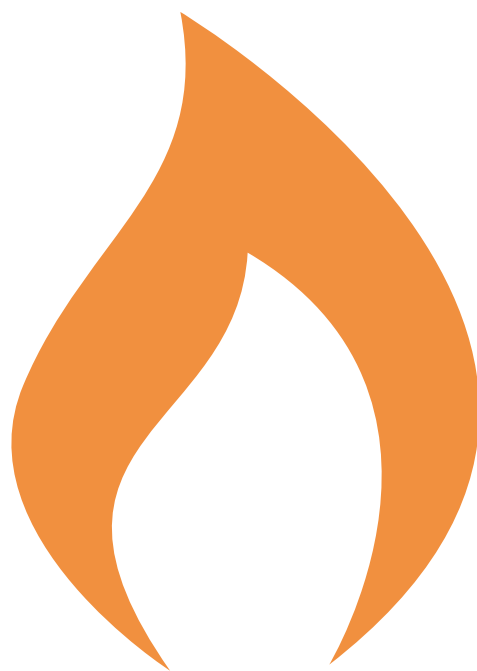




# User Manual

HeliOS

Software Release v1.1



# User Manual

**IgniteNet HeliOS**

Cloud-Enabled Enterprise Access Point Software

FW1.1.0  
E082015-CS-R01  
150000000056A

---

# How to Use This Guide

This guide includes detailed information on IgniteNet 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), 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 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*  
*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.

**August 2015 Revision**

This is the first revision of this guide. It is valid for software release v1.1.0.

---

# Contents

How to Use This Guide	3
Contents	5
Figures	8
Tables	10

---

<b>Section I</b>	<b>Getting Started</b>	<b>11</b>
	<b>1 Introduction</b>	<b>12</b>
	Configuration Options	12
	Network Connections	13
	Connecting to the Web Interface	13
	Setup Wizard	15
	Main Menu	19
	Dashboard	20
	Common Web Page Buttons	20

---

<b>Section II</b>	<b>Web Configuration</b>	<b>23</b>
	<b>2 Status Information</b>	<b>24</b>
	System and Product Information	24
	Internet Status	25
	Local Networks	26
	Wireless Status	27
	Traffic Graphs	29
	<b>3 Network Settings</b>	<b>30</b>
	Internet Settings	30
	Ethernet Settings	33

LAN Settings	35
Hotspot Settings	37
<b>4 Wireless Settings</b>	<b>40</b>
Radio Settings	40
Physical Radio Settings	41
Wireless Networks — General Settings	43
Wireless Networks — Security Settings	46
Wireless Networks — Network Settings	49
Advanced Radio Settings	50
VLAN Settings	54
<b>5 System Settings</b>	<b>56</b>
System Settings	57
Maintenance	58
Displaying System Logs	58
Downloading the Troubleshooting Log	59
Rebooting the Access Point	59
Resetting the Access Point	59
Backing Up Configuration Settings	60
Restoring Configuration Settings	60
Upgrading Firmware	60
User Accounts	61
Services	61
SSH	61
IgniteNet Discovery Tool	62
Telnet	62
Web Server	63
Network Time	64
SNMP	64
<b>Section III Appendices</b>	<b>67</b>
<b>A Troubleshooting</b>	<b>68</b>
Problems Accessing the Management Interface	68

Using System Logs	68
<b>Index</b>	<b>70</b>

---

# Figures

Figure 1: Login Page	14
Figure 2: Select Your Country	15
Figure 3: Select Cloud Managed	16
Figure 4: Select Setup Method	17
Figure 5: Easy Setup	17
Figure 6: Advanced Setup	18
Figure 7: Bridge to Internet	18
Figure 8: Route to Internet	19
Figure 9: The Dashboard	20
Figure 10: Set Configuration Changes	20
Figure 11: System and Product Information	24
Figure 12: Internet Status	25
Figure 13: Options	25
Figure 14: ARP Table	26
Figure 15: DHCP Leases	26
Figure 16: Local Networks	26
Figure 17: Wireless Status	27
Figure 18: Traffic Graphs	29
Figure 19: Internet Settings	30
Figure 20: IP Address Mode – Static IP	31
Figure 21: IP Address Mode – PPPoE	32
Figure 22: IP Alias	32
Figure 23: Ethernet Settings – Internet Source	33
Figure 24: Ethernet Settings – Network Behavior	34
Figure 25: Network – LAN Settings	35
Figure 26: Hotspot Settings (Network Settings)	37
Figure 27: Hotspot Settings (RADIUS Settings)	38
Figure 28: Hotspot Settings (Captive Portal Settings)	39
Figure 29: Radio Settings (Physical Radio Settings)	41



Figure 30: Radio Settings (Wireless Network Configuration)	43
Figure 31: WMM Backoff Wait Times	45
Figure 32: Wireless Security Settings	46
Figure 33: Wireless Network Settings	49
Figure 34: Advanced Radio Settings	50
Figure 35: Configuring VLANs	55
Figure 36: System Settings	57
Figure 37: Maintenance	58
Figure 38: System Log	58
Figure 39: Rebooting the Access Point	59
Figure 40: Resetting to Defaults	59
Figure 41: Restoring Configuration Settings	60
Figure 42: Upgrading Firmware	60
Figure 43: User Accounts	61
Figure 44: SSH Server Settings	62
Figure 45: IgniteNet Discovery Tool Settings	62
Figure 46: Telnet Server Settings	62
Figure 47: Web Server Settings	63
Figure 48: NTP Settings	64
Figure 49: SNMP Settings	64

---

# Tables

Table 1: Radio Channels	42
Table 2: WMM Access Categories	44
Table 3: 802.11 Data Rates	50
Table 4: Tx Power	52
Table 5: Troubleshooting Chart	68

# Section I

## Getting Started

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

This section includes these chapters:

- ◆ [“Introduction” on page 12](#)

# 1

## Introduction

---

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

---

### 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 or later, Mozilla Firefox 5 or later, and Google Chrome 35 or later. 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 Telnet or Secure Shell (SSH) connection over the network. The CLI is used primarily for technical support.

The AP's management agent also supports SNMP (Simple Network Management Protocol). This SNMP agent permits the AP to be managed from any computer in the network using network management software.

The AP's web interface, console interface, and SNMP agent allow you to perform management functions such as:

- ◆ Set management access user names and passwords
- ◆ Configure IP settings
- ◆ Configure SNMP parameters
- ◆ 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 the DHCP protocol.

The AP has a static default management address of 192.168.2.1 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 connect to the AP's Ethernet 1 port and log in to the web interface, as described in ["Connecting to the Web Interface" on page 13](#). Follow the steps described in ["Setup Wizard" on page 15](#) to select your country and specify one of the configuration methods. Then configure the AP with an IP address that is compatible with your network, as described under ["LAN Settings" on page 35](#).

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, or from a network computer using SNMP network management software.

---

## 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 or later, Mozilla Firefox 5 or later, and Google Chrome 35 or later.

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 192.168.2.1 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 with 192.168.2.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 192.168.2.1.
2. Log in to the interface by entering the default user name "root" with the password "admin123", then click Login.



**Note:** It is strongly recommended to change the default user name and password the first time you access the web interface. For information on changing user names and passwords, see [“User Accounts” on page 61](#).

**Figure 1: Login Page**

The image shows the login page for IgniteNet. At the top, the 'IgniteNet' logo is displayed in white, with a small orange flame icon above the 'i'. Below the logo, the text 'Access Point Login' is written in orange. The main content area is a white box with a dark border. Inside this box, the text 'Please enter your username & password' is centered. Below this text are three input fields: 'Username' with a user icon, 'Password' with a lock icon, and a language dropdown menu currently set to 'English'. At the bottom of the white box is a blue 'Login' button with a white magnifying glass icon.

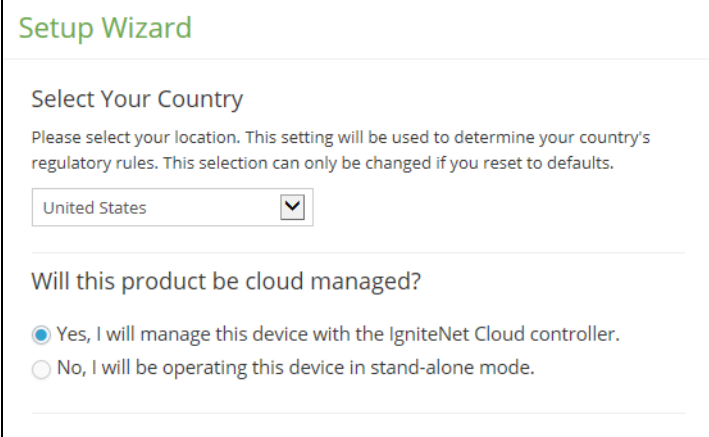
---

## Setup Wizard

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

- Step 1** **Select 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 2: Select Your Country**



The screenshot shows the 'Setup Wizard' interface. At the top, it says 'Setup Wizard' in green. Below that is the section 'Select Your Country'. A message reads: 'Please select your location. This setting will be used to determine your country's regulatory rules. This selection can only be changed if you reset to defaults.' There is a dropdown menu with 'United States' selected. Below this is another section titled 'Will this product be cloud managed?'. It has two radio button options: 'Yes, I will manage this device with the IgniteNet Cloud controller.' (which is selected) and 'No, I will be operating this device in stand-alone mode.'



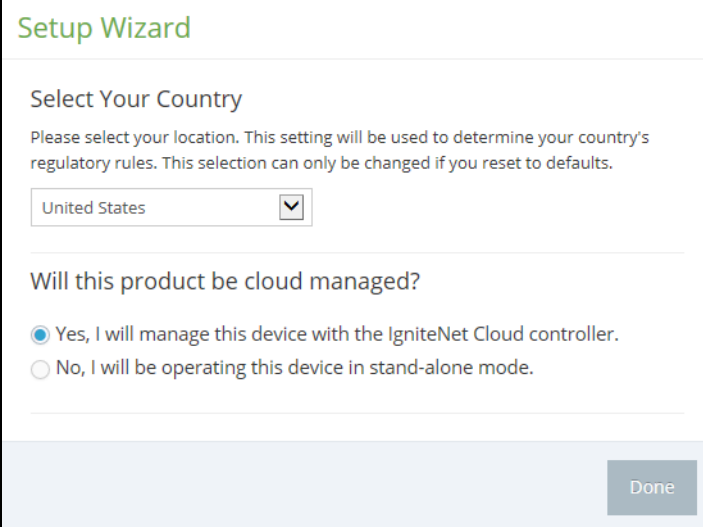
**Caution:** You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.



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

- Step 2** Select to Cloud Manage AP — To manage the AP using the IgniteNet Cloud controller, select “Yes, I will manage this device with the IgniteNet Cloud controller,” and then click “Done.” Otherwise, select “No, I will be operating this device in stand-alone mode” and continue with the Setup Wizard.

**Figure 3: Select Cloud Managed**



**Setup Wizard**

**Select Your Country**

Please select your location. This setting will be used to determine your country's regulatory rules. This selection can only be changed if you reset to defaults.

United States ▼

**Will this product be cloud managed?**

☒ Yes, I will manage this device with the IgniteNet Cloud controller.

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

Done

After you select to manage the AP using the IgniteNet Cloud 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.



- Step 3** Select Setup Method — Select Easy Setup to set basic wireless network access and guest network access parameters, or Advanced Setup to specify networking modes for an AP bridge, AP router, or manual configuration.

**Figure 4: Select Setup Method**

The screenshot shows the 'Setup Wizard' interface. At the top, it says 'Select Your Country' with a subtext: 'Please select your location. This setting will be used to determine your country's regulatory rules. This selection can only be changed if you reset to defaults.' Below this is a dropdown menu currently set to 'United States'. The next section is 'Will this product be cloud managed?' with two radio buttons: 'Yes, I will manage this device with the IgniteNet Cloud controller.' (unselected) and 'No, I will be operating this device in stand-alone mode.' (selected). The final section is 'How do you want to configure this product?' with two radio buttons: 'Easy Setup' (selected) and 'Advanced Setup' (unselected). A 'Done' button is located at the bottom right of the form.

- Step 4** Configure Basic Settings.

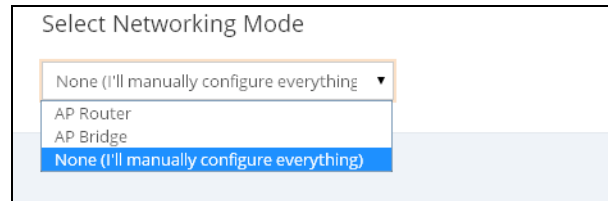
**Figure 5: Easy Setup**

The screenshot shows the 'Easy Setup' configuration screen. It is titled 'Wireless Network Setup'. There are two input fields: 'Wireless network name' and 'Wireless password'. Below the password field is a checkbox labeled 'Show Key' with a subtext: '(If you don't want to password protect your wifi, leave this field blank)'. The next section is 'Guest Network Setup (Optional)' with a subtext: 'Use the fields below to create a second SSID for guest users on your network. Guests won't have access to your local network, only the internet.' Below this are two more input fields: 'Wireless network name' and 'Wireless password'.

- ◆ Easy Setup — Basic wireless network and guest network access parameters. Specify the name and password for the wireless network and guest network. The Networking Mode is set to AP Router as described under [Advanced Setup](#).

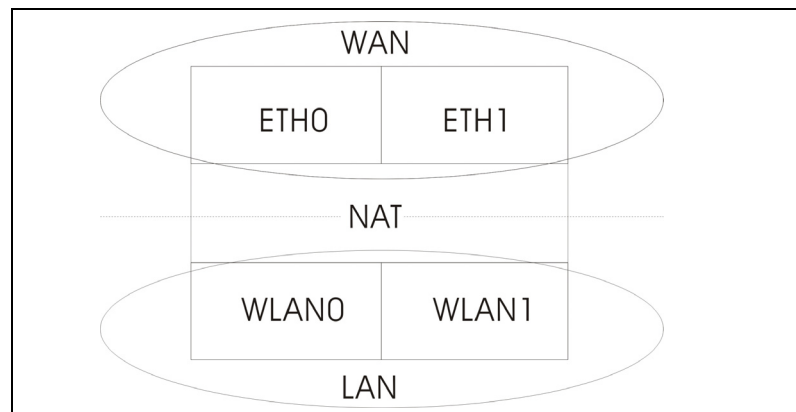
- Wireless Network Setup — Set the name and password for the primary wireless network. A password must be specified to protect the network from unauthorized access.
- Guest Network Setup — Set the name and password for the guest wireless network. This creates a second SSID for guest users, limiting their access only to the Internet.

Figure 6: Advanced Setup



- ◆ Advanced Setup — Networking modes for AP Bridge, AP Router, or manual configuration.
  - AP Bridge Mode — Configures an interface as attached to the WAN (that is, the Internet). In the following figure, Ethernet Port 0 and Ethernet Port 1 are both attached to the WAN. Traffic from these interfaces is directly bridged into the Internet. (This is also called bridge to Internet.)

Figure 7: Bridge to Internet

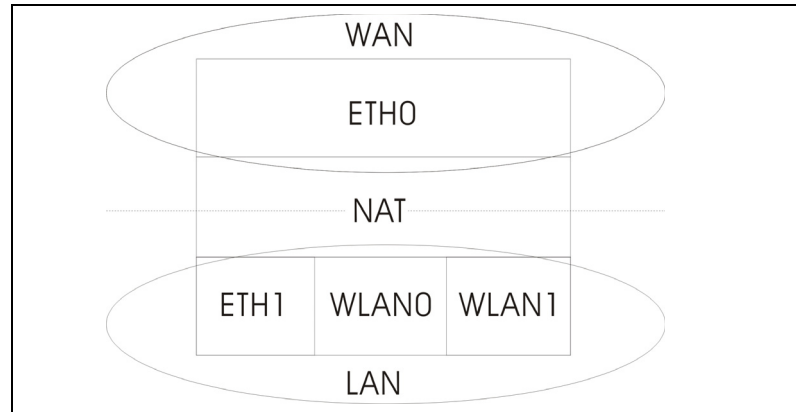


- AP Router Mode — Configures an interface as a member of the LAN. In the following figure, Ethernet Port 1, Wireless LAN 0 (5 GHz Radio), and Wireless LAN 1 (2.4 GHz Radio) are all included in the LAN. Traffic from these interfaces is routed across the access point through Ethernet Port 0 to the Internet. (This is also called route to Internet.)



**Note:** Single-band access points only support one WLAN.

Figure 8: Route to Internet



- **Manual Mode** — Allows all configuration parameters to be manually configured. Any wired module or radio module may be logically placed on the WAN and LAN side of the access point.

## Main Menu

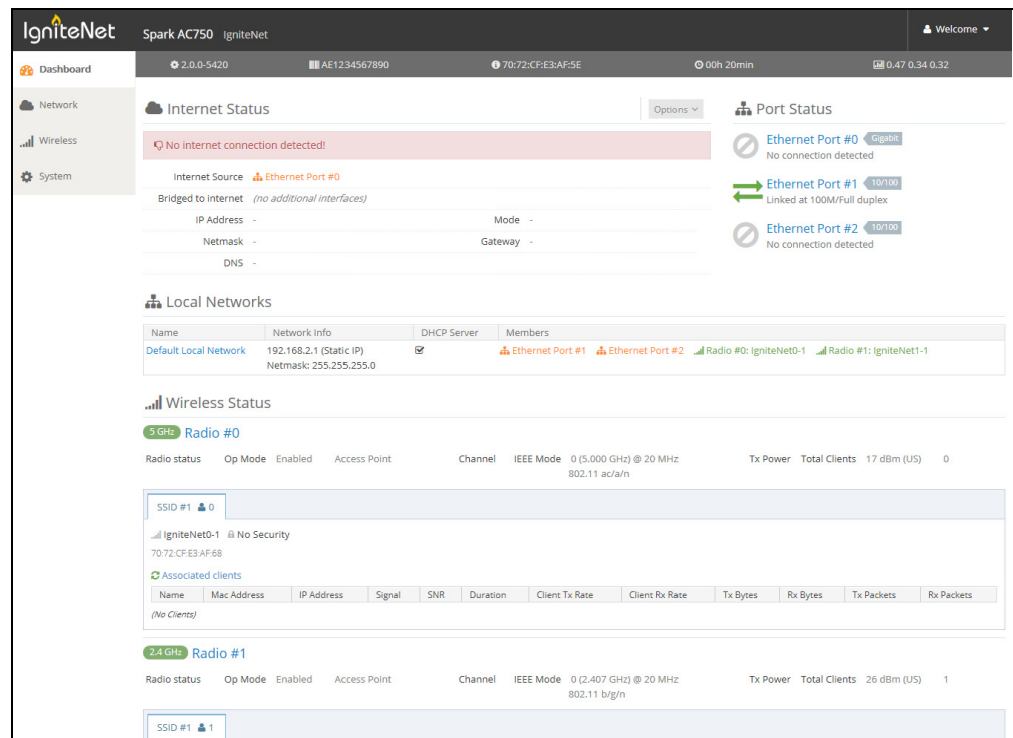
The web interface Main Menu provides access to all the configuration settings available for the AP.

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 Internet status, local network settings, wireless radio status, and traffic graphs. See [“Status Information” on page 24](#).
- ◆ **Network** — Configures Internet, Ethernet, LAN, and Hotspot settings. See [“Network Settings” on page 30](#).
- ◆ **Wireless** — Configures 5 GHz Radio, 2.4 GHz Radio, and VLAN settings. See [“Wireless Settings” on page 40](#).
- ◆ **System** — Configures System (designation and location), Maintenance (such as view log, firmware upgrade, and reset), User Accounts, and Services (management access methods).

**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, wireless radio status, and traffic graphs.

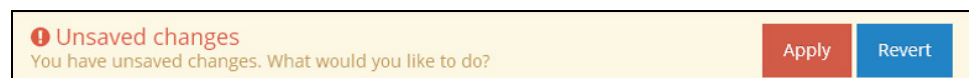
**Figure 9: The Dashboard**



**Common Web Page Buttons** The list below describes the 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 10: Set Configuration Changes**



- ◆ **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.

- ◆ **Welcome > View Users** – Open the Welcome list and click View Users to open the User Accounts menu.



# 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 24](#)
- ◆ [“Network Settings” on page 30](#)
- ◆ [“Wireless Settings” on page 40](#)
- ◆ [“System Settings” on page 56](#)

# 2

## Status Information

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

Status Information includes the following sections:

- ◆ “System and Product Information” on page 24
- ◆ “Internet Status” on page 25
- ◆ “Local Networks” on page 26
- ◆ “Wireless Status” on page 27
- ◆ “Traffic Graphs” on page 29

### System and Product Information

The System and Product Info section shows descriptive information about the AP.

**Figure 11: System and Product Information**



The following items are displayed in this section:

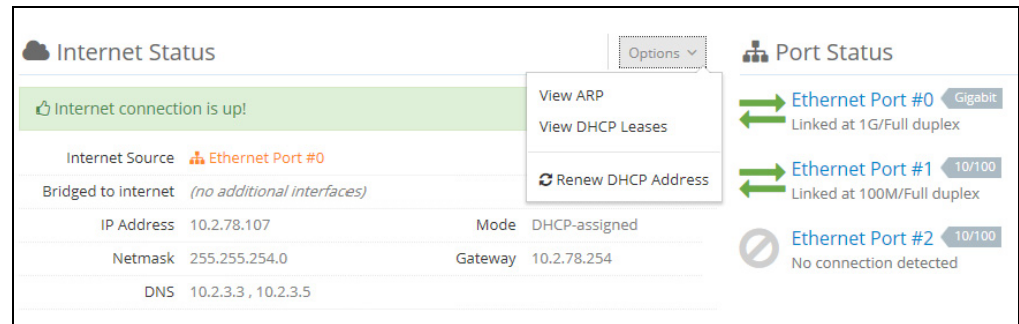
- ◆ The model name of the unit.
- ◆ The software version number.
- ◆ The serial number of the physical access point.
- ◆ Length of time the management agent has been up.
- ◆ The last 1-minute, 5-minute and 15-minute CPU load average.



## Internet Status

The Internet Status section shows information about the Internet connection.

**Figure 12: Internet Status**



The following items are displayed in this section:

- ◆ **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.
- ◆ **Bridged to Internet** — Additional interfaces attached directly to the Internet. (See Configure Settings – “Step 4” on page 17 for a more detailed description.)
- ◆ **IP Address** — IP address of the Internet connection.
- ◆ **Netmask** — The subnet mask of the IP address.
- ◆ **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.
- ◆ **Port Status** — Shows the status of the Ethernet ports, including link up state, MAC address, speed, and duplex mode.
- ◆ **Options** — Includes showing the ARP cache, showing DHCP leases, or renewing DHCP leases.

**Figure 13: Options**

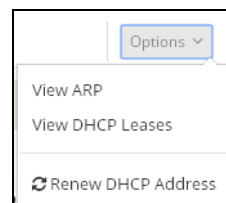


Figure 14: ARP Table

ARP Table					
IP Address	HW type	Flags	MAC Address	Mask	Device
192.168.2.119	0x1	0x2	00:25:d3:8f:f9:95	*	br-lan
172.31.1.164	0x1	0x2	00:ae:00:a3:66:1b	*	eth0.1
192.168.2.99	0x1	0x2	90:e6:ba:cb:cd:d6	*	br-lan
10.2.78.67	0x1	0x2	48:5b:39:d1:1e:f6	*	eth0.1
10.2.78.254	0x1	0x2	e8:ba:70:a0:fb:57	*	eth0.1

Figure 15: DHCP Leases

DHCP Leases				
Expires	MAC Address	IP Address	Client Name	Client Id
11h 24m 37s	192.168.2.119	00:25:d3:8f:f9:95	steve-mini	01:00:25:d3:8f:f9:95

## Local Networks

The Local Networks section shows information about the local network connection.

Figure 16: Local Networks

Local Networks			
Name	Network Info	DHCP Server	Members
Default Local Network	192.168.2.1 (Static IP) Netmask: 255.255.255.0	<input checked="" type="checkbox"/>	Ethernet Port #1  Ethernet Port #2  Radio #0: IgniteNet0-1

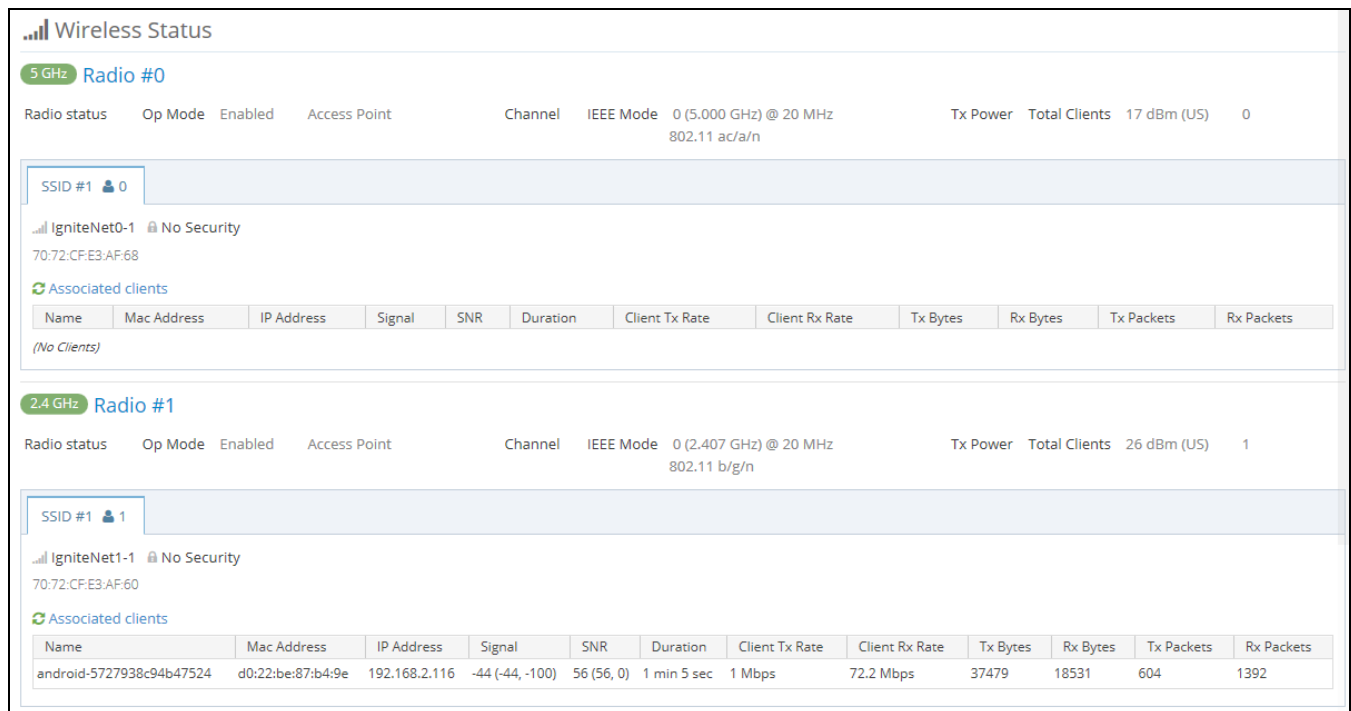
The following items are displayed in this section:

- ◆ **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.

## Wireless Status

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

Figure 17: Wireless Status



The following items are displayed in this section:

- ◆ **Radio #** — Indicates the 5 GHz or 2.4 GHz wireless interface.
  - **Radio Status** — Shows if the wireless interface is enabled or disabled.
  - **Op Mode** — Shows if the unit is configured to operate as an access point (manually configured), an AP in bridge mode, or an AP in router mode.
  - **Channel** — The radio channel the access point uses to communicate with wireless clients. The available channels depend on the 802.11 Mode<sup>1</sup>, Channel Bandwidth<sup>1</sup>, and Country Code settings<sup>2</sup>.
  - **IEEE Mode** — The 802.11 wireless LAN standards supported by the AP.
  - **Tx Power** — The power of the radio signals transmitted from the AP.
  - **Total Clients** — The total number of clients attached to this interface.

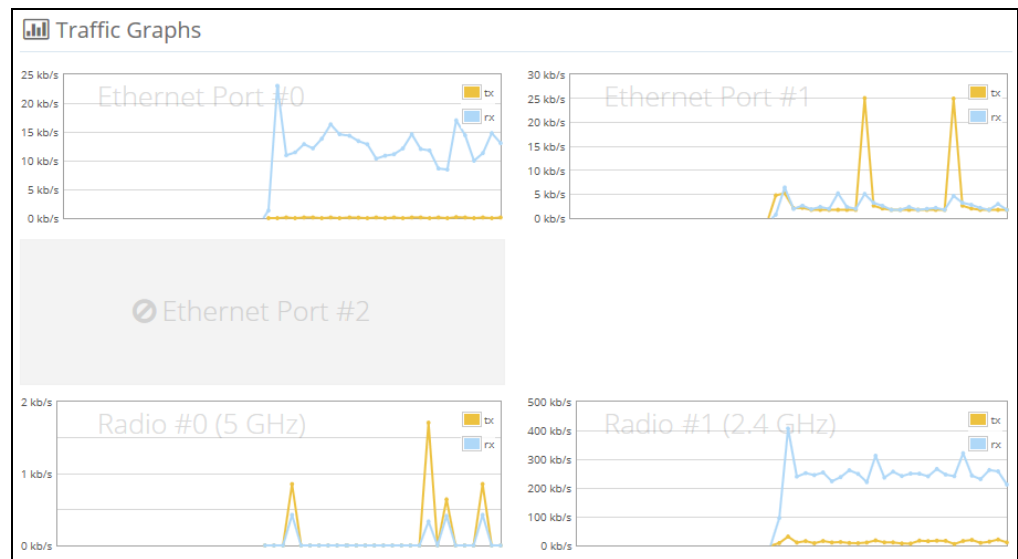
1. See [“Radio Settings”](#) on page 40.  
2. See [“Setup Wizard”](#) on page 15.

- ◆ **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.
  - Network Name — A unique identifier for the local wireless network.
  - Security — Shows whether or not security has been enabled.
  - Associated clients — Shows detailed information about clients.
  - Name — Client name.
  - MAC Address — The MAC address of the wireless client.
  - IP Address — The IP address assigned to the wireless client.
  - Signal — Signal strength (TX/RX) in dBm.
  - Duration — 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 Bytes — The number of transmitted bytes to this client.
  - Rx Bytes — The number of received bytes from this client
  - Tx Packets — The number of transmitted packets to this client.
  - Rx Packets — The number of received packets from this client.

## Traffic Graphs

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

**Figure 18: Traffic Graphs**



# 3

## Network Settings

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

- ◆ “Internet Settings” on page 30
- ◆ “Ethernet Settings” on page 33
- ◆ “LAN Settings” on page 35
- ◆ “Hotspot Settings” on page 37

### 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 19: Internet Settings**

Internet Settings

Internet Source: Ethernet Port #0

IP Address Mode: DHCP

IP Aliases: [Configure](#)

Fallback IP: 192.168.1.20

Fallback Netmask: 255.255.255.0

Manual DHCP Client Id: NO

MTU Size: 1500

[Save](#)

The following items are displayed on this page:

- ◆ **Internet Source** — The Ethernet port used to access the Internet. (Default: Ethernet Port 0; Options: Ethernet Port 0-1)
- ◆ **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 19, "Internet Settings", on page 30.](#)
- **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.

**Figure 20: IP Address Mode – Static IP**

The screenshot shows the 'Internet Settings' configuration page. At the top, the title 'Internet Settings' is displayed. Below it, there are several configuration fields: 'Internet Source' is set to 'Ethernet Port #0' with a dropdown arrow and a help icon; 'IP Address Mode' is set to 'Static IP' with a dropdown arrow and a help icon; 'IP Aliases' has a blue 'Configure' button and a help icon; 'IP Address' is a text field containing '192.168.1.1'; 'Subnet Mask' is a dropdown menu set to '255.255.255.0'; 'Default Gateway' is a text field containing '192.168.1.254'; 'Addl DNS servers' is a text field containing '8.8.8.8'; and 'MTU Size' is a text field containing '1500' with a help icon. At the bottom of the form is a blue 'Save' button with a floppy disk icon.

- **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)
- **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.
- **Addl 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.

- **PPPoE** — To obtain an IP address for the selected Ethernet interface using PPPoE, the following items must be specified.

Figure 21: IP Address Mode – PPPoE

The screenshot shows the 'Internet Settings' configuration page. It includes the following fields and controls:

- Internet Source:** A dropdown menu set to 'Ethernet Port #0' with a help icon.
- IP Address Mode:** A dropdown menu set to 'PPPoE' with a help icon.
- IP Aliases:** A blue 'Configure' button with a help icon.
- User Name:** A text input field.
- Password:** A text input field with a toggle icon for visibility.
- Service Name:** A text input field.
- MTU Size:** A text input field set to '1500' with a help icon.
- Save:** A blue button at the bottom.

- **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)
  - **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)
- ◆ **IP Aliases** — Adds a static IPv4 address under which the access point can also be reached.

Figure 22: IP Alias

The screenshot shows the 'IP Aliases' configuration window with a table of aliases:

IP	Netmask	Comment	
192.168.2.99	255.255.255.0	ECOW#3	

At the bottom right, there is a blue button labeled '+ Add new'.

- ◆ **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-1500 bytes; Default 1500 bytes)



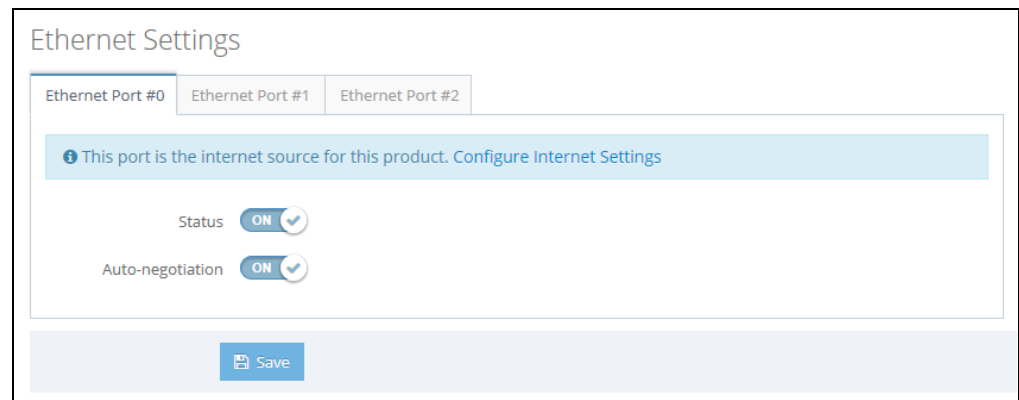
## Ethernet Settings

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), is bridged directly to the Internet, connected to the guest network, or provides hotspot service.

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

- ◆ **Status** — Enables or disables this port. (Default: ON)
- ◆ **Auto-negotiation** — Enables or disables auto-negotiation for a given interface. (Default: ON)  
 1000BASE-T does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port.  
 When auto-negotiation is enabled, the access point will negotiate the best settings for a link based on advertised capabilities.

**Figure 23: Ethernet Settings – Internet Source**



The following status message is displayed if an interface is connected to the Internet:

- ◆ “This port 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 24: Ethernet Settings – Network Behavior

Ethernet Settings

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

Status ☒ ON

Network Behavior

Network Name

Auto-negotiation ☒ ON

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. (See [Figure 7, "Bridge to Internet", on page 18.](#)) 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 IP address in the same subnet.
  - **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 to the Internet. (See [Figure 8, "Route to Internet", on page 19.](#)) 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.
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Networks.
  - **Add to Guest Network** — This port can only access the guest network.
  - **Hotspot Controlled** — This port can only access hotspot services.
  - **Configure Hotspot** — Opens the Hotspot Settings page.

## LAN Settings

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

Figure 25: Network – LAN Settings

The screenshot displays the 'LAN Settings' interface with three network configuration sections:

- Default Local Network:**
  - Members: Ethernet Port #1, Ethernet Port #2, Radio #0: IgniteNet0-1, Radio #1: IgniteNet1-1
  - IP Address: 192.168.2.1
  - Subnet Mask: 255.255.255.0
  - MTU Size: 1500
  - DHCP Server: ON
  - DHCP Start: 100
  - DHCP Max: 150
  - STP: OFF
  - UPnP: ON
  - Smart Isolation: Disable (full access)
- Default Guest Network:**
  - Members: (none)
  - IP Address: 192.168.3.1
  - Subnet Mask: 255.255.255.0
  - MTU Size: 1500
  - DHCP Server: OFF
  - DHCP Start: (empty)
  - DHCP Max: (empty)
  - STP: OFF
  - UPnP: OFF
  - Smart Isolation: Internet access on
- Custom Network:**
  - IP Address: (empty)
  - Subnet Mask: 255.255.255.0
  - MTU Size: 1500
  - DHCP Server: ON
  - DHCP Start: 100
  - DHCP Max: 150
  - STP: OFF
  - UPnP: OFF
  - Smart Isolation: Disable (full access)

At the bottom, there is a '+ Add Custom LAN' button and a 'Save' button.

The following items are displayed on this page:

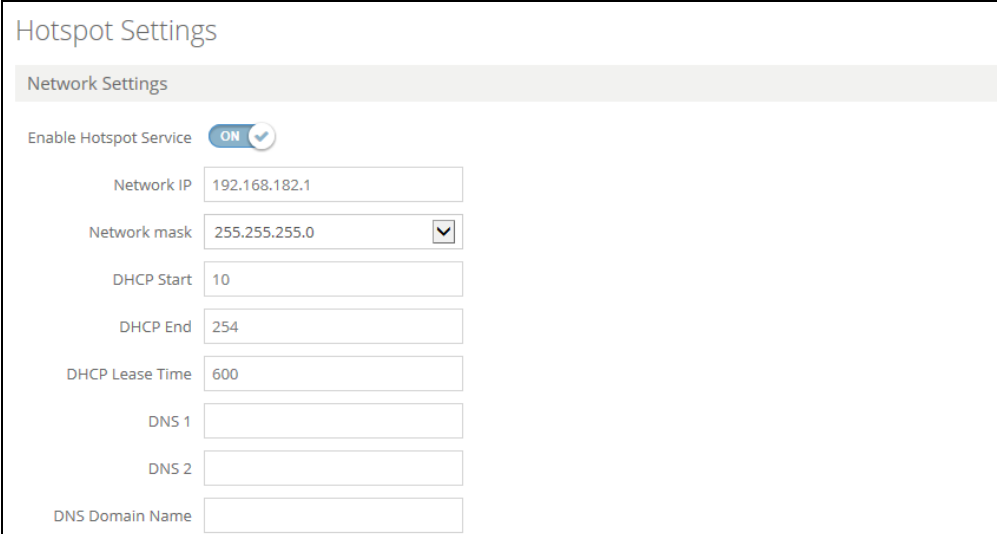
- ◆ **Members** — The interfaces attached to the local area network.
- ◆ **IP Address** — Specifies the IP address for the local network or guest network. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.2.1)
- ◆ **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)

- ◆ **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this network.
- ◆ **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 Max** — Maximum number of addresses in the address pool. (Range: 1-255; Default: 150)
- ◆ **STP** — Enables or disables processing of Spanning Tree Protocol messages. (Default: Disabled)
- ◆ **UPnP** — Enables or disables Universal Plug-and-Play broadcast messages. (Default: Disabled)
- ◆ **Smart Isolation** — Enables network traffic to be restricted to the specified network:
  - **Disable (full access)** — There is no traffic isolation. Clients can access the Internet and other devices on the local LAN.
  - **Internet access only** — Traffic from this network can only be routed to and from the Internet.
  - **LAN access only** — Traffic from this network is restricted to local LAN devices only.

## Hotspot Settings

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

**Figure 26: Hotspot Settings (Network Settings)**



Hotspot Settings

Network Settings

Enable Hotspot Service ☒

Network IP 192.168.182.1

Network mask 255.255.255.0

DHCP Start 10

DHCP End 254

DHCP Lease Time 600

DNS 1

DNS 2

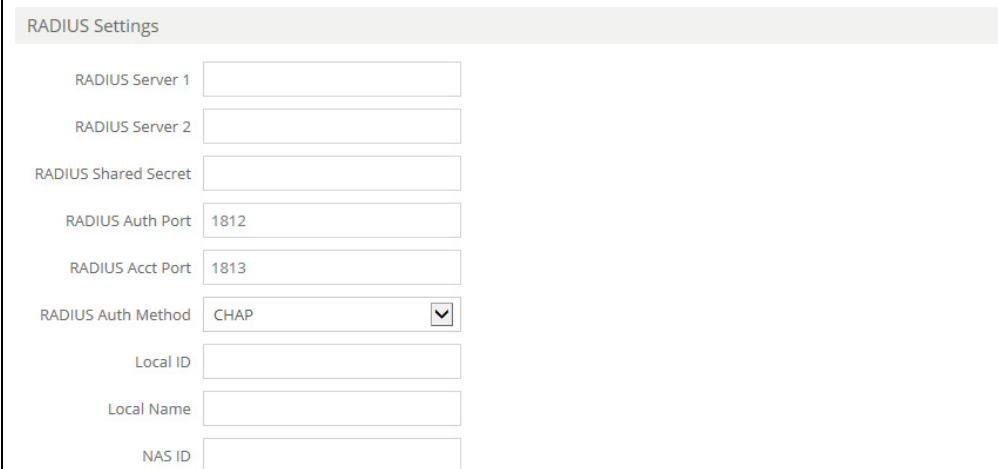
DNS Domain Name

The following items are displayed on this page:

- ◆ **Network IP** — Specifies the IP address for the hotspot. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.182.1)
- ◆ **Network Mask** — Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- ◆ **DHCP Start** — Starting number of (last numeric field) in address pool. (Range: 1-254; Default: 10)
- ◆ **DHCP End** — Ending number of (last numeric field) in address pool. (Range: 1-254; Default: 254)
- ◆ **DHCP Lease Time** — The duration that an IP address is assigned to a DHCP client. (Range: 600-43200 seconds; Default: 600 seconds)
- ◆ **DNS 1** — The IP address of the primary 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.
- ◆ **DNS 2** — The secondary DNS server available to DHCP clients.

- ◆ **DNS Domain Name** — The domain name used to resolve incomplete host names via the Domain Name System. (Range: 1-32 characters)

**Figure 27: Hotspot Settings (RADIUS Settings)**



The screenshot shows a web form titled "RADIUS Settings". It contains the following fields and controls:

- RADIUS Server 1**: A text input field.
- RADIUS Server 2**: A text input field.
- RADIUS Shared Secret**: A text input field.
- RADIUS Auth Port**: A text input field with the value "1812".
- RADIUS Acct Port**: A text input field with the value "1813".
- RADIUS Auth Method**: A dropdown menu with "CHAP" selected.
- Local ID**: A text input field.
- Local Name**: A text input field.
- NAS ID**: A text input field.

The following items are displayed on this page:

- ◆ **RADIUS Server 1** — IP address or host name of the primary RADIUS server.
- ◆ **RADIUS Server 2** — IP address or host name of the secondary RADIUS server.
- ◆ **RADIUS Shared Secret** — A shared text string used to encrypt messages between the access point and the RADIUS server. Be sure that the same text string is specified on the RADIUS server. Do not use blank spaces in the string. (Range: 1-255 characters).
- ◆ **RADIUS Auth Port** — RADIUS server UDP port used for authentication messages. (Range: 1-65535, Default: 1812)
- ◆ **RADIUS Acct Port** — RADIUS server UDP port used for accounting messages. (Range: 1-65535, Default: 1813)
- ◆ **RADIUS Auth Method** — Selects the encryption method to use for messages between the AP and the RADIUS server; CHAP, PAP, or MSCHAPv2. The encryption method must match that used by the RADIUS server.
- ◆ **Local ID** — Local RADIUS server identifier.
- ◆ **Local Name** — Local RADIUS server name
- ◆ **NAS ID** — Local RADIUS server operation identifier.

Figure 28: Hotspot Settings (Captive Portal Settings)

Captive Portal Settings

Captive Portal URL

Captive Portal Secret

Walled Garden

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

Auth White List

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

The following items are displayed on this page:

- ◆ **Captive Portal URL** — Host name of Internet service portal for the hotspot.  
The captive portal forces a hotspot client to access a welcome web page (normally used for authentication) before gaining further access to the Internet. The welcome page may require authentication and/or payment.
- ◆ **Captive Portal Secret** — The password used for logging into the hotspot.
- ◆ **Walled Garden** — A list of web sites to which unauthenticated users are allowed to navigate.
- ◆ **Auth White List** — A list of MAC addresses that are allowed to bypass the captive portal to access the internet.

# 4

## Wireless Settings

---

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

- ◆ [“Radio Settings” on page 40](#)
- ◆ [“VLAN Settings” on page 54](#)

---

### 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, 802.11a/a+n/ac+a+n (5 GHz) or 802.11b/g/b+g+n (2.4 GHz). Supported modes depend on the access point model. 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 0** — the 5 GHz 802.11a/n/ac radio interface
- ◆ **Radio 1** — the 2.4 GHz 802.11b/g/n radio interface

Each radio supports 8 virtual access point (VAP) interfaces based on the SSIDs, referred to as SSID1 ~ SSID8. 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. The AP supports up to a total of 127 wireless clients across all SSID interfaces per radio.



Physical Radio Settings **Figure 29: Radio Settings (Physical Radio Settings)**

Wireless Settings (Radio #0)

Physical Radio Settings

Status ☒ ON

Mode Access Point (Auto-WDS)

802.11 Mode 802.11ac+a+n

Channel Bandwidth 20MHz

Channel Auto

Bandsteering ☐ OFF

The following items are displayed on this page:

- ◆ **Status** — Enables or disables the wireless service on this interface.
- ◆ **Mode** — Selects the mode in which the AP will function.
  - **Access Point (Auto-WDS)** — The AP operates as an access point in WDS mode, which accepts connections from APs in Client WDS mode. (This is the default setting.)  
In this mode, the AP provides services to clients as a normal access point. WDS is used to automatically search for and connect to other AP nodes using the same SSID and security settings.
  - **Client** — The AP can provide a wireless connection to another AP. In this mode, it can pass information from or to locally wired hosts, but does not provide services to any wireless clients.
  - **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 0** (5 GHz Radio) — Default: 11a+n; Options: 11a, 11a+n, 11ac+a+n
  - **Radio 1** (2.4 GHz Radio) — Default: 11b+g; Options: 11b+g, 11b+g+n
- ◆ **Channel Bandwidth** — The AP options for channel bandwidth include 5, 10, 20, 40 and 80 MHz. Using 20 MHz gives an 802.11g connection a speed of 54 Mbps and an 802.11n connection a speed of up to 108 Mbps, and ensures backward compliance for slower 802.11b devices. Setting the channel bandwidth to 40 MHz provides a connection speed for 802.11n of up to 300 Mbps. Using a channel bandwidth of 80MHz provides a connection speed up to 866.7 Mbps. (Default: 20 MHz; Range: 5 MHz, 10 MHz, 20 MHz, 40 MHz, 80MHz)

- ◆ **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)

**Table 1: Radio Channels**

Radio 0 (5 GHz)		Radio 1 (2.4 GHz)	
Radio Channels <sup>a</sup>	Frequency (GHz)	Radio Channels	Frequency (GHz)
Auto	Auto scan	Auto	Auto scan
36	5.180	1	2.412
40	5.200	2	2.417
44	5.220	3	2.422
48	5.240	4	2.427
149	5.745	5	2.432
153	5.765	6	2.437
157	5.785	7	2.442
161	5.805	8	2.447
165	5.825	9	2.452
		10	2.457
		11	2.462

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

- ◆ **Bandsteering** — When enabled, clients that support 2.4 GHz and 5 GHz are first connected to the 5 GHz radio. This feature helps balance the client load over the two radio bands. Note that both radios must have configured SSIDs that match for this feature to fully operate.

## Wireless Networks — General Settings

Figure 30: Radio Settings (General Settings)

The screenshot shows the 'Wireless Networks' configuration page. At the top, there's a table with one row labeled 'SSID1'. Below the table, there are several settings: 'Status' is a toggle switch set to 'ON'; 'SSID' is a text field containing 'IgniteNet1-1' with a 'Scan' button and a 'Broadcast' checkbox checked; 'Client Isolation' is a toggle switch set to 'OFF'; 'WMM' is a toggle switch set to 'ON'; and 'Minimum signal allowed' is a text field containing '0'.

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: IgniteNet0-# (where # is 1-8) for 5 GHz, IgniteNet1-# (where # is 1-8) for 2.4 GHz; Range: 1-32 characters)
- ◆ **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. When enabled, the parameters for each Access Category (AC) queue will be employed on the access point and QoS capabilities advertised to WMM-enabled clients. (Default: Enabled)

When enabled, WMM must be supported on any device trying to associated with the access point. Devices that do not support this feature will not be allowed to associate with the access point.

Wireless networks offer an equal opportunity for all devices to transmit data from any type of application. Although this is acceptable for most applications, multimedia applications (with audio and video data) are particularly sensitive to the delay and throughput variations that result from this "equal opportunity" wireless access method. For multimedia applications to run well over a wireless

network, a Quality of Service (QoS) mechanism is required to prioritize traffic types and provide an “enhanced opportunity” wireless access method.

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. WMM employs techniques that are a subset of the IEEE 802.11e QoS standard and it enables the access point to inter-operate with both WMM-enabled clients and other devices that may lack any WMM functionality.

**Access Categories** — WMM defines four access categories (ACs): voice, video, best effort, and background. These categories correspond to traffic priority levels and are mapped to IEEE 802.1D priority tags (see [Figure 2, “WMM Access Categories”, on page 44](#)). The direct mapping of the four ACs to 802.1D priorities is specifically intended to facilitate inter operability with other wired network QoS policies. While the four ACs are specified for specific types of traffic, WMM allows the priority levels to be configured to match any network-wide QoS policy. WMM also specifies a protocol that access points can use to communicate the configured traffic priority levels to QoS-enabled wireless clients.

**Table 2: WMM Access Categories**

Access Category	WMM Designation	Description	802.1D Tags
AC_VO (AC3)	Voice	Highest priority, minimum delay. Time-sensitive data such as VoIP (Voice over IP) calls.	7, 6
AC_VI (AC2)	Video	High priority, minimum delay. Time-sensitive data such as streaming video.	5, 4
AC_BE (AC0)	Best Effort	Normal priority, medium delay and throughput. Data only affected by long delays. Data from applications or devices that lack QoS capabilities.	0, 3
AC_BK (AC1)	Background	Lowest priority. Data with no delay or throughput requirements, such as bulk data transfers.	2, 1

**WMM Operation** — WMM uses traffic priority based on the four ACs; Voice, Video, Best Effort, and Background. The higher the AC priority, the higher the probability that data is transmitted.

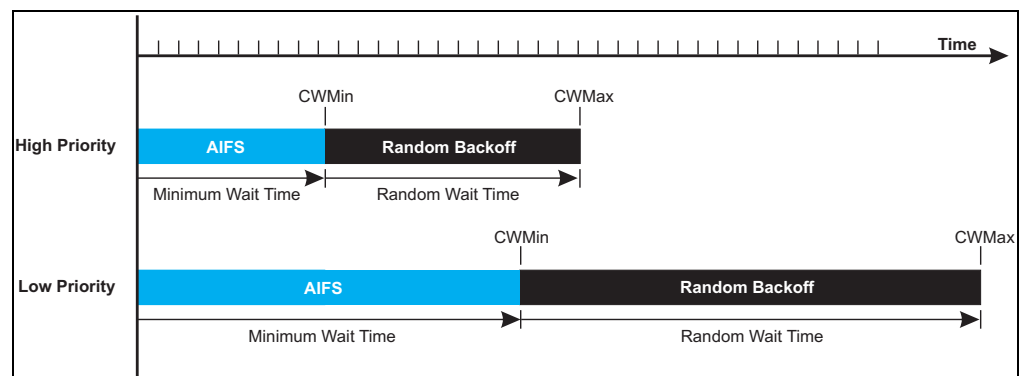
When the access point forwards traffic, WMM adds data packets to four independent transmit queues, one for each AC, depending on the 802.1D priority tag of the packet. Data packets without a priority tag are always added to the Best Effort AC queue. From the four queues, an internal “virtual” collision resolution mechanism first selects data with the highest priority to be granted a transmit opportunity. Then the same collision resolution mechanism is used externally to determine which device has access to the wireless medium.

For each AC queue, the collision resolution mechanism is dependent on two timing parameters:

- AIFSN (Arbitration Inter-Frame Space Number), a number used to calculate the minimum time between data frames
- CW (Contention Window), a number used to calculate a random backoff time

After a collision detection, a backoff wait time is calculated. The total wait time is the sum of a minimum wait time (Arbitration Inter-Frame Space, or AIFS) determined from the AIFSN, and a random backoff time calculated from a value selected from zero to the CW. The CW value varies within a configurable range. It starts at CWMin and doubles after every collision up to a maximum value, CWMax. After a successful transmission, the CW value is reset to its CWMin value.

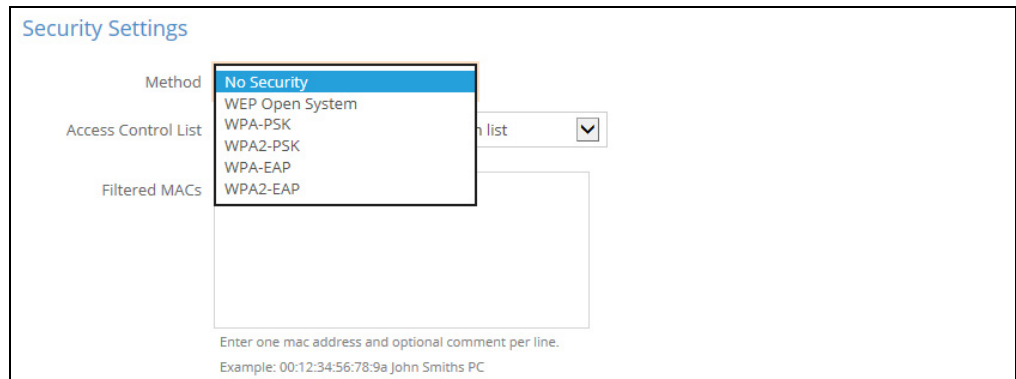
Figure 31: WMM Backoff Wait Times



For high-priority traffic, the AIFSN and CW values are smaller. The smaller values equate to less backoff and wait time, and therefore more transmit opportunities.

- ◆ **Minimum signal allowed** — Only allows clients to associate to this SSID if their signal strength (SNR) is equal or greater than the specified value. Setting the value to zero disables this feature. (Default: 0, disabled)

Wireless Networks — Security Settings



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

- ◆ **Method** — Sets the wireless security method for each VAP, including association mode, encryption, and authentication. (Default: 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.
  - **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.
  - **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.

- **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.)
  - **TKIP** — TKIP is used as the multicast encryption cipher.
  - **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)
- **Radius Acct Server** — Specifies the IP address or host name of the RADIUS accounting server.
- **Radius Acct Port** — The UDP port number used by the RADIUS server for accounting messages. (Range: 1024-65535; Default: 1813)
- **Radius 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: 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.

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.

- ◆ **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** — Enter a physical address for each client. Enter six pairs of hexadecimal digits separated by colons, and followed by an optional comment; for example, 00:90:D1:12:AB:89 John Smith's PC

## Wireless Networks — Network Settings

Figure 33: Wireless Network Settings

The screenshot shows the 'Network Settings' interface. It has a title 'Network Settings' at the top. Below it are four settings:

- Network Behavior:** A dropdown menu currently showing 'Route to Internet'.
- Network Name:** A dropdown menu currently showing 'Default local network'.
- Limit Upload:** A toggle switch currently set to 'OFF'.
- Limit Download:** A toggle switch currently set to 'OFF'.

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

- ◆ **Network Behavior** — One of the following connection methods must be specified. (Default: Route to Internet)
  - **Bridge to Internet** — Configures an interface as attached to the WAN. Traffic from this interface is directly bridged into the Internet. (See [Figure 7, "Bridge to Internet", on page 18.](#))
  - **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 8, "Route to Internet", on page 19.](#))
    - **Network Name** — The network to be routed. The default is "Default local network" as displayed under LAN Settings – Local Network.
  - **Add to Guest Network** — This interface can only support the guest network.
  - **Hotspot Controlled** — This interface can only support hotspot services.
    - **Configure Hotspot** — Opens Hotspot Settings page.
  - **VLAN Tag Traffic** — Tags any packets passing from this VAP (virtual access point) to the associated Ethernet port as configured under ["VLAN Settings" on page 54.](#) (Range: 3-4095)
- ◆ **Limit Upload** — Enables rate limiting of traffic from the VAP interface as it is passed to the wired network. You can set a maximum rate in Kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

- ◆ **Limit Download** — Enables rate limiting of traffic from the wired network as it is passed to the VAP interface. You can set a maximum rate in kbytes per second. (Range: 256-10048576 Kbytes per second; Default: OFF)

## Advanced Radio Settings

Figure 34: Advanced Radio Settings

Advanced Radio Settings

802.11 Rates: Auto

Tx Power: 17 dBm (50 mW)

ACK Timeout: 64 3.6 miles (5.8 km)

Fragmentation Thresh.: 2346

RTS Thresh.: 2347

SGI: ON

STBC: OFF

AMPDU: ON

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

- ◆ **802.11 Rates** — The minimum data rate at which the AP transmits packets on the wireless interface.

Table 3: 802.11 Data Rates

Option	Rate (Max)	Coding Method	Radio 0 (5 GHz)	Radio 1 (2.4 GHz)
Auto	Auto	Based on signal strength	?	?
1M	1 Mbps	CKK		?
2M	2 Mbps	CKK		?
5.5M	5.5 Mbps	CKK		?
11M	11 Mbps	CKK	?	?
6M	6 Mbps	OFDM	?	?
9M	9 Mbps	OFDM	?	?
12M	12 Mbps	OFDM	?	?
18M	18 Mbps	OFDM	?	?
24M	24 Mbps	OFDM	?	?
36M	36 Mbps	OFDM	?	?
48M	48 Mbps	OFDM	?	?
54M	54 Mbps	OFDM	?	?
MCS0	15 Mbps	BPSK, single stream	?	?
MCS1	30 Mbps	QPSK, single stream	?	?

Table 3: 802.11 Data Rates (Continued)

Option	Rate (Max)	Coding Method	Radio 0 (5 GHz)	Radio 1 (2.4 GHz)
MCS2	45 Mbps	QPSK, single stream	?	?
MCS3	60 Mbps	16-QAM, single stream	?	?
MCS4	90 Mbps	16-QAM, single stream	?	?
MCS5	120 Mbps	64-QAM, single stream	?	?
MCS6	135 Mbps	64-QAM, single stream	?	?
MCS7	150 Mbps	64-QAM, single stream	?	?
MCS8	30 Mbps	BPSK, double stream	?	?
MCS9	60 Mbps	QPSK, double stream	?	?
MCS10	90 Mbps	QPSK, double stream	?	?
MCS11	120 Mbps	16-QAM, double stream	?	?
MCS12	180 Mbps	16-QAM, double stream	?	?
MCS13	240 Mbps	64-QAM, double stream	?	?
MCS14	270 Mbps	64-QAM, double stream	?	?
MCS15	300 Mbps	64-QAM, double stream	?	?
NSS1-MCS0	32.5 Mbps	256-QAM, single stream	?	
NSS1-MCS1	65 Mbps	256-QAM, single stream	?	
NSS1-MCS2	97.5 Mbps	256-QAM, single stream	?	
NSS1-MCS3	130 Mbps	256-QAM, single stream	?	
NSS1-MCS4	195 Mbps	256-QAM, single stream	?	
NSS1-MCS5	260 Mbps	256-QAM, single stream	?	
NSS1-MCS6	292.5 Mbps	256-QAM, single stream	?	
NSS1-MCS7	325 Mbps	256-QAM, single stream	?	
NSS1-MCS8	390 Mbps	256-QAM, single stream	?	
NSS1-MCS9	433.3 Mbps	256-QAM, single stream	?	
NSS2-MCS0	65 Mbps	256-QAM, double stream	?	
NSS2-MCS1	130 Mbps	256-QAM, double stream	?	
NSS2-MCS2	195 Mbps	256-QAM, double stream	?	
NSS2-MCS3	260 Mbps	256-QAM, double stream	?	
NSS2-MCS4	390 Mbps	256-QAM, double stream	?	
NSS2-MCS5	520 Mbps	256-QAM, double stream	?	
NSS2-MCS6	585 Mbps	256-QAM, double stream	?	
NSS2-MCS7	650 Mbps	256-QAM, double stream	?	
NSS2-MCS8	780 Mbps	256-QAM, double stream	?	
NSS2-MCS9	866.7 Mbps	256-QAM, double stream	?	

- ◆ **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. (Default: 17 dBm for 5 GHz radio, 27 dBm for 2.4 GHz radio)

**Table 4: Tx Power**

Power	Radio 0 (5 GHz)	Radio 1 (2.4 GHz)
0 dBm (1 mW)	?	?
4dBm (2 mW)	?	?
5 dBm (3 mW)	?	?
7 dBm (5 mW)	?	?
8 dBm (6 mW)	?	?
9 dBm (7 mW)	?	?
10 dBm (10 mW)	?	?
11 dBm (12 mW)	?	?
12 dBm (15 mW)	?	?
13 dBm (19 mW)	?	?
14 dBm (25 mW)	?	?
15 dBm (31 mW)	?	?
16 dBm (39 mW)	?	?
17 dBm (50 mW)	?	?
18 dBm (63 mW)		?
19 dBm (79 mW)		?
20 dBm (100 mW)		?
21 dBm (125 mW)		?
22 dBm (158 mW)		?
23 dBm (199 mW)		?
24 dBm (251 mW)		?
25 dBm (316 mW)		?
26 dBm (398 mW)		?
27 dBm (501 mW)		?

- ◆ **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: 0 microseconds)

- ◆ **Fragmentation Thresh.** — Sets the maximum frame size above which packets are fragmented. This 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 Thresh.** — Sets the packet size threshold at which a Request to Send (RTS) signal must be sent to a receiving station prior to the sending station starting communications. The access point sends RTS frames to a receiving station to negotiate the sending of a data frame. After receiving an RTS frame, the station sends a CTS (clear to send) frame to notify the sending station that it can start sending data.

If the RTS threshold is set to 1, the access point always sends RTS signals. If set to 2346, 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 will be 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: 1-2346 bytes; Default: 2346 bytes)

- ◆ **SGI** — The 802.11n draft specifies two guard intervals: 400ns (short) and 800ns (long). Support of the 400ns Short Guard Interval is optional for transmit and receive. The purpose of a guard interval is to introduce immunity to propagation delays, echoes, and reflections to which digital data is normally very sensitive. Enabling the SGI sets it to 400ns. (Default: Disabled)
- ◆ **STBC** — Space-time Block Coding sends multiple copies of the same data over a number of antennas, using the various received versions to improve the reliability of data transfer. The transmitted signal may traverse a difficult environment with scattering, reflection, and refraction which may then be further corrupted by thermal noise in the receiver, so some of the received copies will be better than others. This redundancy results in a higher chance of being able to use one or more of the received copies to correctly decode the received signal. (Default: Disabled)
- ◆ **AMPDU** — Enables or disables the use of Aggregated MAC Protocol Data Units. Physical layer (PHY) data rate improvements do not increase real throughput beyond a point because of 802.11 protocol overheads. The main media access control feature that provides a performance improvement is aggregation. Aggregation of MAC protocol data units (MPDUs) is referred to as MPDU aggregation or (A-MPDU). (Default: Enabled)

---

## 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 configure a VLAN for up to 13 VAP interfaces.

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.
- ◆ A management VLAN can be used for managing the access point through remote management tools, such as the web interface, SSH, Telnet or SNMP. The access point can be configured to only accept management traffic that is tagged with the specified management VLAN ID. This ID must be assigned to the Ethernet ports or radio interfaces which are designated to handle management traffic.
- ◆ 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.



**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 35: Configuring VLANs

Wireless VLAN Settings

Create up to 12 VLAN-tagged networks.

+ Add new

VLAN Id	Ports	SSIDs	
<input type="text" value="3"/>	<div><input type="checkbox"/> Ethernet Port #0 <input type="checkbox"/> Ethernet Port #1</div> <div><input checked="" type="checkbox"/> Ethernet Port #2</div>	<div> Ethernet Port #2  Radio #1: IgniteNet1-1</div>	<div>✕</div>
<input type="text" value="20"/>	<div><input type="checkbox"/> Ethernet Port #0 <input checked="" type="checkbox"/> Ethernet Port #1</div> <div><input type="checkbox"/> Ethernet Port #2</div>	(None)	<div>✕</div>

Save

The following items are displayed on this page:

- ◆ **VLAN ID** — A VLAN identifier to be assigned. (Range: 3-4095)  
(VLAN 1 and 2 are reserved for internal use.)
- ◆ **Ports** — The Ethernet ports assigned to the specified VLAN.
- ◆ **SSIDs** — The SSID of a VAP configured to be a member of the specified VLAN.  
This option is configured under Radio Settings (Network Settings – Network Behavior).

# 5

---

## System Settings

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

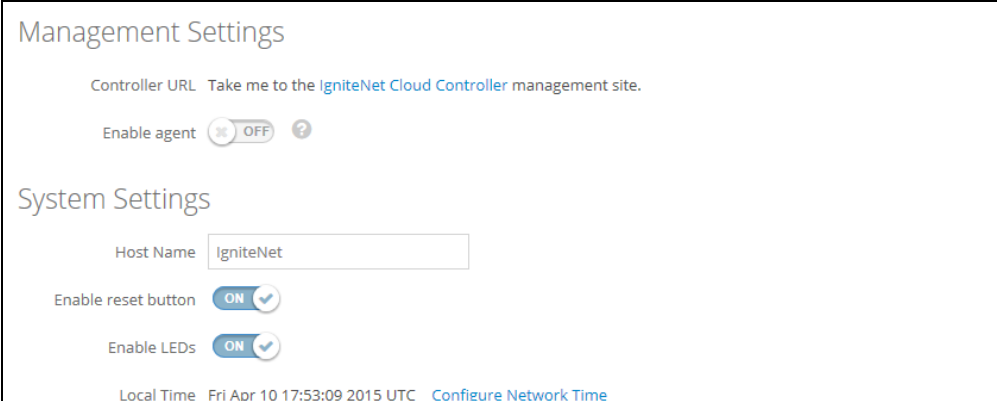
- ◆ [“System Settings” on page 57](#)
- ◆ [“Maintenance” on page 58](#)
- ◆ [“User Accounts” on page 61](#)
- ◆ [“Services” on page 61](#)



## System Settings

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

**Figure 36: System Settings**



The screenshot shows the 'System Settings' page. It is divided into two main sections: 'Management Settings' and 'System Settings'.

**Management Settings:**

- Controller URL:** A link that says 'Take me to the IgniteNet Cloud Controller management site.'
- Enable agent:** A toggle switch currently set to 'OFF' with a help icon.

**System Settings:**

- Host Name:** A text input field containing 'IgniteNet'.
- Enable reset button:** A toggle switch currently set to 'ON'.
- Enable LEDs:** A toggle switch currently set to 'ON'.
- Local Time:** Displays 'Fri Apr 10 17:53:09 2015 UTC' with a link to 'Configure Network Time'.

The following items are displayed on this page:

- ◆ **Enable agent** — Set to “On” to manage this AP from the IgniteNet Cloud controller. Click on the link to **cloud.ignitenet.com** where you can create an account and register your AP.
- ◆ **Host Name** — An alias for the AP, enabling the device to be uniquely identified on the network. (Default: IgniteNet; Range: 0-50 characters)
- ◆ **Enable reset button** — Enables or disables the hardware reset button.
- ◆ **Enable LEDs** — Enables or disables the AP’s status LEDs.
- ◆ **Local Time** — The local time, given as day of week, month, time, year.
- ◆ **Configure Network Time** — Links to the [Network Time \(NTP\)](#) section on the Services page.

Maintenance

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

Figure 37: Maintenance

System Actions

View Log

View system log

Troubleshooting Log

Download this device's troubleshooting log

Reboot

Reboot your device

Reset

Reset to factory default settings

Backup

Download this device's configuration settings

Restore

Restore the configuration settings of this device

Upgrade

Upgrade your device's firmware (current version is 2.0.0-5420)

**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 38: System Log

System log

Syslog output

Jun 27 07:02:52 ACN-AP user.warn kernel: [PHY\_ConfigBBWithParaFile][PHY\_

Jun 27 07:02:52 ACN-AP user.warn kernel: [PHY\_ConfigBBWithParaFile][AGC\_

Jun 27 07:02:52 ACN-AP user.warn kernel: [phy\_RF6052\_Config\_ParaFile][R

Jun 27 07:02:52 ACN-AP user.warn kernel: [phy\_RF6052\_Config\_ParaFile][R

Jun 27 07:02:52 ACN-AP user.warn kernel: 4#60;=== FirmwareDownload8812

Jun 27 07:02:52 ACN-AP user.warn kernel: [PHY\_ConfigTXPwrTrackingWithPa

Jun 27 07:02:52 ACN-AP user.warn kernel: 0x55d = 0xff

Jun 27 07:02:52 ACN-AP user.warn kernel: 8812 Enable Tx 2 Path

Jun 27 07:02:52 ACN-AP user.warn kernel: 0x838 B(1)= 0, 0x456 = 0x32

Jun 27 07:02:52 ACN-AP user.warn kernel: TBTT\_PROHIBIT = 0x80000104

Jun 27 07:02:52 ACN-AP user.warn kernel: type =3, OPMODE = 0x10

Jun 27 07:02:52 ACN-AP user.info kernel: device wlan0 entered promiscuo

Jun 27 07:02:52 ACN-AP user.warn kernel: setup wlan0\_br[0] to 83AF92C0 1

Jun 27 07:02:52 ACN-AP user.warn kernel: +++ OPEN[wlan0] for priv = 0x8;

Open in new window

Close

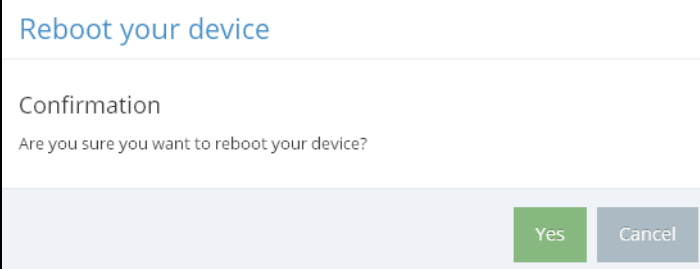
### Downloading the Troubleshooting Log

Click “Troubleshooting 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 troubleshooting log file contains information that can help IgniteNet resolve technical issues with the AP.

### Rebooting the Access Point

The Reboot page allows you to reboot the access point.

Figure 39: Rebooting the Access Point



Reboot your device

---

Confirmation

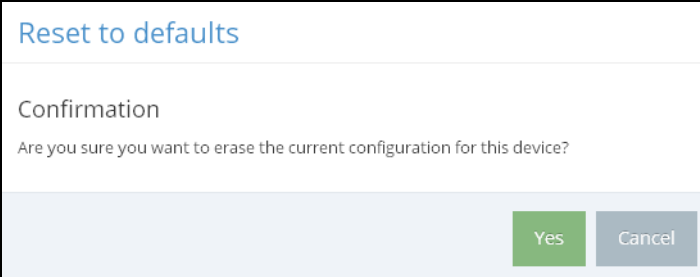
Are you sure you want to reboot your device?

Yes Cancel

### 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 40: Resetting to Defaults



Reset to defaults

---

Confirmation

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

Yes Cancel



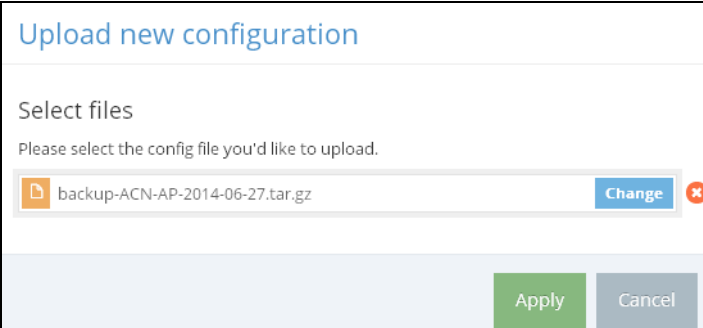
**Note:** It is also possible to reboot or reset the access point by inserting a pin in the pin hole labeled “Reset” on the connector panel of the access point and:

- ◆ press 2 seconds to reboot the access point;
- ◆ press 10 seconds to reset the access point to the 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-IgniteNet-2015-04-10.tar.gz.cpt

**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 41: Restoring Configuration Settings**



Upload new configuration

Select files

Please select the config file you'd like to upload.

backup-ACN-AP-2014-06-27.tar.gz

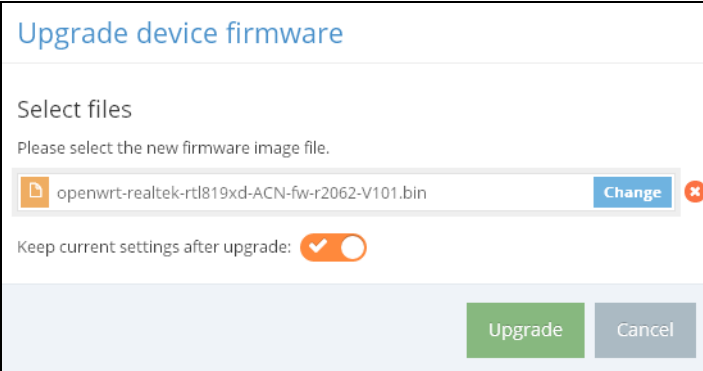
Change

Apply Cancel

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

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 42: Upgrading Firmware**



Upgrade device firmware

Select files

Please select the new firmware image file.

openwrt-realtek-rtl819xd-ACN-fw-r2062-V101.bin

Change

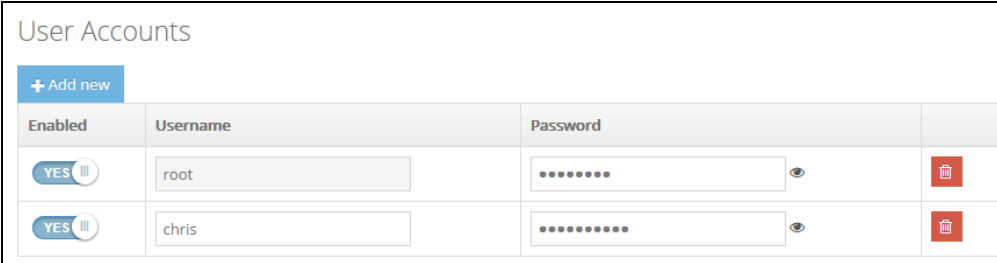
Keep current settings after upgrade: ☒



Upgrade Cancel

## User Accounts

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

**Figure 43: User Accounts**



Enabled	Username	Password	
<input checked="" type="checkbox"/>	root	.....	
<input checked="" type="checkbox"/>	chris	.....	

The following items are displayed on this page:

- ◆ **Enabled** — Click to enable or disable the user account.
- ◆ **Username** — The name of the user. (Range: 3-15 ASCII characters, no special characters)
- ◆ **Password** — The user password. (Range: 3-15 ASCII characters, case sensitive, no special characters)

## Services

The Services page allows you to control remote management access to the AP and configure NTP time servers.

The Telnet, Web, and SNMP management interfaces are enabled and open to access from the Internet. To provide more security, specific services can be disabled and management access prevented from the Internet.

**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 44: SSH Server Settings

The screenshot shows the 'SSH' settings page. At the top, there's a header 'SSH'. Below it, the 'SSH Server' toggle is turned 'ON' with a checkmark icon. Underneath, the 'Port' is set to '22' in a text input field. At the bottom, the 'Allow SSH from WAN' checkbox is checked.


The following items are displayed on this page:

- ◆ **SSH Server** — Enables or disables SSH access to the access point. (Default: Disabled)
- ◆ **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.

### IgniteNet Discovery Tool

The IgniteNet Discovery agent allows the AP to be discovered by other devices on the local network or over the Internet.

Figure 45: IgniteNet Discovery Tool Settings

The screenshot shows the 'IgniteNet Discovery Tool' settings page. At the top, there's a header 'IgniteNet Discovery Tool'. Below it, the 'Discovery Agent' toggle is turned 'ON' with a checkmark icon. Underneath, the 'Allow over WAN' checkbox is checked.


The following items are displayed on this page:

- ◆ **Discovery Agent** — Enables or disables IgniteNet Discovery. (Default: Enabled)
- ◆ **Allow over WAN** — Allows discovery tool access from the WAN.

### Telnet

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

Figure 46: Telnet Server Settings

The screenshot shows the 'Telnet' settings page. At the top, there's a header 'Telnet'. Below it, the 'Telnet Server' toggle is turned 'ON' with a checkmark icon. Underneath, the 'Port' is set to '23' in a text input field. At the bottom, the 'Allow Telnet from WAN' checkbox is checked.

The following items are displayed on this page:

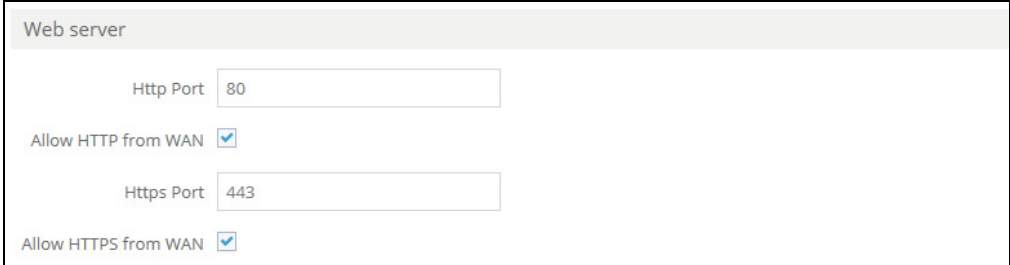
- ◆ **Telnet Server** — Enables or disables Telnet access to the access point.  
(Default: Enabled)
- ◆ **Port** — Sets the TCP port number for the Telnet server on the access point.  
(Range: 1-65535; Default: 23)
- ◆ **Allow Telnet from WAN** — Allows Telnet management access from the WAN.

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

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

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

**Figure 47: Web Server Settings**



Web server

Http Port

Allow HTTP from WAN ☒

Https Port

Allow HTTPS from WAN ☒

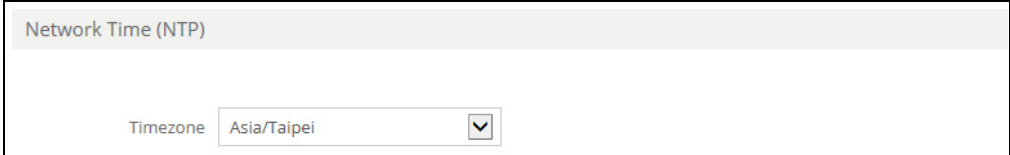
The following items are displayed on this page:

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

**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 startup.

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 sequence to receive a time update.

**Figure 48: NTP Settings**

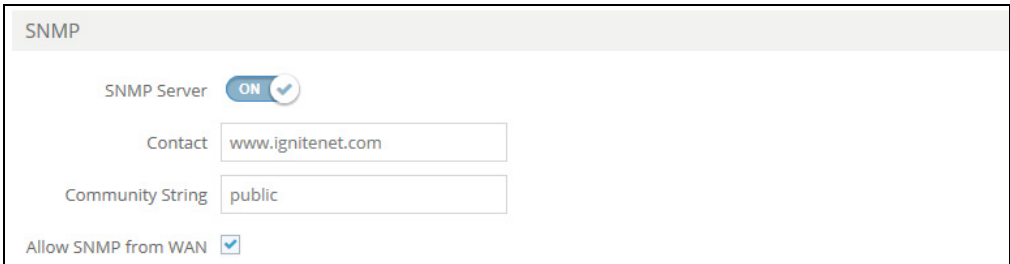


The following items are displayed on this page:

- ◆ **Timezone** — To display a time corresponding to your local time, choose one of the predefined time zones from the scroll-down list.

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

**Figure 49: SNMP Settings**



The following items are displayed on this page:

- ◆ **SNMP Server** — Enables or disables SNMP on the access point. (Default: Enabled)
- ◆ **Contact** — Administrator responsible for the access point.
- ◆ **Community String** — A community string that acts like a password and permits access to the SNMP protocol. (Range: 1-32 characters, case sensitive; Default: public)



The default string “public” provides read-only access to the access point’s Management Information (MIB) database.

- ◆ **Allow SNMP from WAN** — Allows SNMP management access from the WAN.



# Section III

## Appendices

This section provides additional information and includes these items:

- ◆ [“Troubleshooting” on page 68](#)



# Troubleshooting

## Problems Accessing the Management Interface

Table 5: Troubleshooting Chart

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

## 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. Enable SNMP in the System > Services menu.
2. Enable SNMP access from the WAN when connecting from a remote location.
3. Repeat the sequence of commands or other actions that lead up to the error.
4. Make a list of the commands or circumstances that led to the fault. Also make a list of any error messages displayed.
5. Record all relevant system settings.

6. Display the log file through the System > Maintenance page, and copy the information from the log file.
7. Download the Troubleshooting Log to a file from the System > Maintenance page.
8. 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

## A

- AMPDU 53
- authentication 46
  - pre-shared key 46, 47
  - RADIUS server 38, 46, 47
  - WPA 46
  - WPA2 46

## B

- Bandsteering 42
- bootp 46
- bridge mode 18, 34, 49

## C

- captive portal 39
- channel
  - active 27
  - bandwidth 41
  - restrictions 15
  - selection 42
- community string, SNMP 64
- configuration settings
  - restoring 60
  - saving 60
- country code 27, 42
  - selection 13, 15
- CTS, clear to send 53

## D

- data rate, selecting 50
- device status, displaying 27
- DFS 41
- DHCP 13, 30, 31
  - hotspot settings 37
  - lease time 37
  - leases 25
  - server settings 35
  - server status 26
- DNS 25
  - domain name 38
  - IP address 37
  - server address 31
- downloading software 60

## E

- event logs 58

## F

- filter
  - address 49
  - between wireless clients 43
  - HTTP from WAN 63
  - HTTPS from WAN 63
  - management access 61
  - VLANs 54
- firmware
  - displaying version 24
  - upgrading 60

## G

- gateway address 13, 31, 68

## H

- hotspot, configuration 37
- HTTP 63
  - port specification 63
- HTTPS 63
  - port specification 63

## I

- IEEE 802.11a/ac/n 40
  - configuring interface 41
  - radio channel 41
- IEEE 802.11b/g/n 40
  - configuring interface 41
  - radio channel 41
- IEEE 802.1X 47, 48
- initial configuration 13
- introduction 12
- IP address 13, 31, 34
  - configuring 13
  - DHCP 30
  - DNS server 25, 31, 37
  - Ethernet interface 31
  - gateway 25, 31
  - guest network 35

- hotspot 37
- Internet connection 25
- local network 35
- PPPoE 30, 32
- RADIUS server 38
- static 30
- wireless client 28

## L

- log messages 58

## M

- MAC address
  - authentication 48
  - local 25
  - wireless client 28

## O

- open system 46

## P

- password
  - captive portal secret 39
  - community string 64
  - default 13
  - guest network 18
  - PPPoE 32
  - pre-shared key 17, 47
  - user account 61
  - wireless network 18
- PPPoE, configuring 32
- pre-shared key 47

## R

- radio channel
  - active 27
  - configuring 42
- RADIUS 46, 47
  - configuring for IEEE 802.1X 47
  - configuring for WPA 47
  - configuring local settings 38
  - IP address 38
- rate limiting 49
- reset button 57
- router mode 18, 34, 49
- RTS, threshold 53

## S

- SGI 53

- shared key 46, 47
- SNMP 12
  - allow from WAN 65
  - community string 64
  - enabling 64
- SNTP 64
- software
  - displaying version 24
  - upgrading 60
- SSID 18, 28, 40, 41, 43, 46, 55
- status information
  - Internet 25
  - local network 26
  - wireless 27
- STBC 53
- STP, spanning tree protocol 36
- subnet mask 13, 26, 31, 35, 37, 68
- system log 58
- system software, upgrading 60

## T

- time zone 64
- transmit power 15
  - configuring 52

## U

- upgrading software 60
- user password 13, 61

## V

- VLAN, configuration 54

## W

- WDS 41
- WEP 46
- WEP, shared key 46
- WMM 43, 44
- WPA 46, 47
- WPA, pre-shared key 47
- WPA2 47

