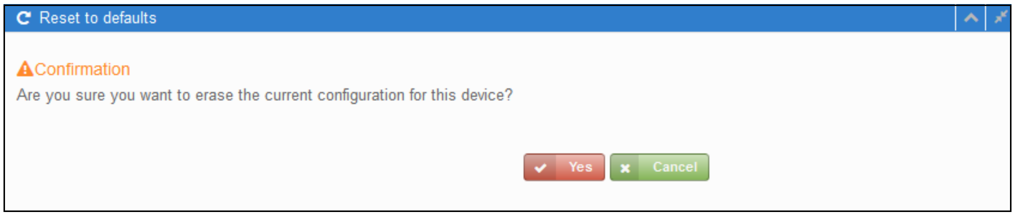
⚠Confirmation

Are you sure you want to reboot your device?

Resetting the Access Point

The “Reset to factory default settings” 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 regain management access to this device.

Figure 20: Resetting to Defaults



Reset to defaults

⚠Confirmation

Are you sure you want to erase the current configuration for this device?

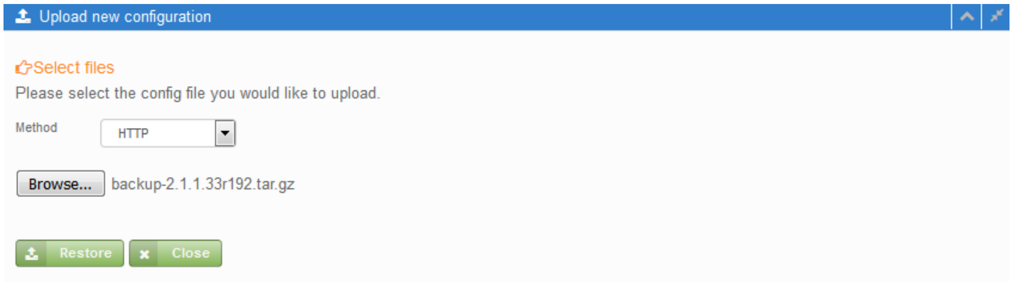
Backing Up Configuration Settings

The “Download this device’s configuration settings” page 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-2.1.1.33r192.tar.gz

Restoring Configuration Settings

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

Figure 21: Restoring Configuration Settings



Upload new configuration

Select files

Please select the config file you would like to upload.

Method: HTTP

backup-2.1.1.33r192.tar.gz

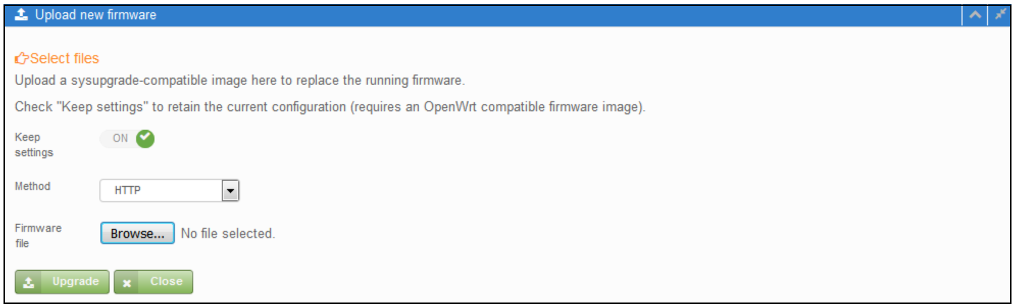
Click the Browse button to locate the configuration file, and then click the “Upload archive” button to begin restoring the configuration settings.

Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation.

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 22: Upgrading Firmware



Upload new firmware

Select files

Upload a sysupgrade-compatible image here to replace the running firmware.

Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings: ON ✓

Method: HTTP

Firmware file: No file selected.

Click the Browse button to locate the configuration file, and then click “Upgrade” to begin upgrading firmware.

Section III

Appendices

This section provides additional information and includes these items:

- "Troubleshooting" on page 43

A

Troubleshooting

Problems Accessing the Management Interface

Table 2: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser or Telnet/SSH	◆ 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 Telnet/SSH, you may have exceeded the maximum number of concurrent Telnet/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 > System Log menu, and copy the information from the log file.

5. Contact your distributor's service engineer, and send a detailed description of the problem, along with all of the information mentioned in the above steps.

Index