IgniteNet

User Manual

MetroLinq™

Software Release v1.1.2



User Manual

IgniteNet MetroLinq™

Cloud-Enabled 60 GHz Outdoor Point-to-Point Access Point

FW1.1.2
E042016-CS-R01
150200001394A

How to Use This Guide

This guide includes detailed information on IgniteNet MetroLinqaccess 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.

April 2016 Revision

This is the first revision of this guide. It is valid for software release v1.1.2.

Contents

How to Use This Guide 3

Contents 5

Figures 8

Tables 10

Section I Getting Started 11

1 Introduction 12

Configuration Options 12

Network Connections 13

Connecting to the Web Interface 13

Setup Wizard 14

Main Menu 16

Dashboard 17

Common Web Page Buttons 17

Section II Web Configuration 19

2 Status Information 20

System and Product Information 20

Internet Status 21

Port Status 22

Interface Information 22

Wireless Status 23

Traffic Graphs 24

Services 24

3 Network Settings 25

Internet Settings 25
Ethernet Settings 27

4 Wireless Settings 29
Radio Settings 29
Physical Radio Settings 29
Wireless Networks — General Settings 31
Wireless Networks — Security Settings 32
Advanced Radio Settings 32

5 System Settings 34
System Settings 35
Maintenance 36
Displaying System Logs 36
Downloading the Troubleshooting Log 37
Rebooting the Access Point 37
Resetting the Access Point 37
Backing Up Configuration Settings 38
Restoring Configuration Settings 38
Upgrading Firmware 38
User Accounts 39
Services 39
SSH 39
IgniteNet Discovery Tool 40
Telnet 40
Web Server 41
Network Time 41
Diagnostics 42

Section III Appendices 43

A Troubleshooting 44
Problems Accessing the Management Interface 44
Using System Logs 44

Index 46

Figures

Figure 1: Login Page 14
Figure 2: Select Your Country 14
Figure 3: Select Cloud Managed 15
Figure 4: The Dashboard 17
Figure 5: Set Configuration Changes 17
Figure 6: System and Product Information 20
Figure 7: Internet Status 21
Figure 8: Port Status 22
Figure 9: Interface Information 22
Figure 10: Wireless Status 23
Figure 11: Traffic Graphs 24
Figure 12: Services 24
Figure 13: Internet Settings 25
Figure 14: IP Address Mode – Static IP 26
Figure 15: IP Alias 27
Figure 16: Ethernet Settings – Internet Source 28
Figure 17: Ethernet Settings – Network Behavior 28
Figure 18: Radio Settings (Physical Radio Settings) 29
Figure 19: 60 GHz Radio Settings (Physical Radio Settings) 31
Figure 20: Radio Settings (General Settings) 31
Figure 21: Wireless Security Settings 32
Figure 22: Advanced Radio Settings 32
Figure 23: System Settings 35
Figure 24: Maintenance 36
Figure 25: System Log 36
Figure 26: Rebooting the Access Point 37
Figure 27: Resetting to Defaults 37
Figure 28: Restoring Configuration Settings 38
Figure 29: Upgrading Firmware 38

Figure 30: User Accounts 39
Figure 31: SSH Server Settings 40
Figure 32: IgniteNet Discovery Tool Settings 40
Figure 33: Telnet Server Settings 40
Figure 34: Web Server Settings 41
Figure 35: NTP Settings 42
Figure 36: Diagnostics 42

Tables

Table 1: Radio Channels 30
Table 2: Troubleshooting Chart 44

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 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 web interface allows you to perform management functions such as:

- Set management access user names and passwords
- Configure IP settings
- Configure 60 GHz and 5 GHz radio settings
- Control access through wireless security settings
- 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 192.168.1.20 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 LAN 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 14 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 "Internet Settings" on page 25.

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

Connecting to the Web Interface

The AP offers a user-friendly web-based management interface for the configuration of all the unit's features. Any PC directly attached to the unit can access the management interface using a web browser, such as Internet Explorer 9.x or later, Mozilla Firefox 32 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 192.168.1.20 and a subnet mask of 255.255.255.0. You must set your PC IP address to be on the same subnet as the AP (that is, the PC and AP addresses must both start with192.168.1.x).

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

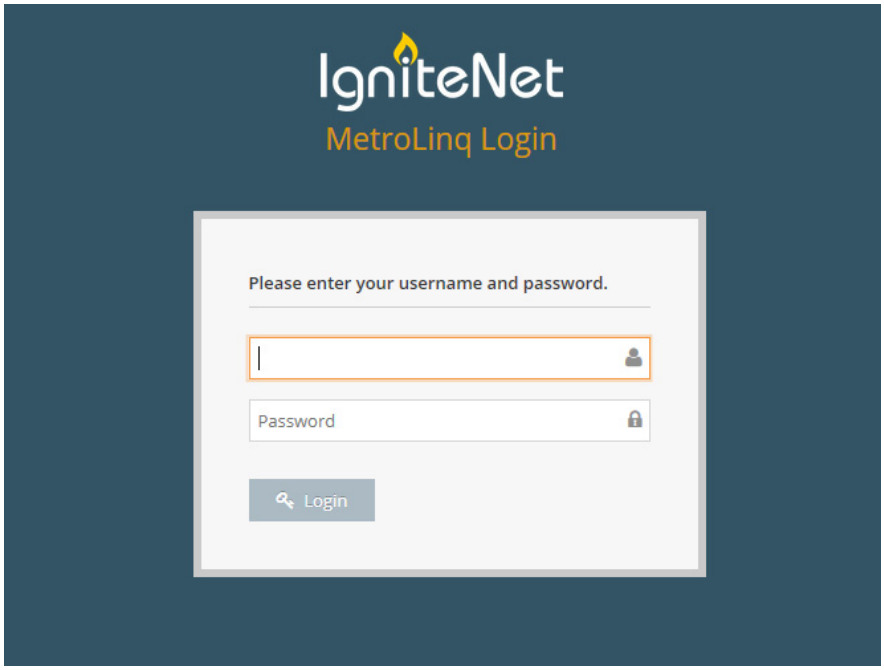
1. Use your web browser to connect to the management interface using the default IP address of 192.168.1.20.

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 39.

Figure 1: Login Page

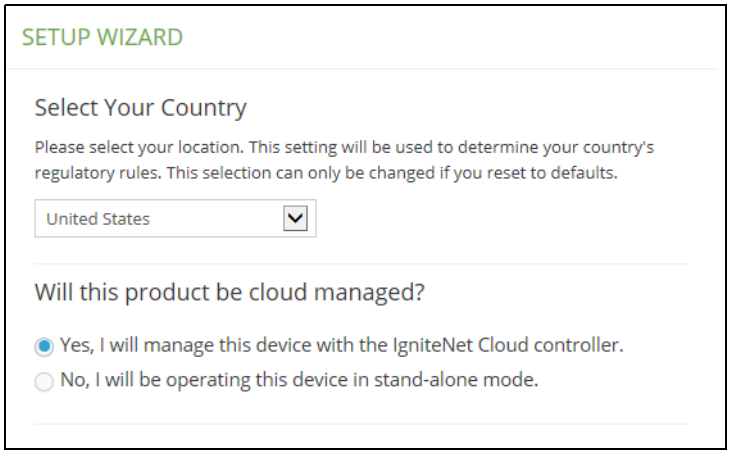


Setup Wizard

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



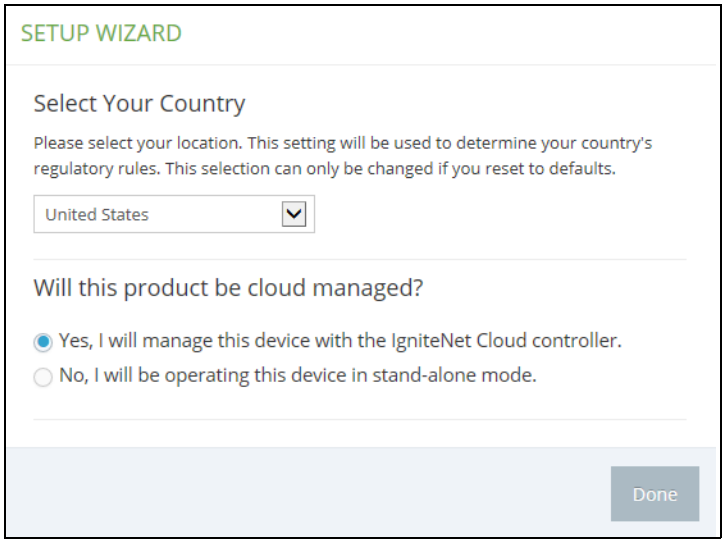
Caution: You must set the country code to the country of operation. Setting the country code ensures that the radios operate within the local regulations specified for wireless networks.

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." Otherwise, select "No, I will be operating this device in stand-alone mode."

Click "Done" to complete the Setup Wizard.

Figure 3: Select Cloud Managed



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.

Main Menu

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

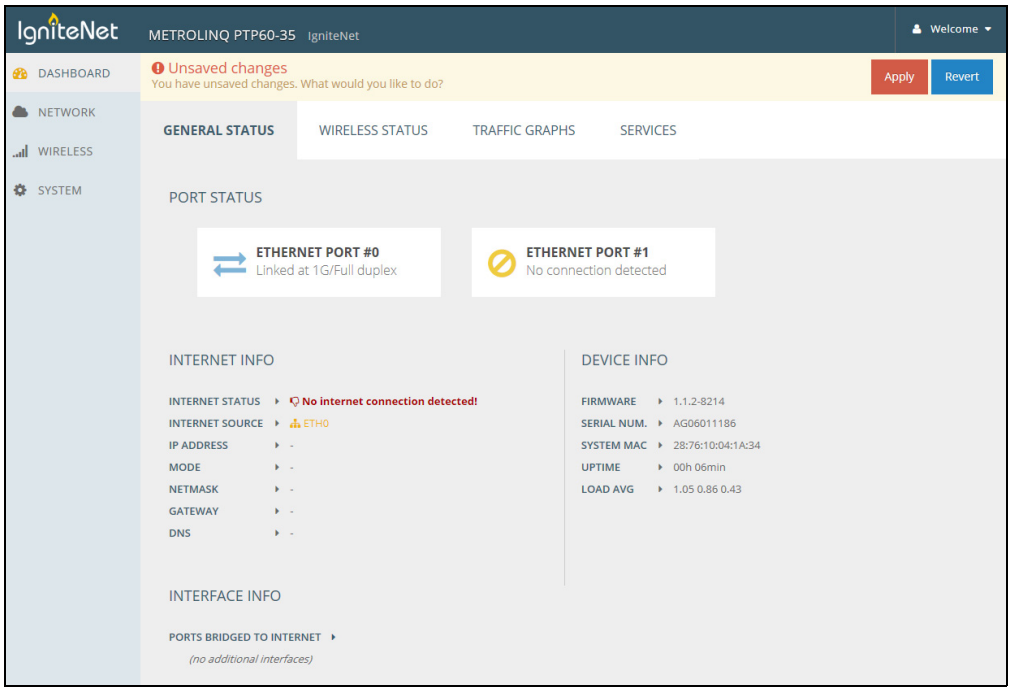
To configure settings, click the relevant Main Menu item. Each Main Menu item is summarized below with links to the relevant section in this guide where the configuration parameters are described in detail:

- **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 20.
- **Network** — Configures Internet and Ethernet settings. See "Network Settings" on page 25.
- **Wireless** — Configures 5 GHz and 60 GHz radio settings. See "Wireless Settings" on page 29
- **System** — Configures System (designation and location), Maintenance (such as view log, firmware upgrade, and reset), User Accounts, Services (management access methods), and Diagnostics (Ping, Traceroute, and Nslookup).

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, traffic graphs, and services.

Figure 4: The Dashboard

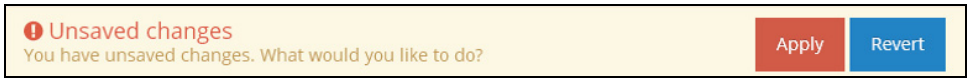


Common Web Page Buttons

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 5: 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 20
- "Network Settings" on page 25
- "Wireless Settings" on page 29
- "System Settings" on page 34

2 Status Information

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

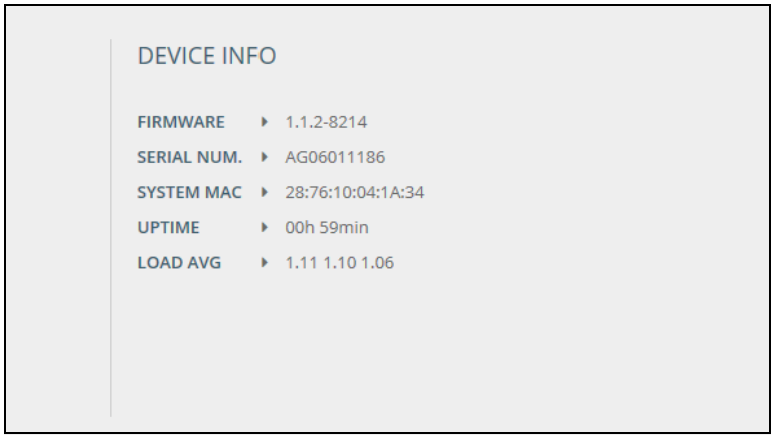
Status Information includes the following sections:

- "System and Product Information" on page 20
- "Internet Status" on page 21
- "Port Status" on page 22
- "Interface Information" on page 22
- "Wireless Status" on page 23
- "Traffic Graphs" on page 24
- "Services" on page 24

System and Product Information

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

Figure 6: System and Product Information



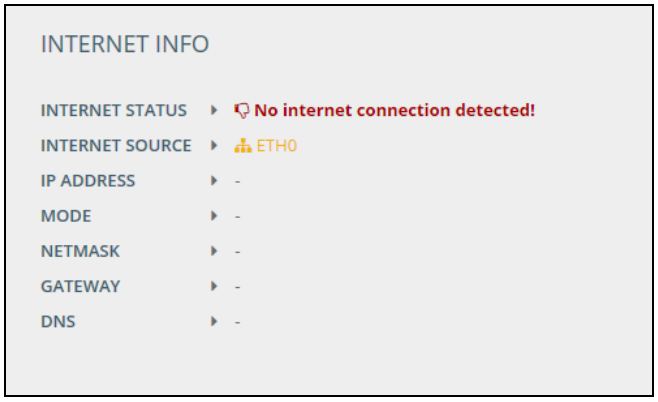
The following items are displayed in this section:

- The software version number.
- The serial number of the physical access point.
- The system MAC address of the 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 Info section shows information about the Internet connection.

Figure 7: Internet Status



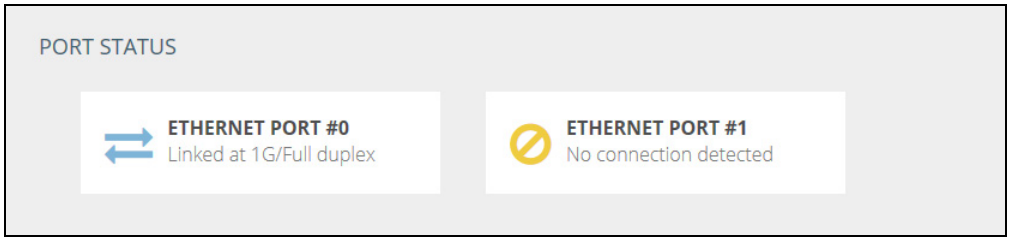
The following items are displayed in this section:

- **Internet Source** — The Ethernet port connected to the Internet. By default, this is Ethernet Port 0.
- **IP Address** — IP address of the Internet connection.
- **Mode** — Shows if the IP address is a static setting or by DHCP.
- **Netmask** — The subnet mask of the IP address.
- **Gateway** — The IP address of the gateway router that is used when a destination address is not on the local subnet.
- **DNS** — The IP address of the Domain Name Server on the network. A DNS maps numerical IP addresses to domain names and can be used to identify network hosts by familiar names instead of the IP addresses.

Port Status

The Port Status section shows information about Ethernet port connections.

Figure 8: Port Status



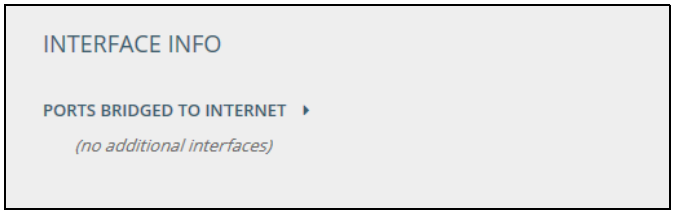
The following items are displayed in this section:

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

Interface Information

The Interface Info section shows information about additional interfaces connected to the Internet.

Figure 9: Interface Information



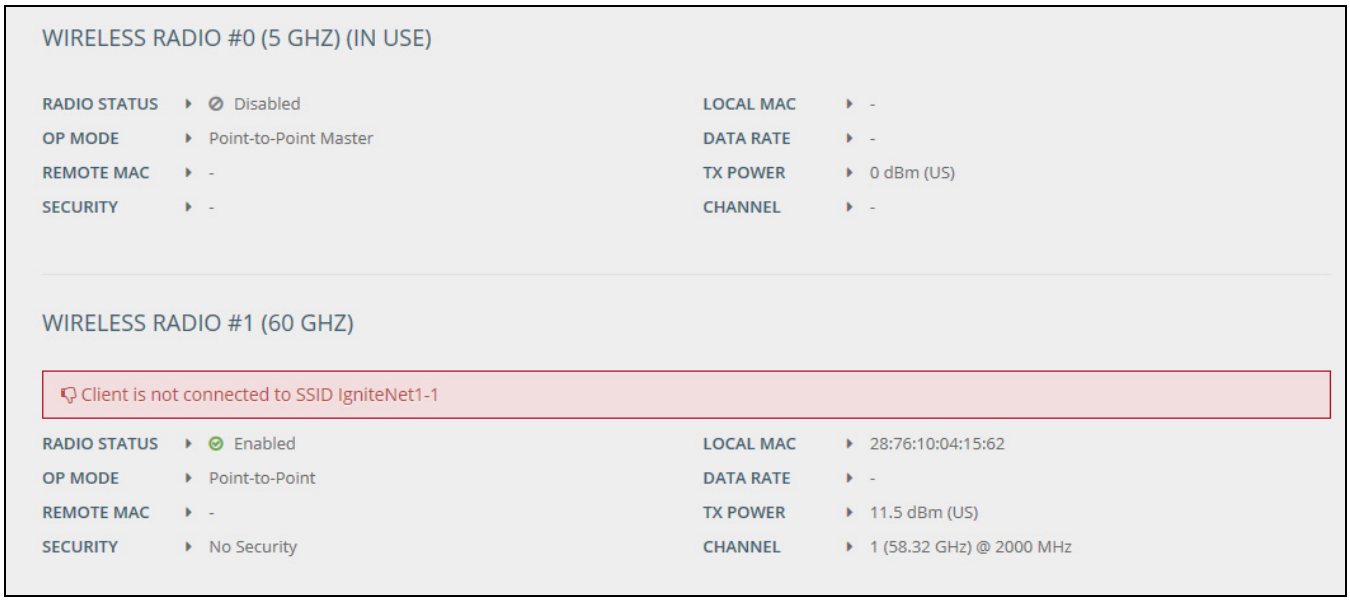
The following items are displayed in this section:

- **Ports Bridged to Internet** — Additional interfaces attached directly to the Internet. Lists interfaces attached to the WAN (that is, the Internet). The MetroLinq bridges all wired and wireless interfaces and this configuration cannot be modified.

Wireless Status

The Wireless Status section shows information about the radio settings and link status of the 5 GHz and 60 GHz wireless interfaces.

Figure 10: Wireless Status



The following items are displayed in this section:

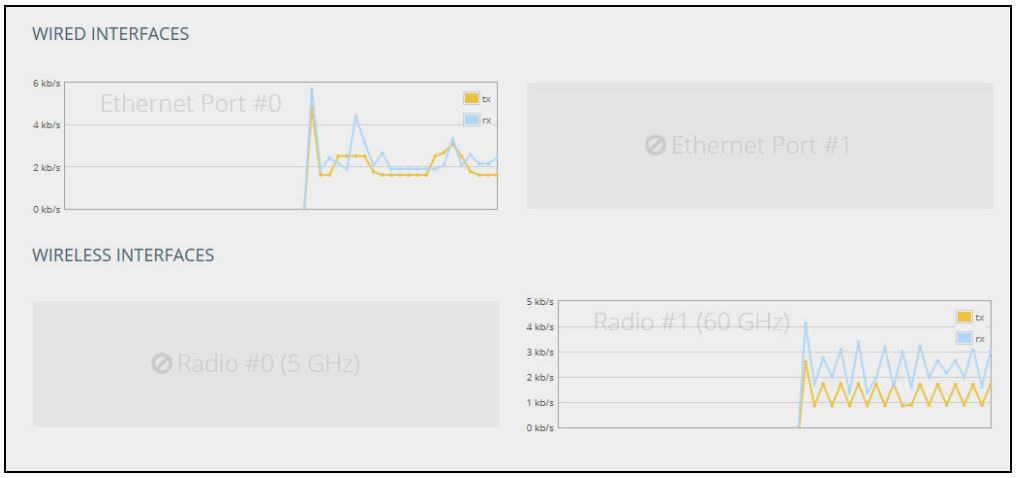
- Radio Status — Shows if the wireless interface is enabled or disabled.
- Op Mode — Shows if the wireless interface is configured to operate in Point-to-Point Master, Point-to-Point Slave, or Point-to-Point Auto mode.
- Remote MAC — The MAC address of the remote AP.
- Security — Shows whether or not security has been enabled.
- Local MAC — The MAC address of the AP radio interface.
- Data Rate — The data transmit rate on the wireless link.
- Tx Power — The power of the radio signals transmitted from the AP.
- Channel — The radio channel the access point uses to communicate on the point-to-point link. The available channels depend on the Channel Bandwidth[1] and Country Code settings[2].

1. See "Radio Settings" on page 29.
2. See "Setup Wizard" on page 14.

Traffic Graphs

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

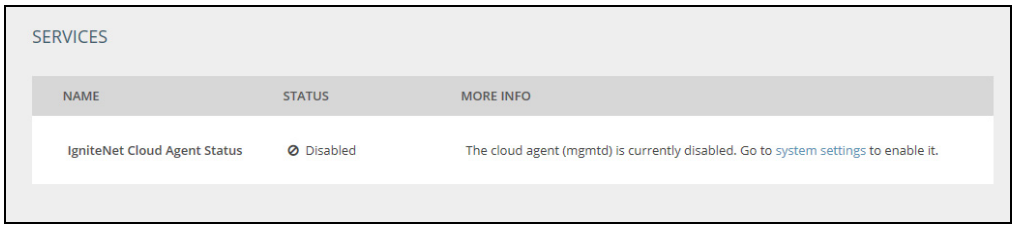
Figure 11: Traffic Graphs



Services

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

Figure 12: Services



3 Network Settings

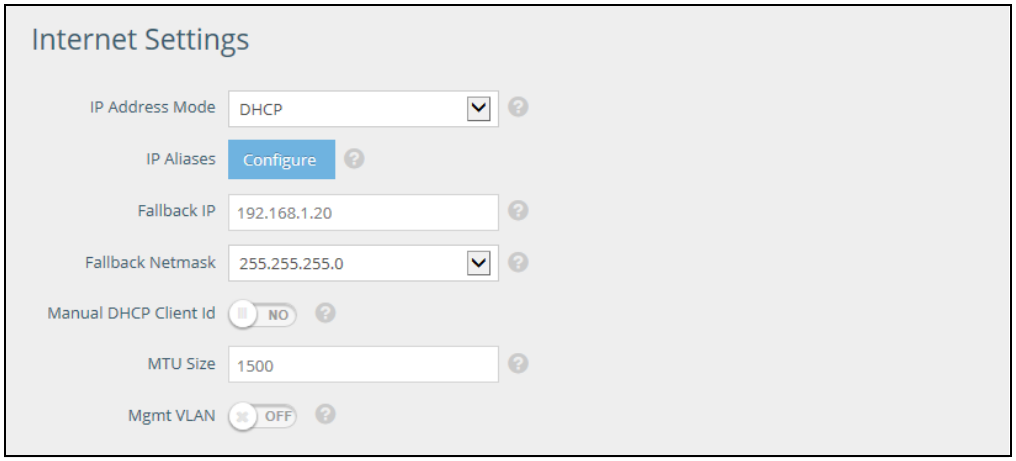
This chapter describes basic network settings on the access point. It includes the following sections:

- "Internet Settings" on page 25
- "Ethernet Settings" on page 27

Internet Settings

The Internet Settings page configures the basic Internet settings for the AP, such as the IP address mode, IP aliases, as well as the maximum MTU size.

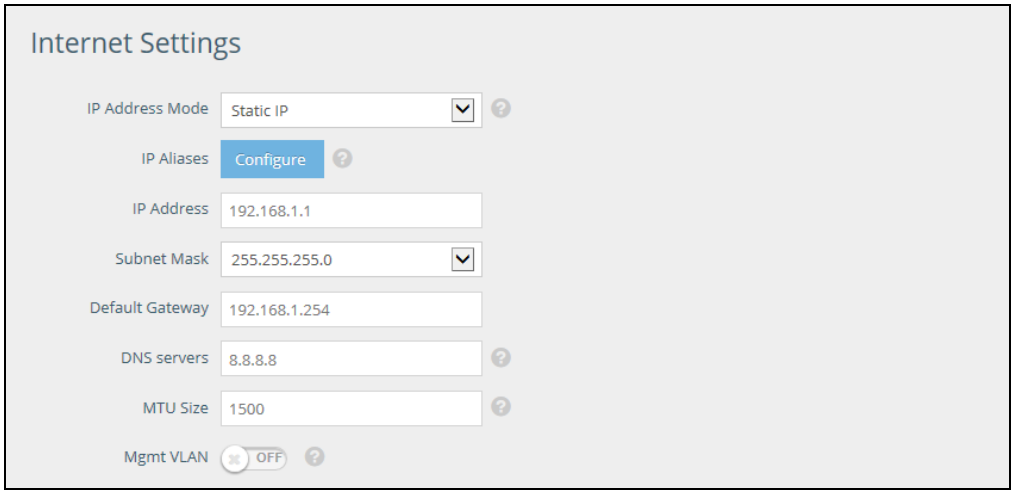
Figure 13: Internet Settings



The following items are displayed on this page:

- **IP Address Mode** — The method used to provide an IP address for the Internet access port. (Default: DHCP; Options: DHCP, static IP)
  - **DHCP** — Configuration options displayed for DHCP are shown in Figure 13, "Internet Settings", on page 25.
  - **Static IP** — To configure a static IP address for the selected Ethernet interface, the following items must be specified.

Figure 14: IP Address Mode – Static IP



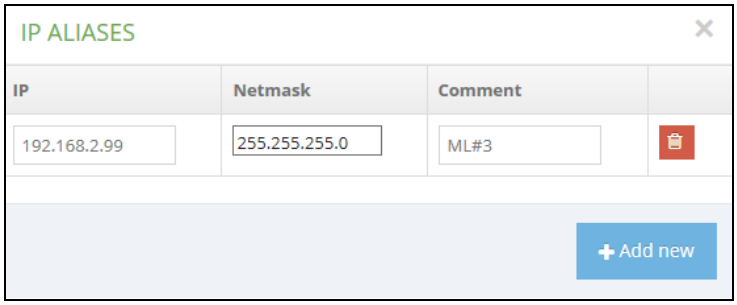
- **IP Address** — Specifies an IP address for the access point. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
- **Subnet Mask** — Indicates the local subnet mask. (Default: 255.255.255.0)
- **Default Gateway** — The IP address of the default gateway, which is used if the requested destination address is not on the local subnet.

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

  If you have a DNS servers located on the local network, type the IP addresses in the text field provided. Up to four IP addresses can be entered, each separated by spaces.

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

Figure 15: IP Alias



- **Fallback IP** — The IPv4 address used when a DHCP server is unavailable. (Default: 192.168.1.20)
- **Fallback Netmask** — The subnet mask used for the Fallback IP address. (Default: 255.255.255.0)
- **Manual DHCP Client ID** — An optional hostname used to identify the DHCP client.
- **MTU Size** — Sets the size of the maximum transmission unit (MTU) for packets sent on this interface. (Range: 1400-7912 bytes; Default 1500 bytes)
- **Mgmt VLAN** — Configures a specific VLAN for only AP management traffic. (Range: 0-4094)

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

Ethernet Settings

The Ethernet Settings page configures the network behavior of the Ethernet ports, indicating that a port provides an Internet connection.

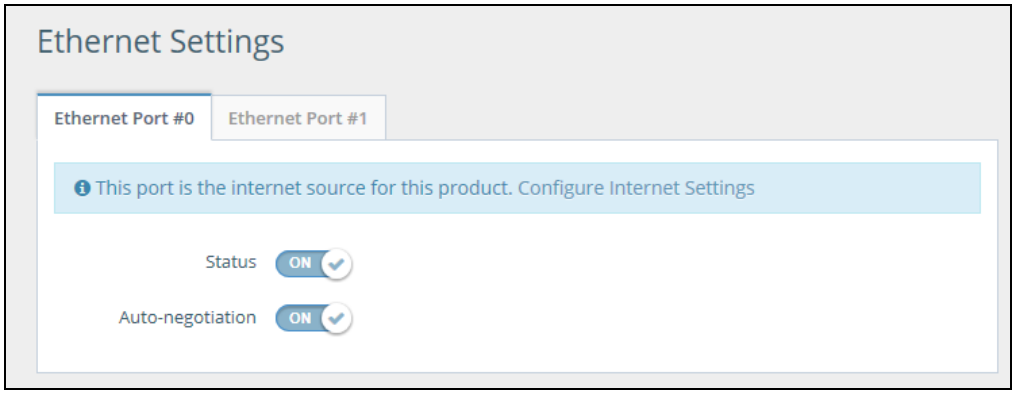
The following items are common for all pages under Ethernet Settings:

- **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 16: Ethernet Settings – Internet Source

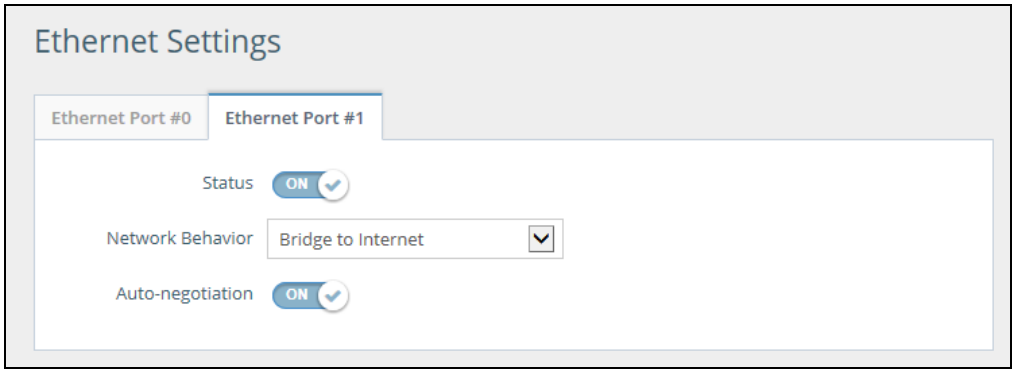


The following status message is displayed if an interface is set as the Internet source:

- "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 17: Ethernet Settings – Network Behavior



The following items are displayed on this page:

- **Network Behavior** — For the Ethernet port which is not providing Internet access, the following connection method must be specified. (Default: Bridge to Internet)

  - **Bridge to Internet** — Configures an interface to be attached to the WAN. Traffic from this interface is directly bridged into the Internet. The MetroLinq has all interfaces set as Bridge to Internet.

4 Wireless Settings

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

- "Radio Settings" on page 29

Radio Settings

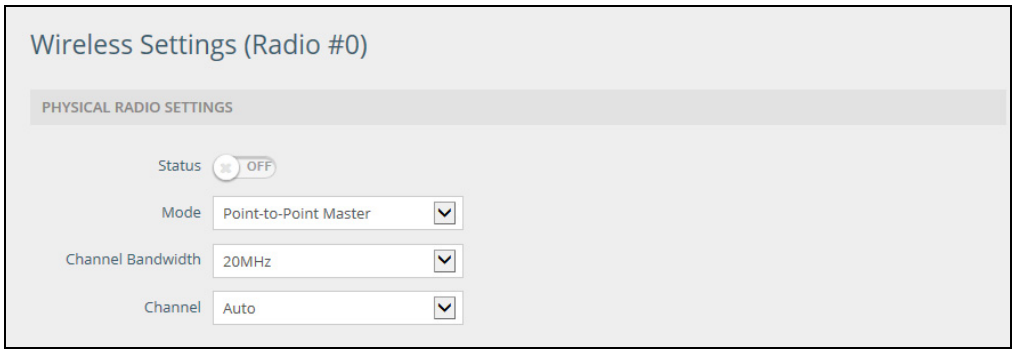
The IEEE 802.11 wireless interfaces include configuration options for radio signal characteristics and wireless security features.

The access point can operate in two radio modes, 802.11ac at 5 GHz and 802.11ad at 60 GHz. Note that the access points can operate at 60 GHz and 5 GHz at the same time, or use the 5 GHz interface as a backup link. The web interface identifies the radio configuration pages as:

- **Radio 0** — the 5 GHz 802.11ac radio interface
- **Radio 1** — the 60 GHz 802.11ad radio interface

Physical Radio Settings

Figure 18: Radio Settings (Physical Radio Settings)



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.
  - **Point-to-Point Master** — (Outdoor APs only) Sets the AP radio as the Master in a point-to-point wireless link between two IgniteNet units. A

point-to-point wireless link requires one unit set as Master and the other set to Slave. Links to any non-IgniteNet units will not work.

- **Point-to-Point Slave** — (Outdoor APs only) Sets the AP radio as the Slave in a point-to-point wireless link between two IgniteNet units.

- **Channel Bandwidth** — The AP options for 5 GHz channel bandwidths include 5, 10, 20, 40 and 80 MHz. Using a larger channel bandwidth setting provides a higher connection speed. For the 60 GHz radio, the channel bandwidth is fixed at 2000 MHz. (5 GHz Default: 20 MHz; 5 GHz Range: 5 MHz, 10 MHz, 20 MHz, 40 MHz, 80MHz)

- **Channel** — The radio channel that the access point uses to communicate on the point-to-point link. Note that the AP at the other end of the link must be set to the same channel and channel bandwidth. (The available channels are dependent on the 802.11 band, Channel Bandwidth, and Country Code settings.)

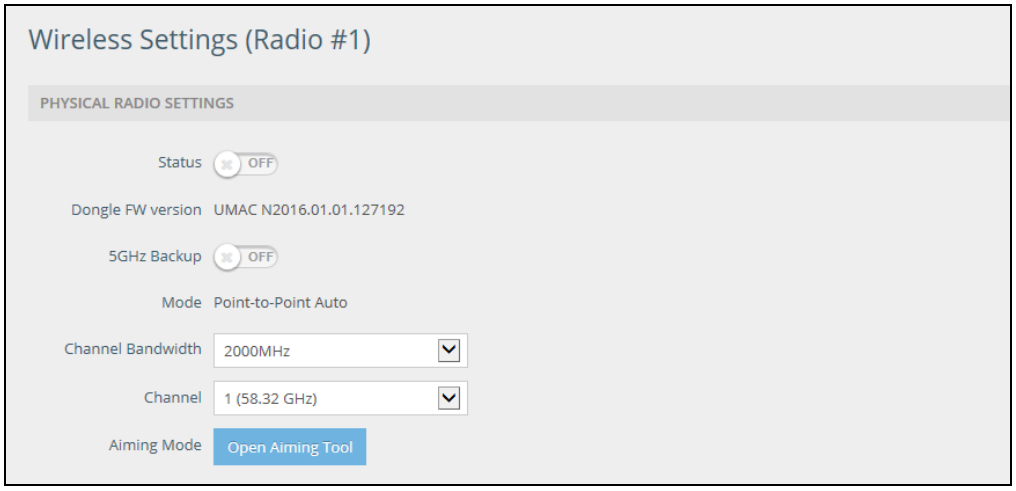
  Selecting Auto (5 GHz) enables the access point to automatically select an unoccupied radio channel. (5 GHz Default: Auto, 60 GHz Default: 1)

Table 1: Radio Channels

Radio 0 (5 GHz)		Radio 1 (60 GHz)	
Radio Channels[a]	**Frequency (GHz)**	**Radio Channels**	**Frequency (GHz)**
Auto	Auto scan	1	58.32
36	5.180	2	60.48
40	5.200	3	62.64
44	5.220	4	64.80
48	5.240		
149	5.745		
153	5.765		
157	5.785		
161	5.805		
165	5.825		

a. Supported channels depend on the channel bandwidth.

Figure 19: 60 GHz Radio Settings (Physical Radio Settings)

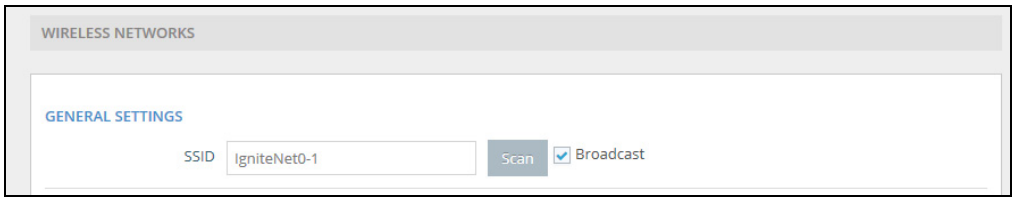


The following additional items are displayed on the 60 GHz radio page:

- **Dongle FW Version** — The firmware version of the 60 GHz radio.
- **5 GHz Backup** — Enables the 5 GHz interface to operate as a backup for the 60 GHz interface. If there is a link failure on the 60 GHz interface, traffic is automatically forwarded to the 5 GHz interface. When the 60 GHz link is restored, traffic reverts back to the 60 GHz interface.
- **Aiming Mode** — Opens the antenna alignment tool for 60 GHz point-to-point links. You can set the tool to operate in a transmit or receive mode. In transmitter mode, the AP continuously sends a signal. In receiver mode, you can visually monitor the received signal strength from the web interface while adjusting the antenna alignment.

Wireless Networks — General Settings

Figure 20: Radio Settings (General Settings)



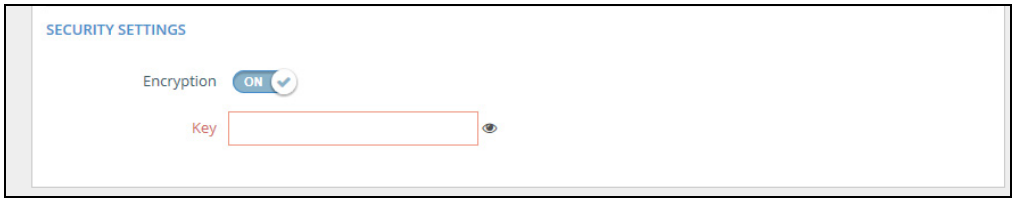
The following items are displayed in this section of the Wireless Settings page:

- **SSID** — The name of the basic service set provided by the interface. APs at each end of a point-to-point link must set the same SSID. (Default: IgniteNet0-1 for 5 GHz, IgniteNet1-1 for 60 GHz; Range: 1-32 characters)
- **Broadcast** — The SSID can be broadcast at regular intervals so that other APs can scan and discover it. This feature also makes it easier for hackers to break

into your network because SSIDs are not encrypted, For better security, you can disable the broadcast and configure SSIDs manually. (Default: Enabled)

Wireless Networks — Security Settings

Figure 21: Wireless Security Settings

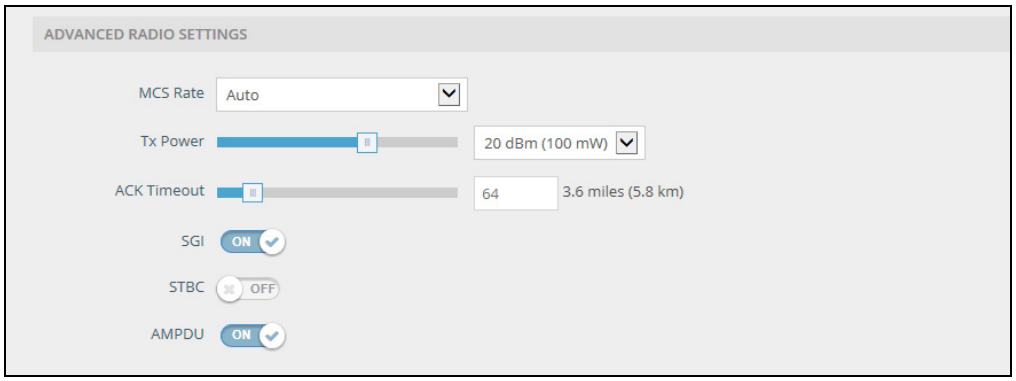


The following items are displayed in this section of the Wireless Settings page:

- **Encryption** — Sets the wireless security method for the interface. (Default: Off)
  - **Off (No Security)** — When the Encryption is set to off, there is no security on the wireless link.
  - **On (WPA2-PSK)**: APs in the point-to-point link use WPA2 security with a Pre-shared Key for authentication and encryption.
    - **Key** — WPA2-PSK uses static shared keys (fixed-length hexadecimal or alphanumeric strings) that are manually configured. The string length must be 8 to 63 ASCII characters (letters and numbers). No special characters are allowed.

Advanced Radio Settings

Figure 22: Advanced Radio Settings



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

- **MCS Rate** — The minimum data rate at which the AP transmits packets on the wireless interface. A setting of "Auto" sets the rate depending on the signal strength.
- **Tx Power** — Adjusts the power of the radio signals transmitted from the access point. The higher the transmission power, the farther the transmission range. Power selection is not just a trade off between coverage area and maximum

supported clients. You also have to ensure that high-power signals do not interfere with the operation of other radio devices in the service area. (The range of power settings and defaults are dependent on the AP model, radio band, and the Country setting.)

- **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. (5 GHz Range: 32-255 microseconds; Default: 64 microseconds, 60 GHz Range: 10-28 microseconds; Default: 10 microseconds)

- **SGI** — The 802.11 standard 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: Enabled)

- **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)

5 System Settings

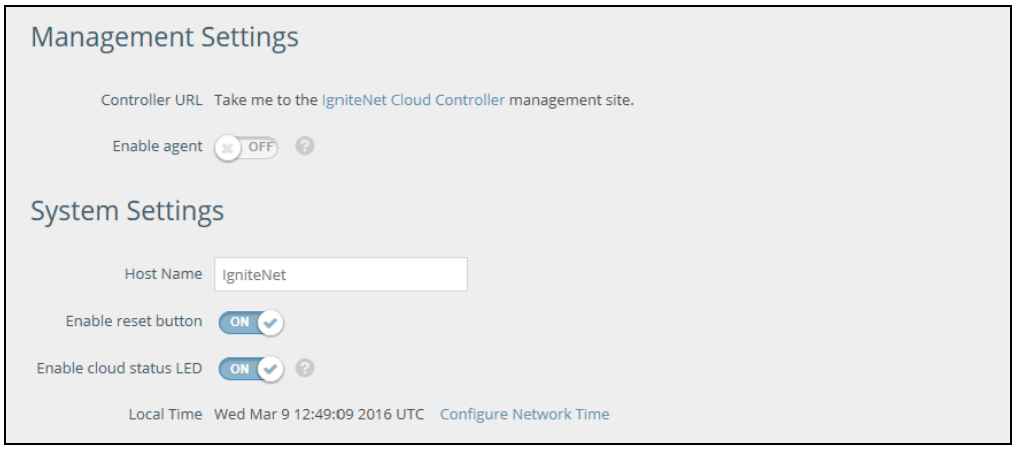
This chapter describes maintenance settings on the access point. It includes the following sections:

- "System Settings" on page 35
- "Maintenance" on page 36
- "User Accounts" on page 39
- "Services" on page 39
- "Diagnostics" on page 42

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 23: System Settings



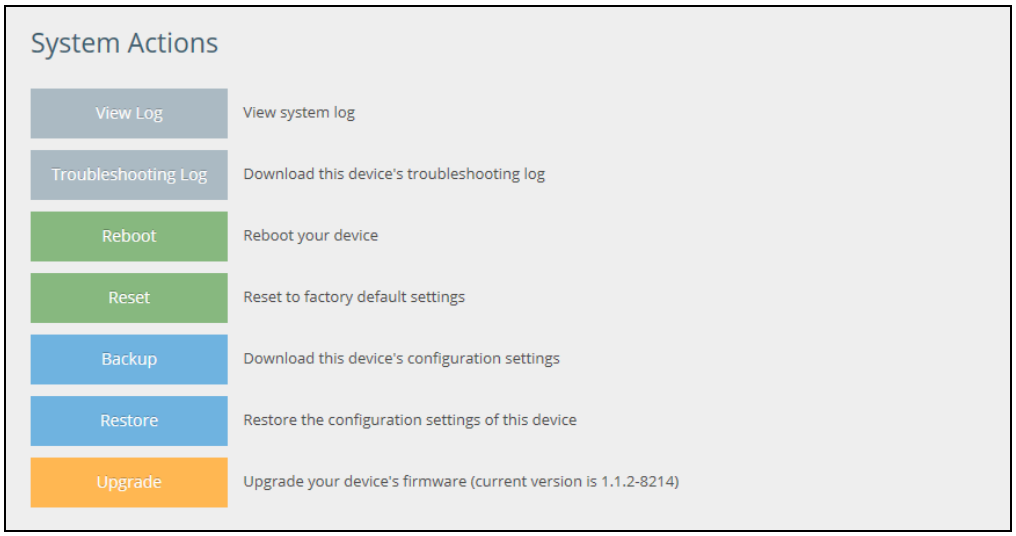
The following items are displayed on this page:

- **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.

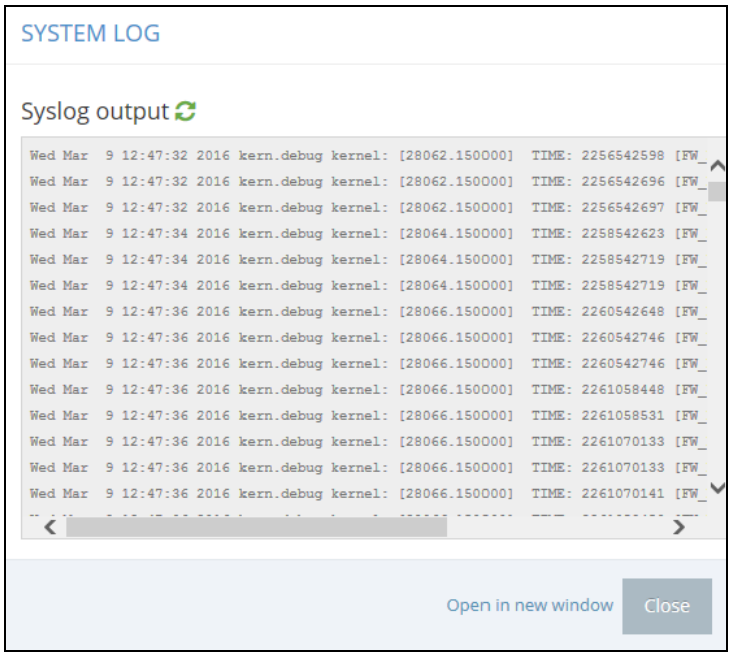
Figure 24: Maintenance



Displaying System Logs

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

Figure 25: System Log



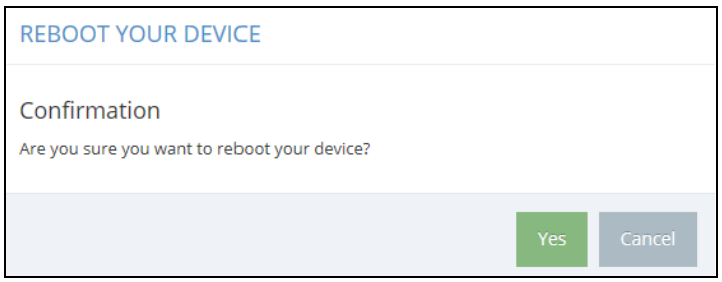
Downloading the Troubleshooting Log

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.

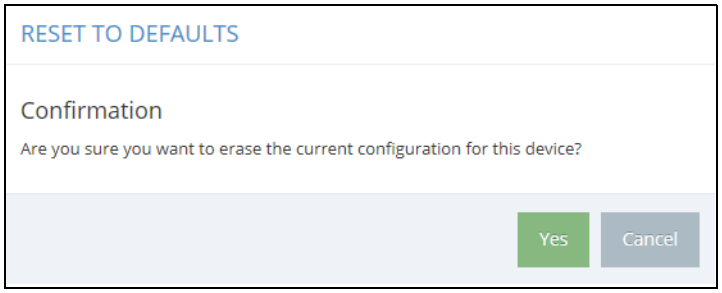
Figure 26: Rebooting the Access Point



Resetting the Access Point

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

Figure 27: Resetting to Defaults



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

- press 2 seconds to reboot the access point;
- press 5 seconds to reset the access point to the factory defaults.

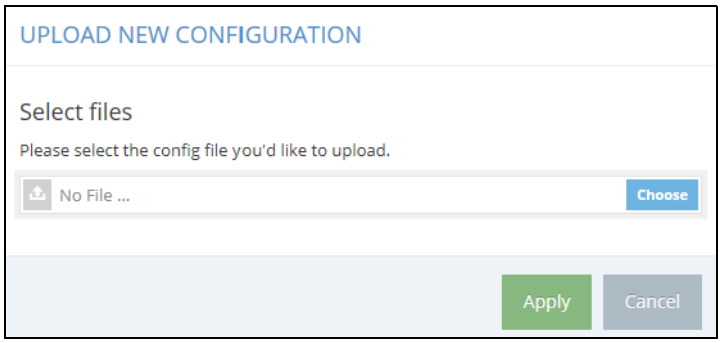
Backing Up Configuration Settings

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-2016-03-09.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 28: Restoring Configuration Settings

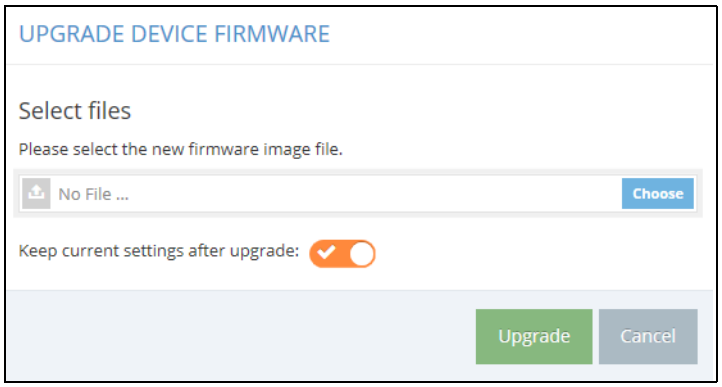


Upgrading Firmware

You can upgrade new access point software from a local file on the management workstation. New software may be provided periodically from 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 configurtion settings are corrupted, the system defaults will be used.

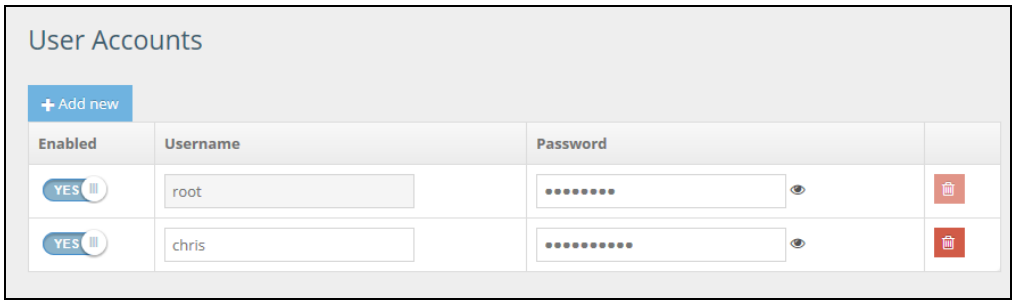
Figure 29: Upgrading Firmware



User Accounts

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

Figure 30: User Accounts



The following items are displayed on this page:

- **Enabled** — Click to enable or disable the user account.
- **Username** — The name of the user. (Range: 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.

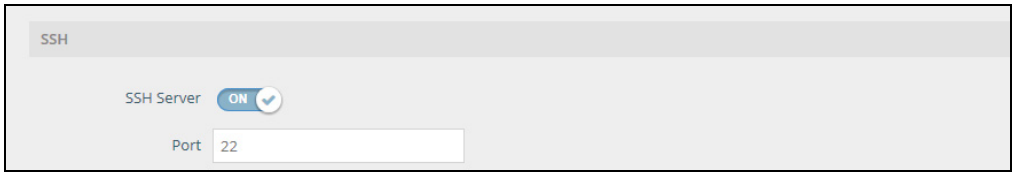
The Telnet and Web management interfaces are enabled and open to access from the Internet. To provide more security, specific services can be disabled and management access prevented from the Internet.

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 31: SSH Server Settings



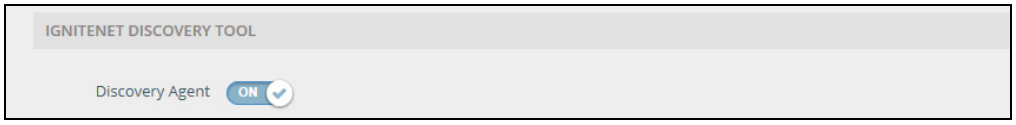
The following items are displayed on this page:

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

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 32: IgniteNet Discovery Tool Settings



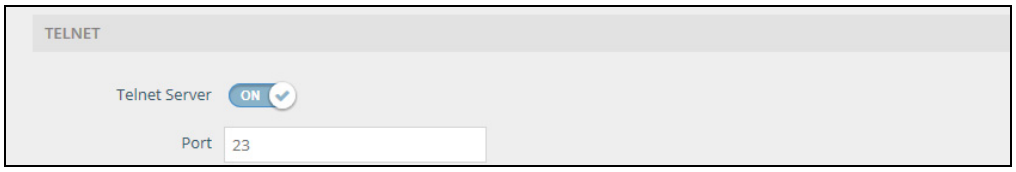
The following items are displayed on this page:

- **Discovery Agent** — Enables or disables IgniteNet Discovery. (Default: Enabled)

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 33: Telnet Server Settings



The following items are displayed on this page:

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

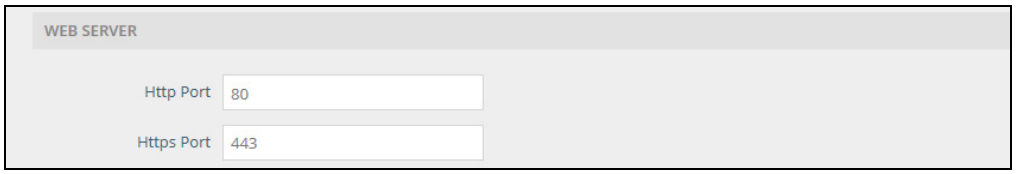
Web Server

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 34: Web Server Settings



The following items are displayed on this page:

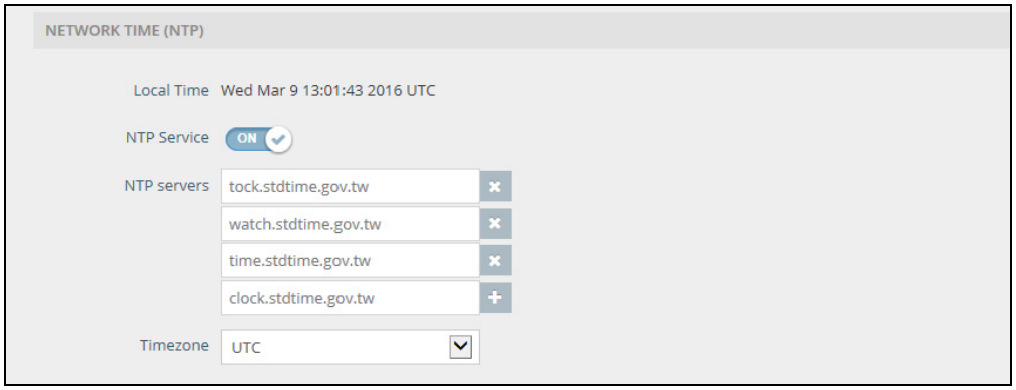
- **HTTP Port** — The TCP port to be used by the HTTP Web browser interface. (Range: 1-65535; Default: 80)
- **HTTPS Port** — The TCP port to be used by the HTTPS Web browser interface. (Range: 1-65535; Default: 443)

Network Time

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

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

Figure 35: NTP Settings



The following items are displayed on this page:

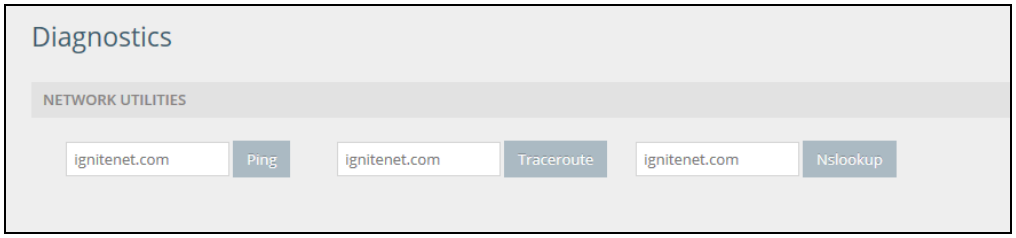
- **Local Time** — Displays the local time as day of week, month, hour:minute:second, year, based on Universal Time Coordinates.
- **NTP Service** — Enables or disables sending of requests for time updates. (Default: Enabled)
- **NTP Servers** — Sets the host names for time servers. The switch attempts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

Diagnostics

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

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

Figure 36: Diagnostics



Section III

Appendices

This section provides additional information and includes these items:

- "Troubleshooting" on page 44

A Troubleshooting

Problems Accessing the Management Interface

Table 2: Troubleshooting Chart

Symptom	Action
Cannot connect using Telnet or web browser	◆ Be sure the AP is powered up. ◆ Check network cabling between the management station and the AP. ◆ Check that you have a valid network connection to the AP and that intermediate switch ports have not been disabled. ◆ Be sure you have configured the AP with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the AP's IP. ◆ If you are trying to connect to the AP using a tagged VLAN group, your management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag. ◆ If you cannot connect using Telnet, you may have exceeded the maximum number of concurrent Telnet/SSH sessions permitted. Try connecting again at a later time.
Forgot or lost the password	◆ Reset the AP to factory defaults using its Reset button.

Using System Logs

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

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

6. 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 33
authentication
    pre-shared key 32

B

bridge mode 28

C

channel
    active 23
    bandwidth 30
    restrictions 14
    selection 30
configuration settings
    restoring 38
    saving 38
country code 23, 30
    selection 13, 14

D

data rate, selecting 32
device status, displaying 23
DHCP 13, 25
DNS 21
    server address 26
downloading software 38

E

event logs 36

F

filter
    management access 39
firmware
    displaying version 21
    upgrading 38

G

gateway address 13, 26, 44

H

HTTP 41
    port specification 41
HTTPS 41
    port specification 41

I

IEEE 802.11a/ac/n 29
IEEE 802.11b/g/n 29
initial configuration 13
introduction 12
IP address 13, 26
    configuring 13
    DHCP 25
    DNS server 21, 26
    Ethernet interface 25
    gateway 21, 26
    Internet connection 21
    PPPoE 25
    static 25

L

log messages 36

M

MAC address
    local 22

N

NTP
    enabling 42
    servers 42

P

password
    default 13
    user account 39

R

radio channel
    active 23

configuring 30
reset button 35

S

SGI 33
shared key 32
SNTP 41
software
displaying version 21
upgrading 38
SSID 24, 31
status information
Ethernet ports 22
interfaces 22
Internet 21
wireless 23
STBC 33
subnet mask 13, 26, 44
system log 36
system software, upgrading 38

T

time zone 42
transmit power 14
configuring 32

U

upgrading software 38
user password 13, 39

W

WPA2 32