antaira®

making connectivity simple...

Wireless Software User's Manual

Version 1.1

(February 2019)

© Copyright 2019 Antaira Technologies, LLC.

Trademark Information

Antaira is a registered trademark of Antaira Technologies, LLC., Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Antaira Technologies, LLC. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC. will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

Table of Contents

FCC Notice

This equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

CE Mark Warning

This is a Class-A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Industrial Ethernet Wireless APs

Software User Manual

This manual supports the following models:

- AMS-2111(-T)
- AMS-7131-AC(-T)

This manual supports the following software version:

Release: Antaira v3.04

Please check our website (www.antaira.com) for any updated manual or contact us by e-mail (support@antaira.com).

1. Access with Web Browser
1.1. Web GUI Login

All of Antaira's industrial managed devices are embedded with HTML web GUI interfaces. They provide user-friendly management features through its design and allows users to manage the devices from anywhere on the network through a web browser.

Step 1: To access the WEB GUI, open a web browser and type the following IP address: http://192.168.1.1

Step 2: The default WEB GUI login:

Username: root

Password: password
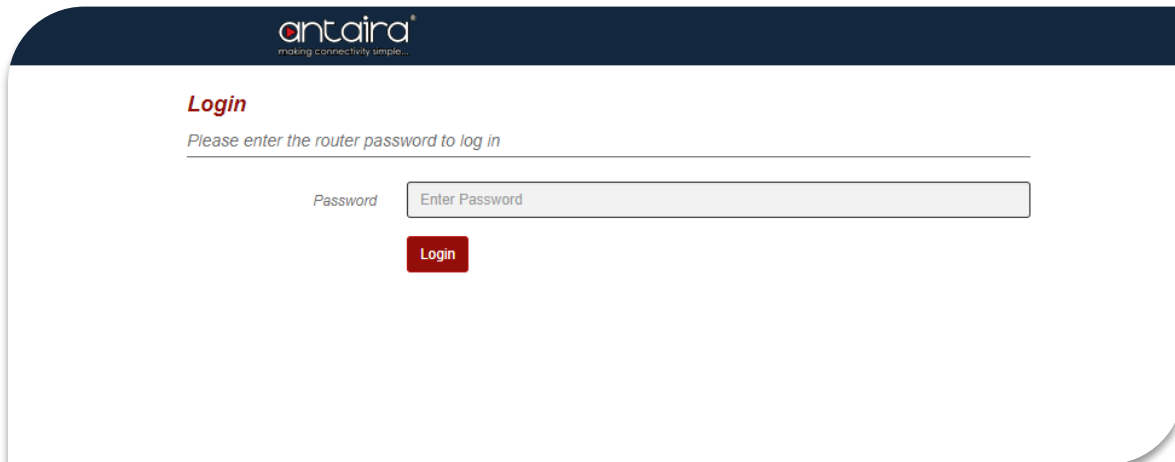
1.2.　　Operation Modes
1.2.1.　　Access Point

The access point mode allows Wi-Fi devices to connect to a wired network. In this mode, multiple wireless devices can be supported on a single wired local area network. In the example below, Internet is provided via the Modem/Router. The Access Point is connected directly to the Modem/Router by an Ethernet cable. Multiple devices can then connect to the access point's Wi-Fi and access the Internet.
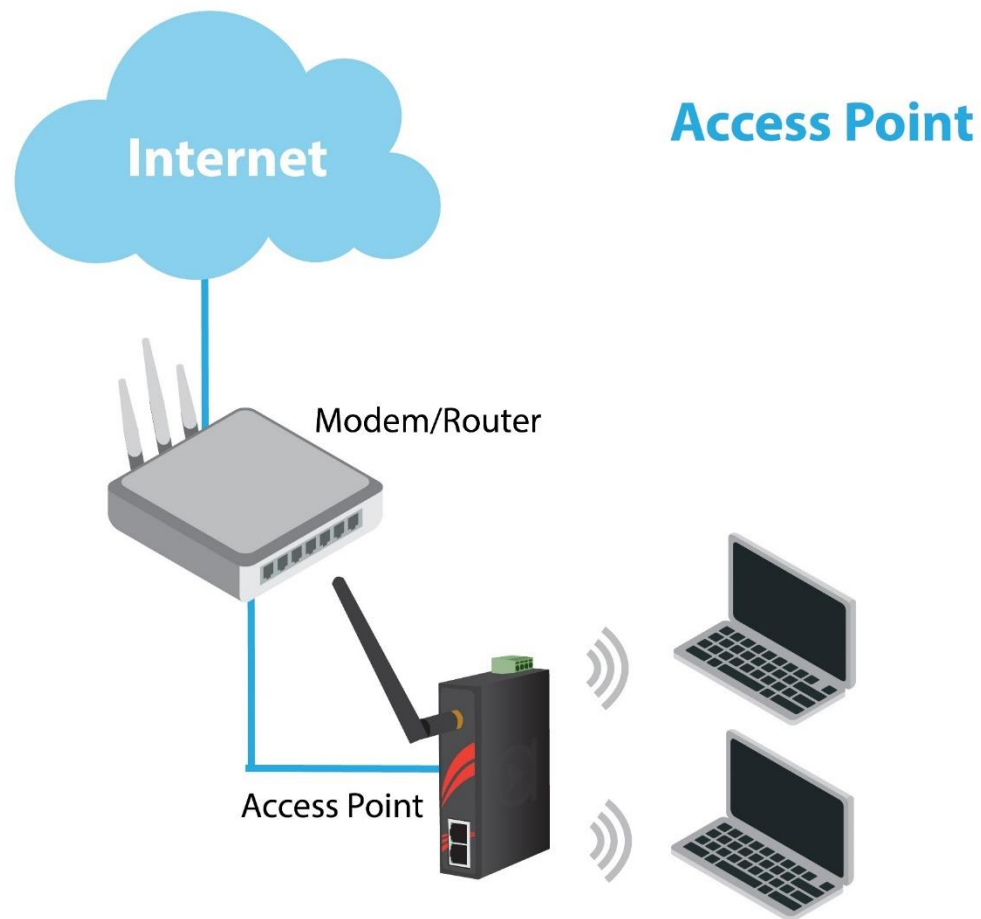
1.2.2. WDS Station

In a typical Access Point to Station/Client connection, whenever traffic is passed through the AP, the MAC address of the client packet changes to the MAC address of the AP. This can add overhead and latency. A Wireless Distribution System (WDS) allows one or more access points to connect wirelessly and share internet access across. WDS also preserves the MAC addresses of client frames across links between the WDS AP to WDS Stations, reducing the latency caused in typical wireless setups. WDS Stations can only be paired with WDS AP.
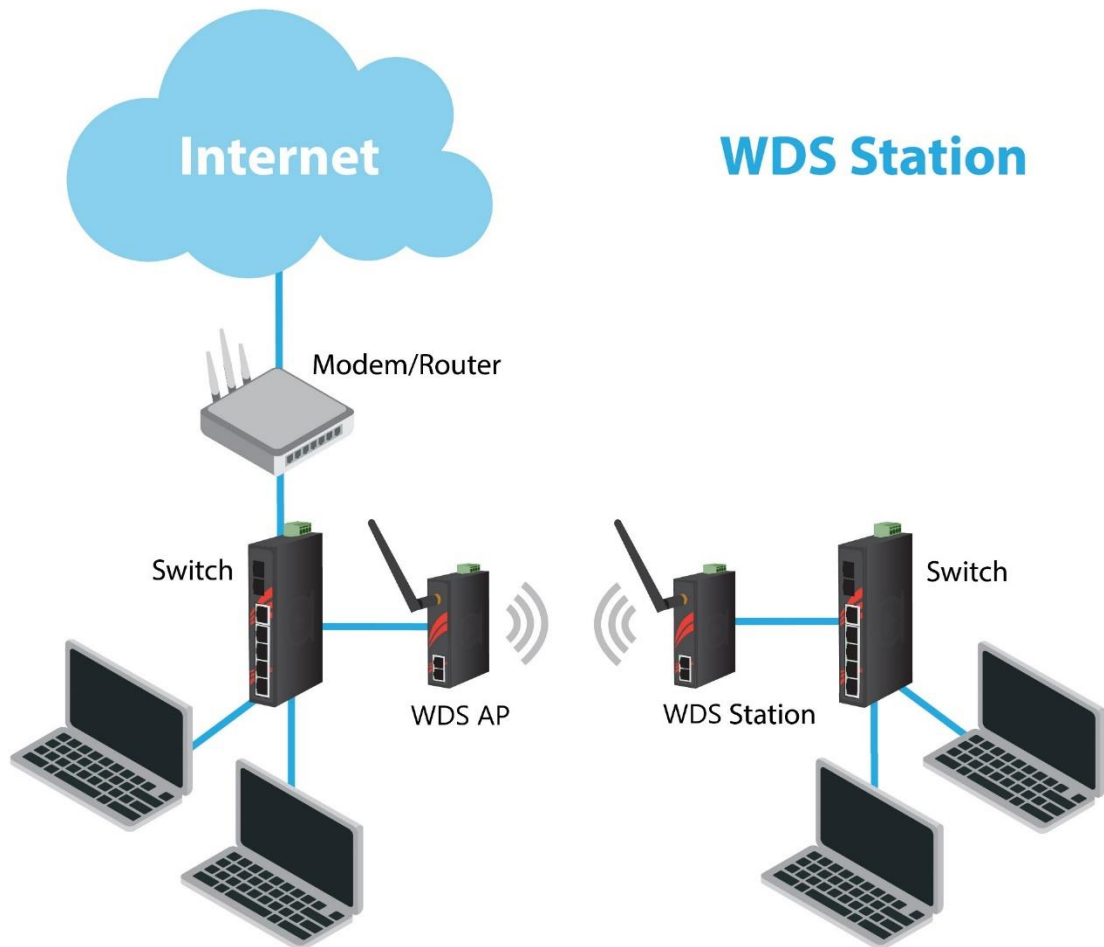
1.2.3.   Transparent Bridge

Transparent Bridge is similar to WDS Station mode, except it does not have to be paired to a WDS AP. Using Transparent Bridge Mode allows the Wi-Fi client device to receive IP addresses from a DHCP server.
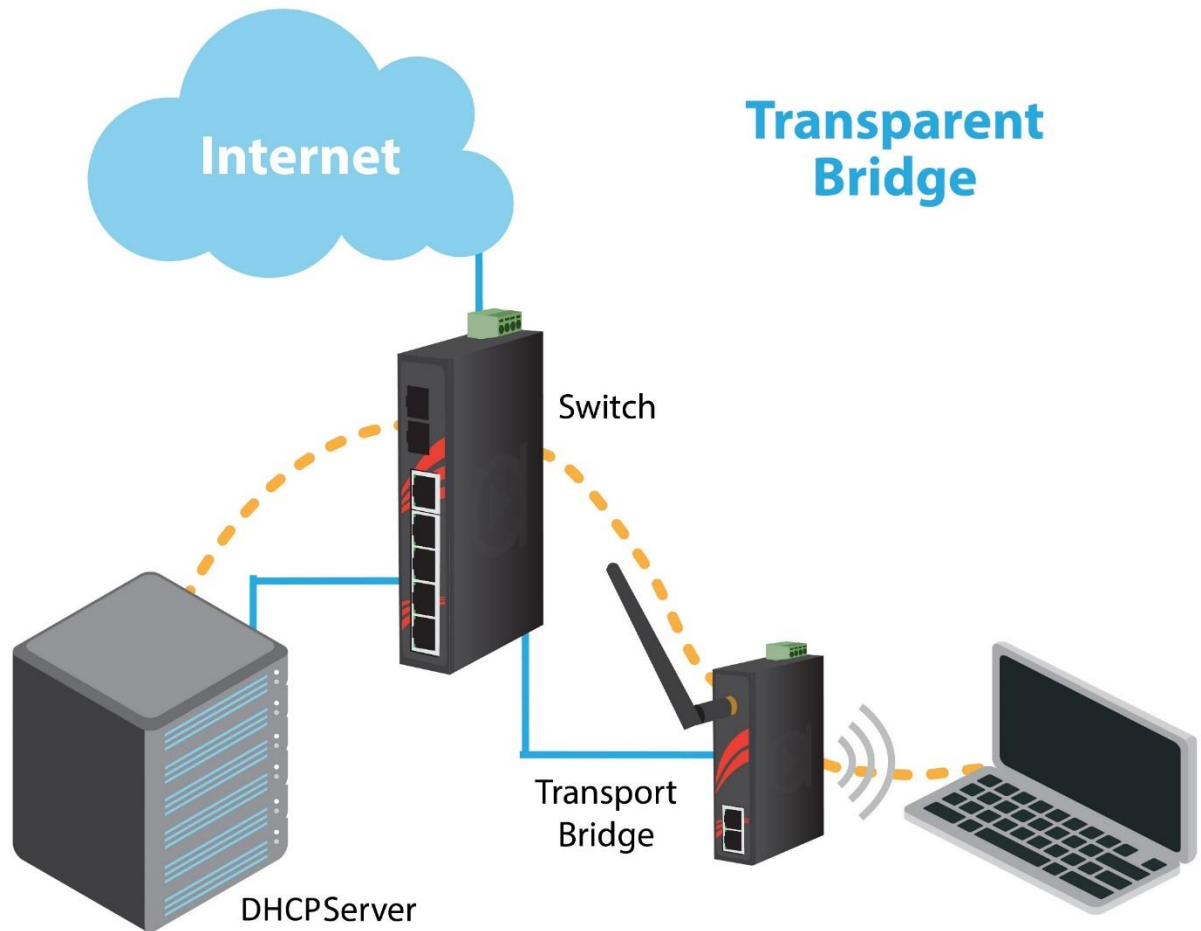
1.2.4.   Repeater Mode

In Repeater Mode, the access point will act as a relay for another wireless signal. Repeater Mode takes an existing signal from a wireless AP or wireless router and rebroadcasts it. This mode is beneficial for extending the wireless range and coverage. The drawback is that the re-transmitted signal throughput is halved for every repeater used.
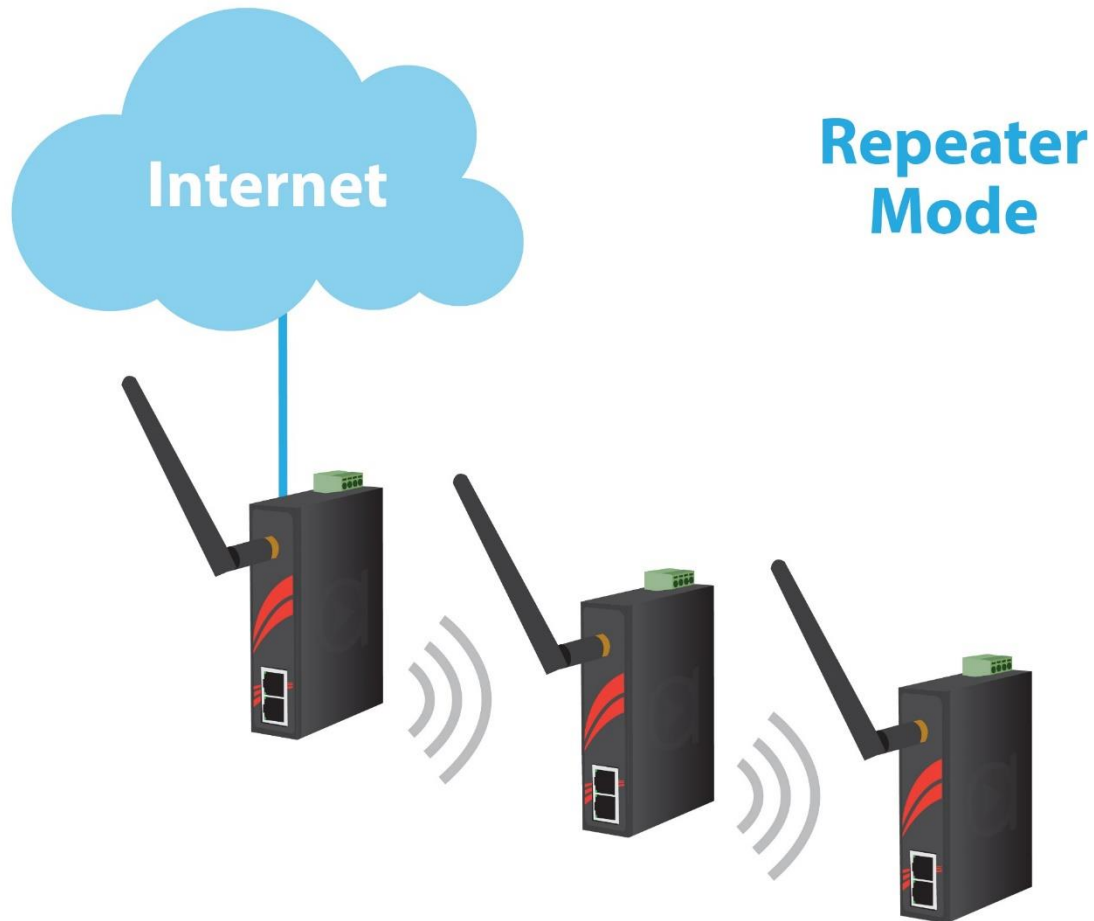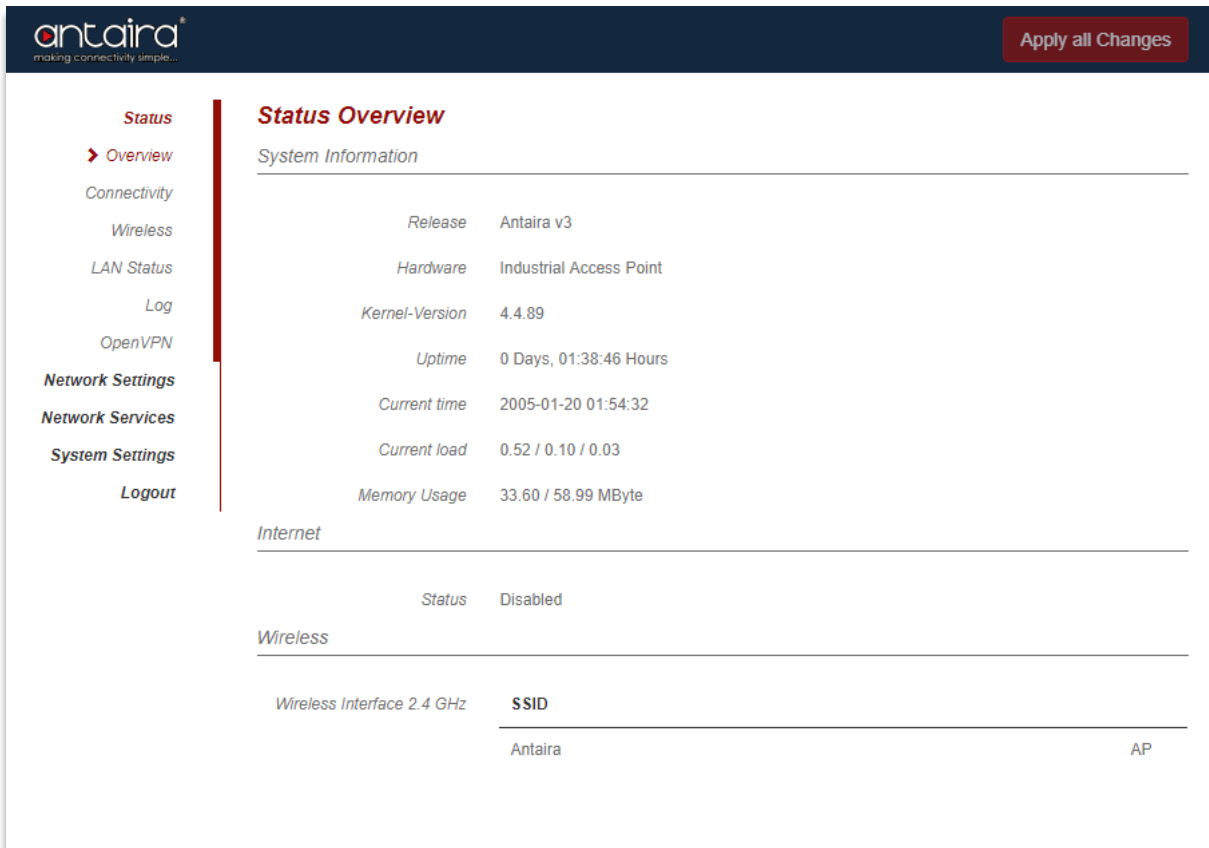
2. Status

2.1. Overview

When logged into the Web GUI Interface, the Overview page provides information of the current Access Point.

Status > Overview

Item	Description
Release	Displays current firmware.
Hardware	Displays description of access point.
Kernel-Version	Displays current kernel-version.
Uptime	Displays current uptime.
Current Time	Displays current time.
Current Load	Displays current load.
Memory Usage	Displays current memory usage.

2.2.   Connectivity

Status > Connectivity

Item	Description
Connection Type	Displays current uplink information.

2.3. Wireless
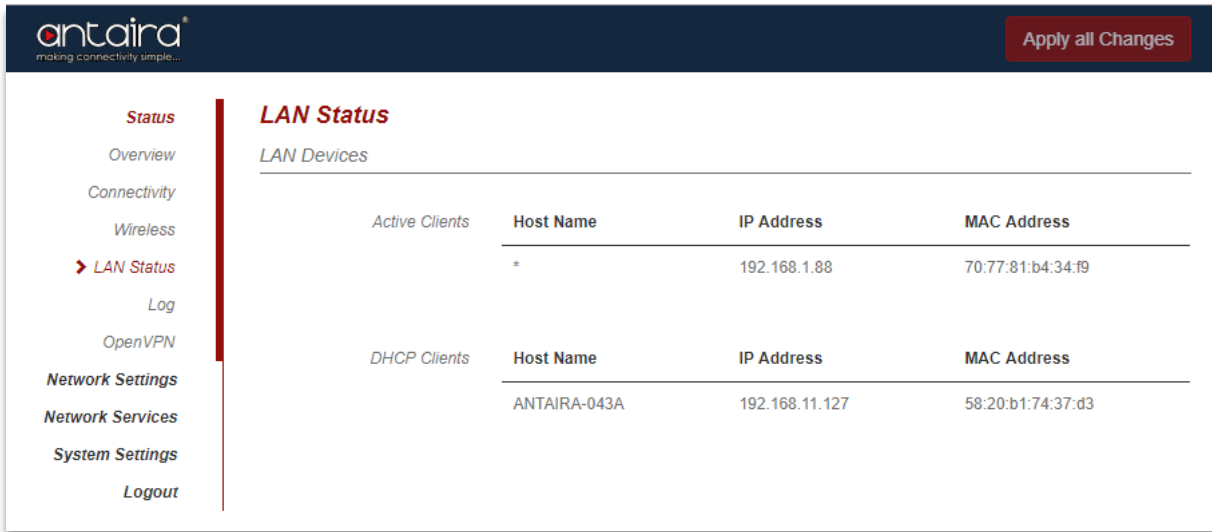
The wireless interface information is provided here.

Status > Wireless

Item	Description
Channel	Displays the Wireless Channel.
BSSID	Displays the Basic Service Set Identifier.
AP SSID	Displays the Access Points' Service Set Identifier.
Wireless-Clients	Displays wireless client's hostname, MAC Address, signal strength, and noise level.

2.4. LAN Status

The Local Area Network status information is provided here.

Status > LAN Status

Item	Description
Active Clients	Displays Active client's hostname, IP Address, and MAC Address.
DHCP Clients	Displays DHCP client's hostname, IP Address, and MAC Address.

2.5. Log

The Log page displays local log information.

Syslog Level

Indicates what type of message will be displayed in the System Log. Default is All.

Settings	Description
All	Displays all messages.
Emergency	Displays specific messages with severity level less than or equal to Emergency.
Alert	Displays specific messages with severity level less than or equal to Alert.
Critical	Displays specific messages with severity level less than or equal to Critical.
Error	Displays specific messages with severity level less than or equal to Error.
Warning	Displays specific messages with severity level less than or equal

	to Warning.
Notice	Displays specific messages with severity level less than or equal to Notice.
Info	Displays specific messages with severity level less than or equal to Informational.
Debug	Displays specific messages with severity level less than or equal to Debug.

Service

Filter logs by the Service name type.

Message

Filter logs by the Message.

2.6.   OpenVPN

The OpenVPN Information log page is provided here.
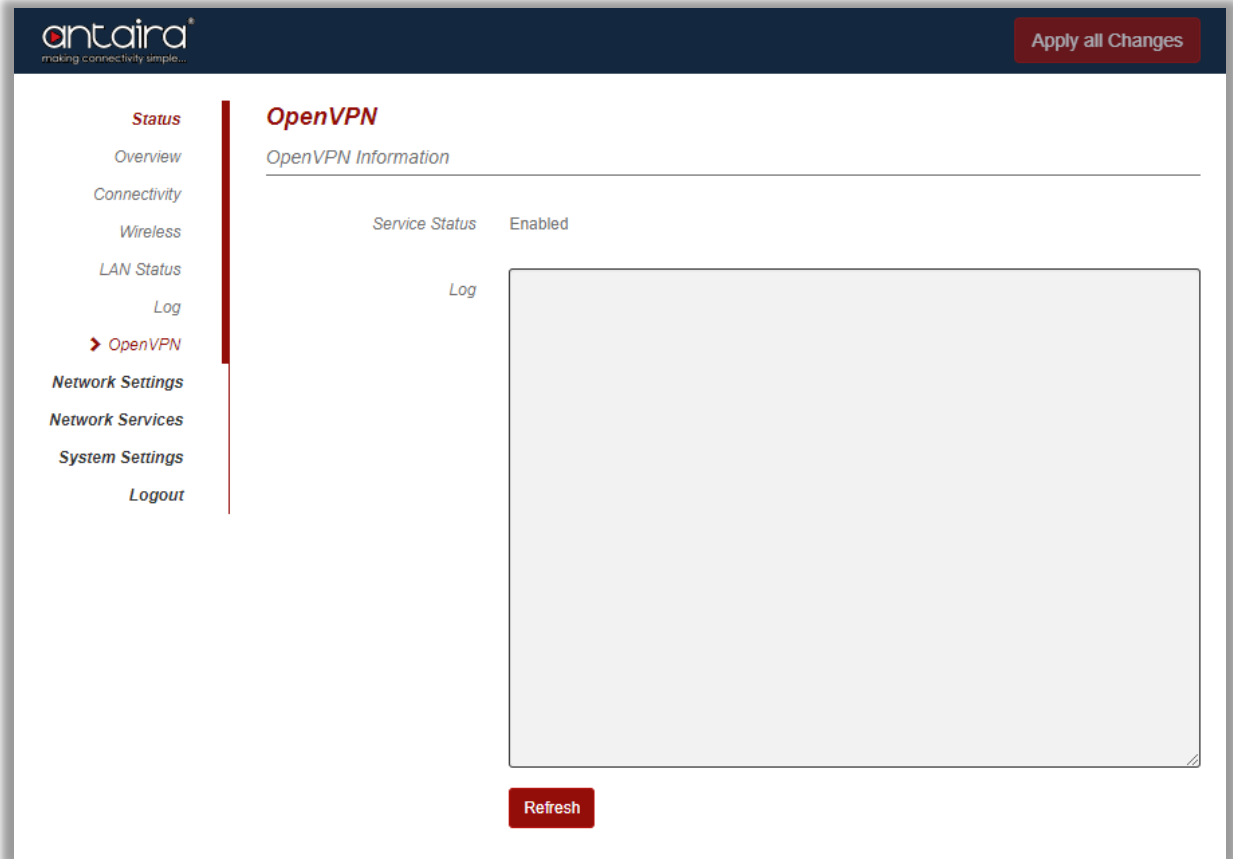
Status > OpenVPN

Item	Description
Service Status	Displays whether OpenVPN service is Enabled or Disabled.
Log	Displays log information about OpenVPN.

3. Network Settings
3.1. Connectivity

This page configures the Wide Area Network side of the Antaira Access Point.
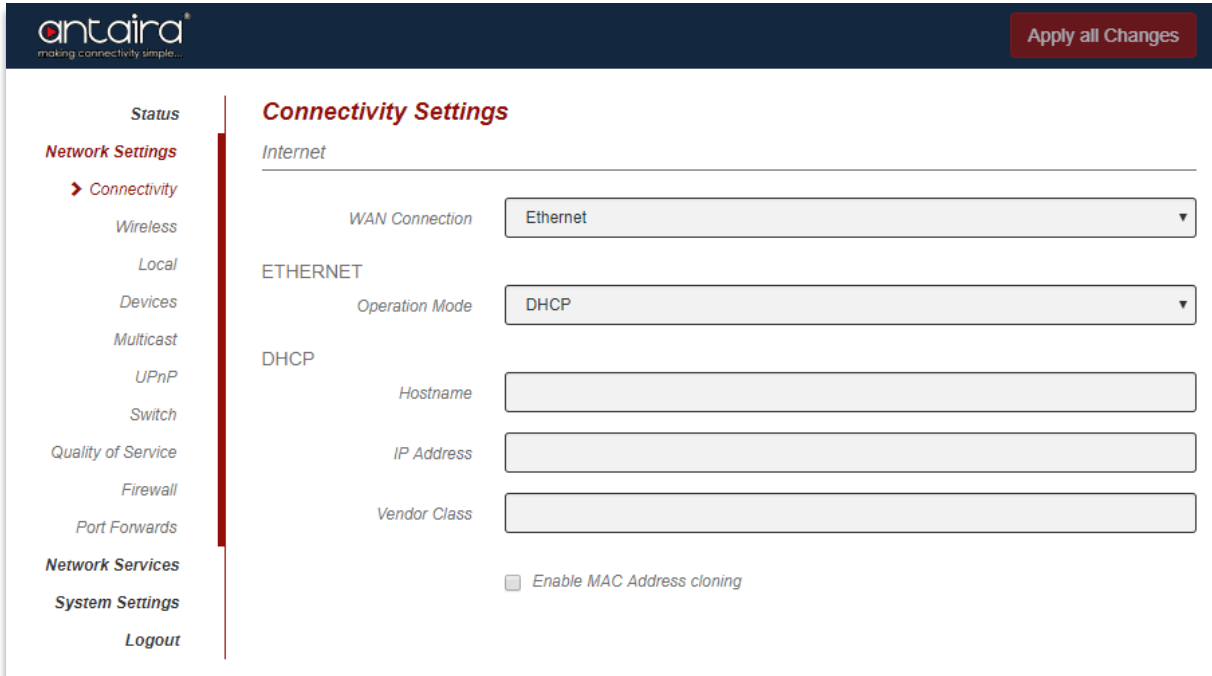
Network Settings > Connectivity

WAN Connection

Select an interface to be the Wide Area Network interface. The options are listed below:

Settings	Description
Disabled	Disables the WAN interface.
Ethernet	Uses the Ethernet port as the WAN interface.
USB	
Wireless	Uses WiFi for the WAN interface.

Operation Modes using Ethernet

Select the Operation Mode for the WAN when using the Ethernet port interface. The options are listed below:

Settings	Description
DHCP	The AP will obtain its WAN-side IP Address from a DHCP server.
Static	A static IP Address will be used.

PPPoE	Configure as a PPPoE-Cilent.
PPTP	Establishes a connection via PPTP.

Operation Modes using Wireless

Select the Operation Mode for the WAN when using the wireless interface. The options are listed below:

Settings	Description
NAT	The AP will obtain its WAN-side IP Address from a DHCP server.
Transparent Bridge	The Antaira Access Point will operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs.
WDS Station	Configure as a WDS Station.

3.2.   Wireless

This page configures the Wireless Interface of the Antaira Access Point. The SSID and Encryptions can be configured here.
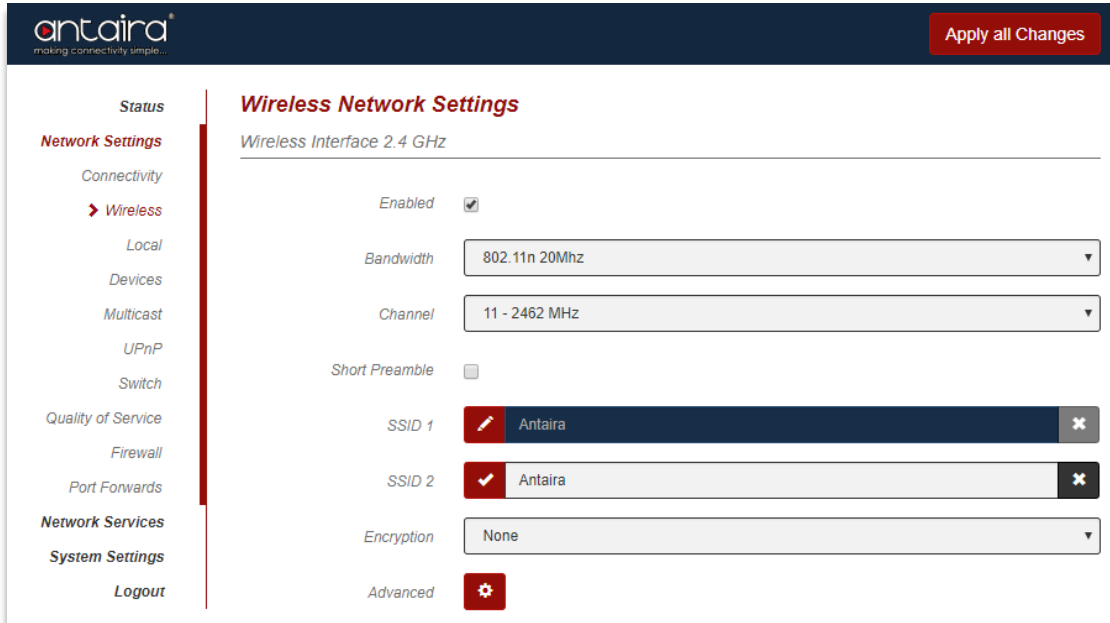
Network Settings > Wireless

Item	Description
Enabled	Enable/Disable the Wi-Fi interface.
Bandwidth	The channel bandwidth for the Wi-Fi instance. Supports 802.11n auto/20Mhz/40Mhz and 802.11g.
Channel	Select a desired channel or set to auto for automatic selection.
Short Preamble	Select to use a short preamble for Wi-Fi data transmission errors.
SSID #	The Service Set Identifier instance name.
Encryption	The Wi-Fi security setting. Supports no Encryption, WPA/WPA2, and Radius.
Passphrase	The WPA/WPA2 passphrase.
WPS	Wi-Fi Protected Setup pushbutton.
Advanced	Click the Advanced button to display more settings.
Bridge to	Bridge the Wi-Fi to the LAN, WAN, or GUEST_LAN.
WDS AP	Select to enable WDS AP Mode.
Hidden SSID	Select to hide the SSID from showing to clients.
Station Isolation	Enable Station Isolation on the Antaira Access Point.
Key Renew Interval	Enter a value in seconds for key renew interval. Leave empty for default.

simple

MAC Address Filter	Create a Whitelist (Allowed) or Blacklist (Denied) filter for MAC Addresses.

3.3.   Local

This page configures the Local Area Network side of the Antaira Access Point. The LAN can also be configured as a DHCP server.

Network Settings > Local

LAN Configuration

Configure the LAN IP Address and Net Mask.

Item	Description
IP Address/Net Mask	The LAN side IP Address and Net Mask setting.

DHCP Server

The LAN side of the Antaira Access Point can be configured as a DHCP Server.

Item	Description
Enable DHCP	Enable/Disable the DHCP Server option.
Client IP Range	Configure the client pool range of IP Addresses.
Max. Client Leases	Set the maximum amount of IP Addresses that can be leased.
Client Lease Time	Set the amount of time before a leased IP Address expires.
Gateway	Enter optional Gateway address to be pushed to the clients.

Additional DNS Servers

Add up to three DNS Servers. These DNS Servers can be used instead of the WAN DNS.

Item	Description
DNS Server #	Enter the DNS Server address here.
Ignore WAN DNS	Check this box to ignore using the WAN DNS.

3.4.   Devices

This page configures static bindings. IP Addresses can be statically mapped to Mac Addresses here.
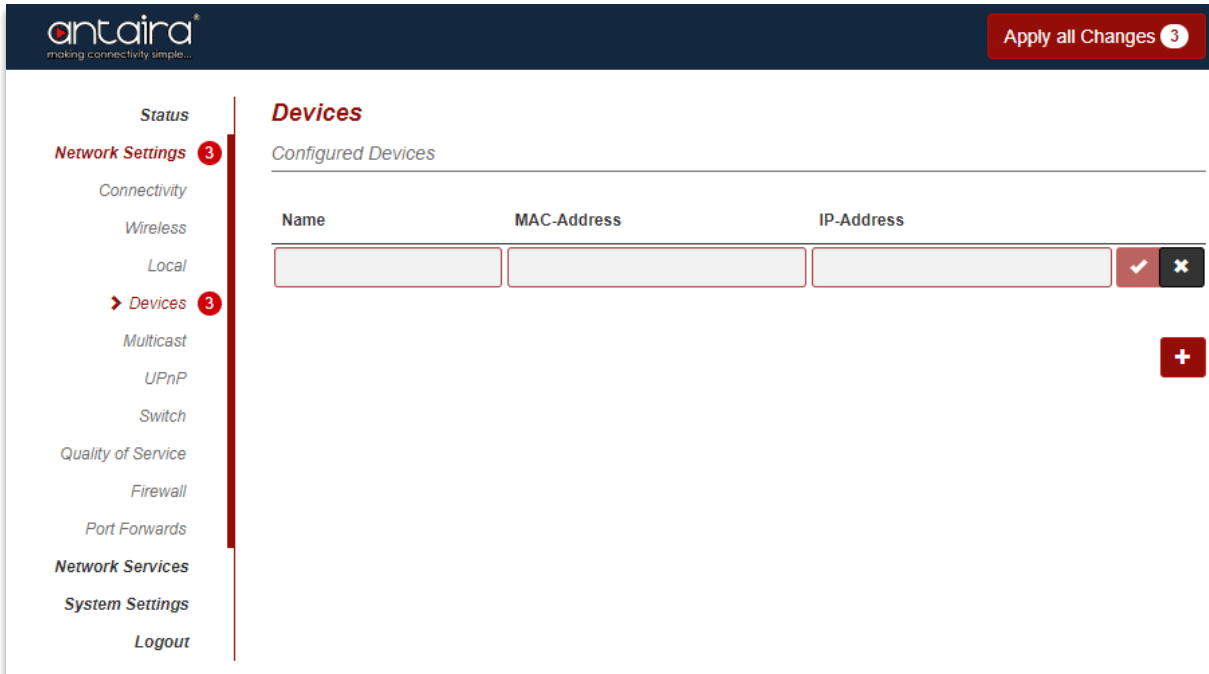
Network Settings > Devices

Item	Description
Name	Enter a name for the device.
MAC-Address	Enter the target MAC Address.
IP-Address	Enter an IP Address to statically bind.

3.5.   Multicast

Enable or Disable IGMP Proxy. Disabled by default.
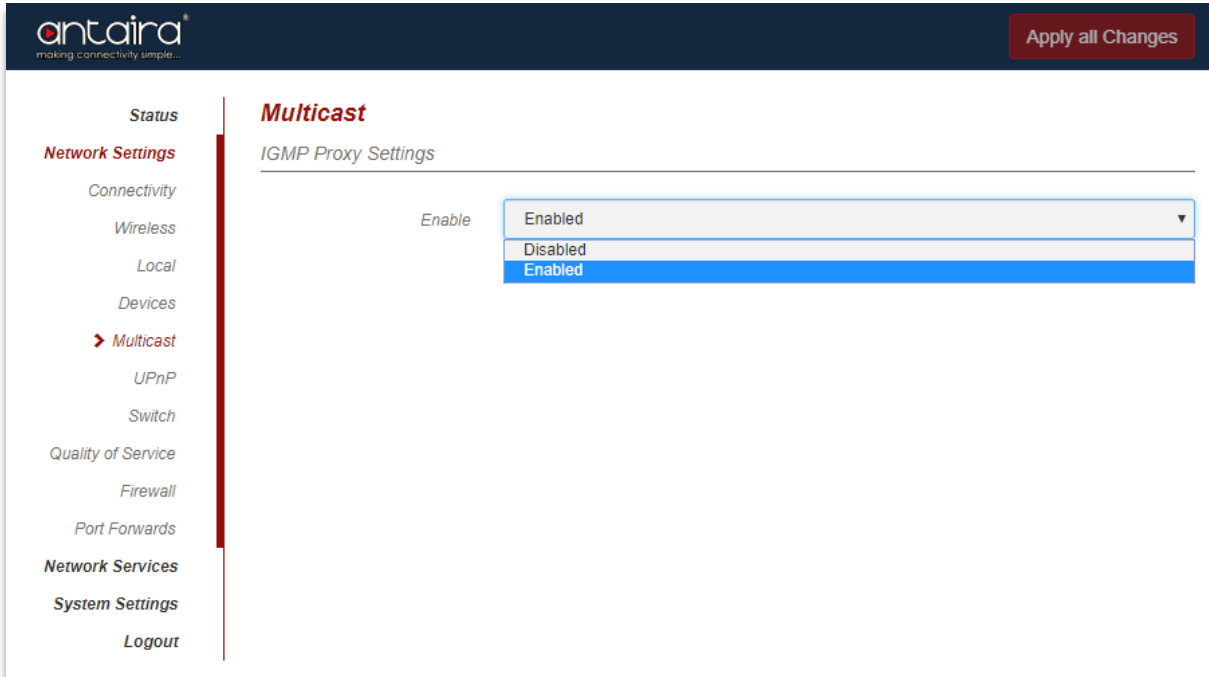
Network Settings > Multicast

3.6.   UPnP

Enable or Disable Universal Plug and Play. Disabled by default.
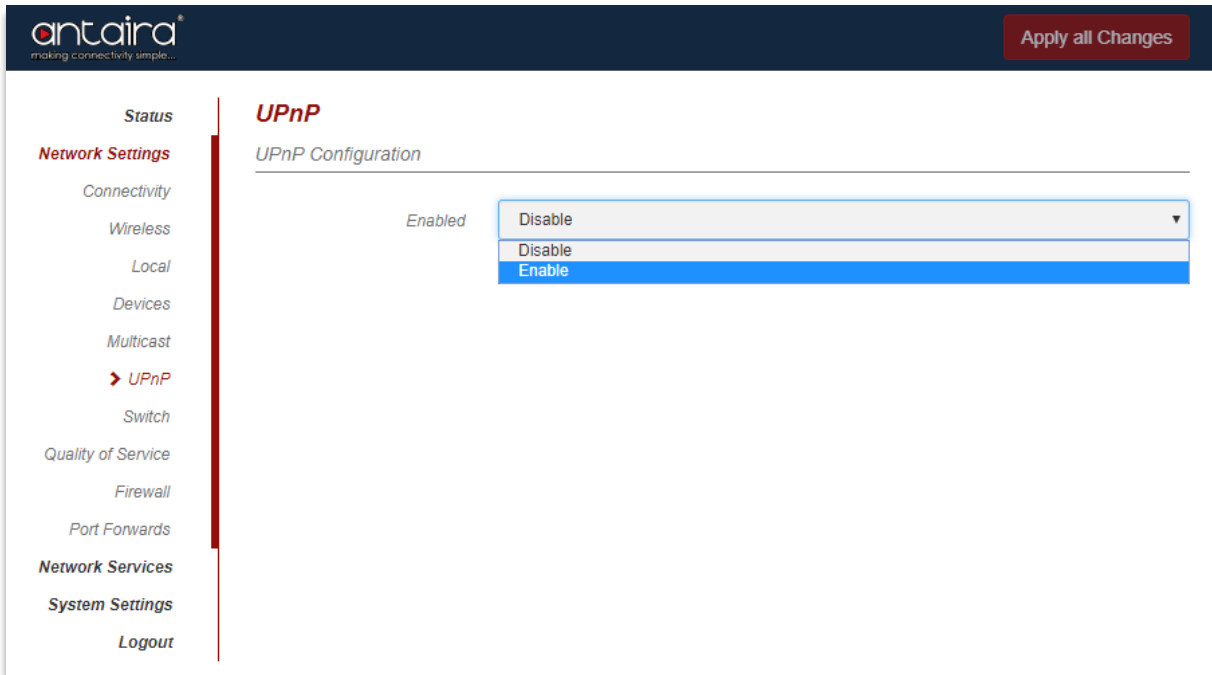
Network Settings > UPnP

3.7. Quality of Service

Enable or Disable QoS. Disabled by default.
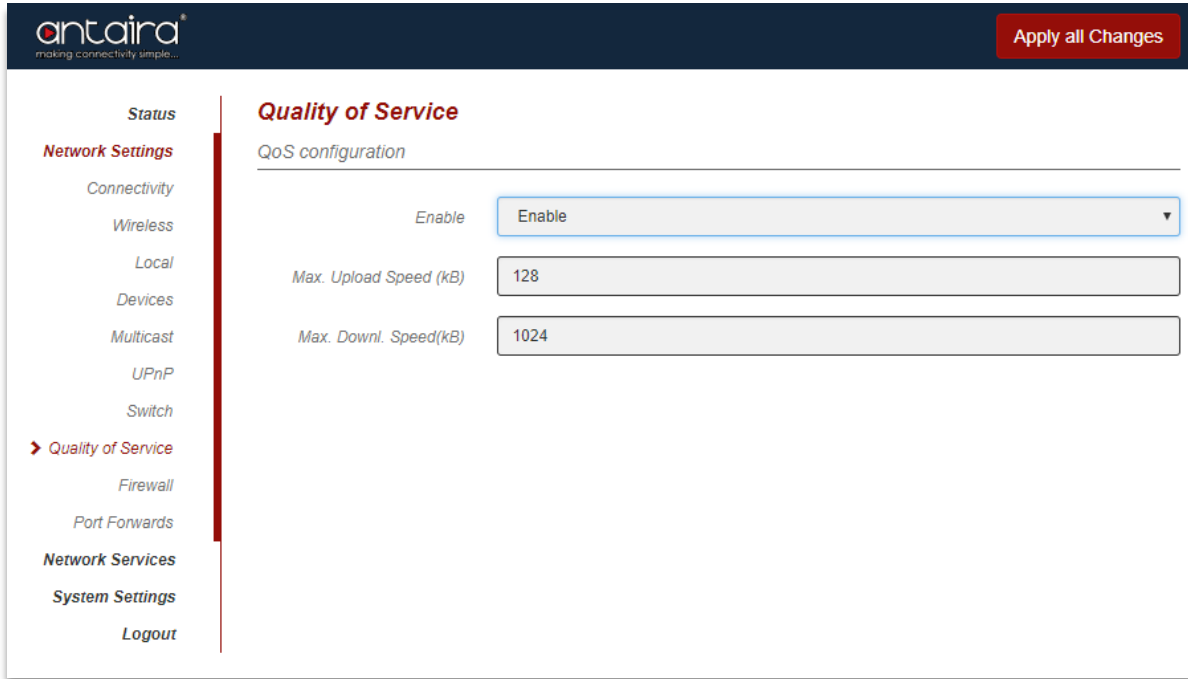
Network Settings > Quality of Service

Item	Description
Enable	Enable or Disable Quality of Service.
Max. Upload Speed (kB)	Enter the allowed maximum upload speed in kB.
Max. Downl. Speed (kB)	Enter the allowed maximum download speed in kB.

3.8. Firewall

This page configures Firewall services.
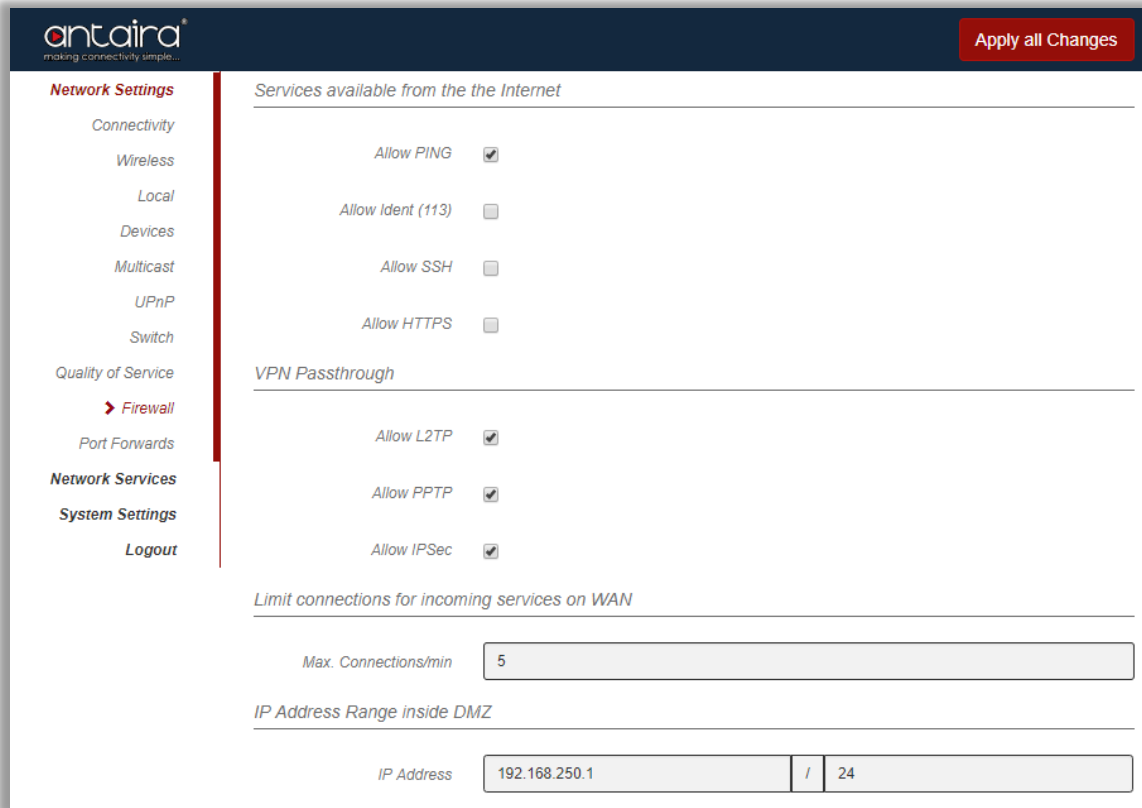
Network Settings > Quality of Service

Services available from the Internet

Allow or block certain protocols to the Antaira Access Point.

Item	Description
Allow PING	Allow or Deny PING transmission to the Antaira Access Point.
Allow Ident (113)	Allow or Deny Identification Protocol.
Allow SSH	Allow or Deny SSH connections to the Antaira Access Point.
Allow HTTPS	Allow or Deny HTTPS connections to the Antaira Access Point.
Allow L2TP	Allow or Deny L2TP VPN connections.
Allow PPTP	Allow or Deny PPTP VPN connections.
Allow IPSec	Allow or Deny IPSec VPN connections.
Max Connections/min	Limit the connections for incoming services on the WAN. Default is 5.
IP Address Range inside DMZ	Configure the IP Address range inside the DMZ.

3.9.   Port Forwards

Port Forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for a number of applications such as FTP servers, Web servers, e-mail servers, etc. Port Forwarding is also beneficial where different host systems need to be seen using a single common IP address/port.
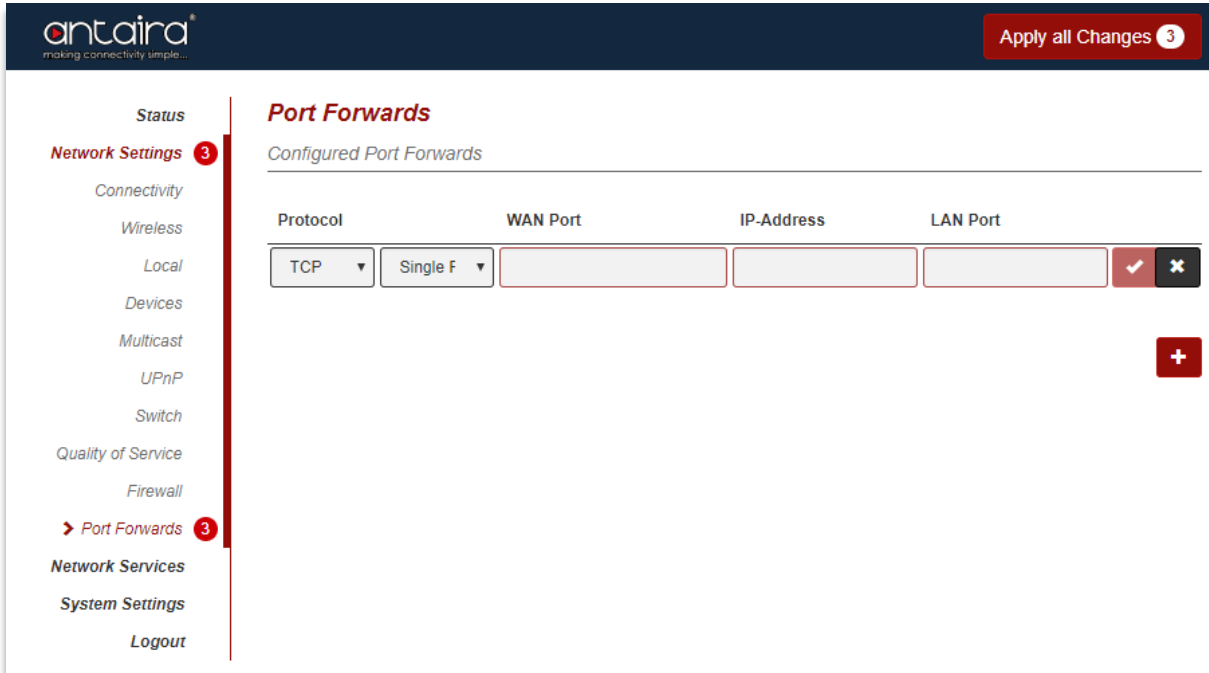
Network Settings > Port Forwards

Item	Description
Protocol	Select the protocol type that needs to be forwarded. Select between TCP, UDP, or both.
WAN Port(s)	Choose between a single port or a range of ports to be forwarded.
IP-Address	
LAN Port	Enter the LAN source port.

4. Network Services

4.1. Router

Item	Description
Hostname	Enter a hostname.
Domain	Enter a domain name.

4.2.   SSH

Enable or Disable SSH. The root password can also be configured here.

Network Services > Router

Item	Description
SSH Server	Enable or Disable SSH.
SSH Port	Configure a custom port number for SSH connections. Default is port 22.
Set the root password	Configure a new password for root login. Default is **password**

4.3.   Dynamic DNS

Enable or Disable Dynamic DNS. Disabled by default.

Network Services > Dynamic DNS

Item	Description
Enable	Enable or Disable Dynamic DNS.
Service	Select a pre-defined service or create a custom one.
Username	Enter a username.
Password	Enter a password.
Domain	Enter a domain name.
Update URL	Enter an updated URL.
Check IP at	Select either WAN or Internet.
Verify (Minutes)	Enter value in minutes.
Refresh	Enter value in hours.

4.4. PPTP Server

Enable or Disable Point-to-Point Tunneling Protocol.

Network Services > Dynamic DNS

Item	Description
Enable	Enable or Disable PPTP Server
Server IP Address	Enter the server's IP address.
Client IP Addresses	Enter a range of the client IP addresses.
PPTP Users	Enter a username and password.

4.5.   OpenVPN
4.5.1.   OpenVPN Configuration

Network Services > OpenVPN

Item	Description
OpenVPN	Enable or Disable OpenVPN services.
Operation Mode	Choose between Server, Client, or upload a custom configuration file.
Device Mode	Choose between TUN (Network Tunnel) or TAP (Network TAP).
Network Protocol	Choose between using UDP or TCP to establish VPN connections. Default is UDP.
Remote Server	When Operation Mode is set to **Client,** enter the Remote Server address here.
Port	Specify the OpenVPN connection port. Default is 1194.
User Authentication	Enable or Disable User Authentication.
Username	Enter the username to authenticate to the Remote Server.
Password	Enter the password to authenticate to the Remote Server.
Masquerade Traffic	

4.5.2.   OpenVPN Certificates
Network Services > OpenVPN

Item	Description
CA (ca.crt)	Enter CA Certificate here.
KEY (client .key)	Enter Client Key here.
CERT (client .crt)	Enter Client Certificate here.
TLS (ta.key)	Enter TA
DH (dh.pem)	

4.6.   WiFi Schedule

This page configures the operating times for the WiFi function on the Antaira Access Point.

Network Services > WiFi Schedule

Item	Description
Operating Times	

4.7.   Access Control

This page allows users to specify a time-frame of accessibility to the Antaira Access Point based on MAC Addresses.

Network Services > Access Control

Item	Description
Client MAC Address #	Enter a client MAC Address.
Access Schedule	Select

4.8. Wake on LAN

This page configures the Wake on LAN (WoL) for particular devices.

Network Services > Wake on LAN

Item	Description
Device Name	Enter a Device Name.
MAC Address	Enter the target MAC Address.
Password	Enter the target password.
Wake on Boot	Enable or Disable Wake on Boot.

5. System Settings

5.1. Localization

This page configures the Language and Time Zone for the Antaira Access Point.
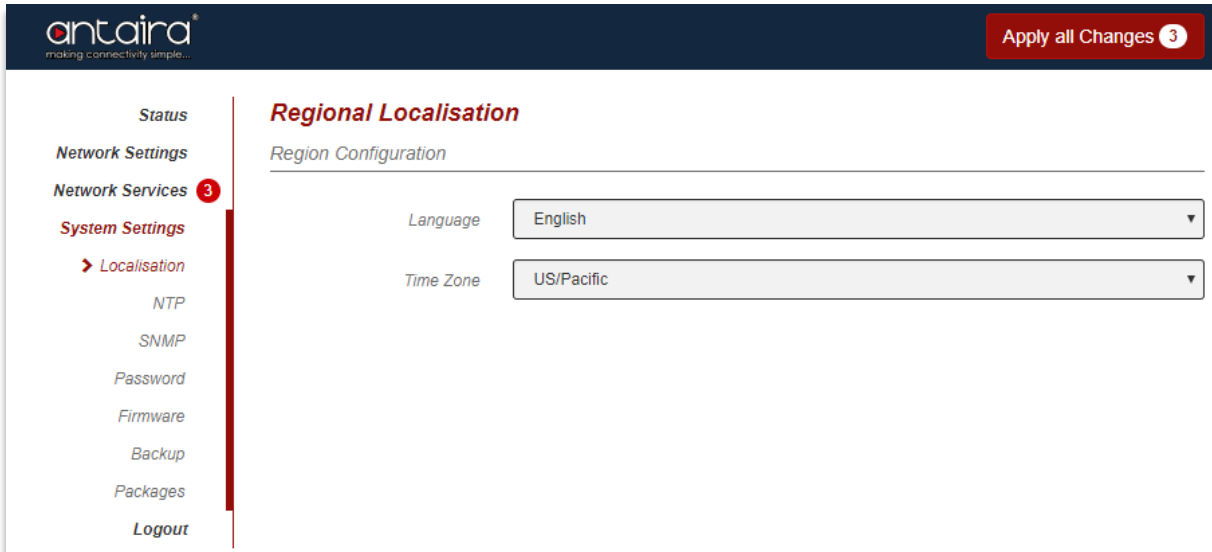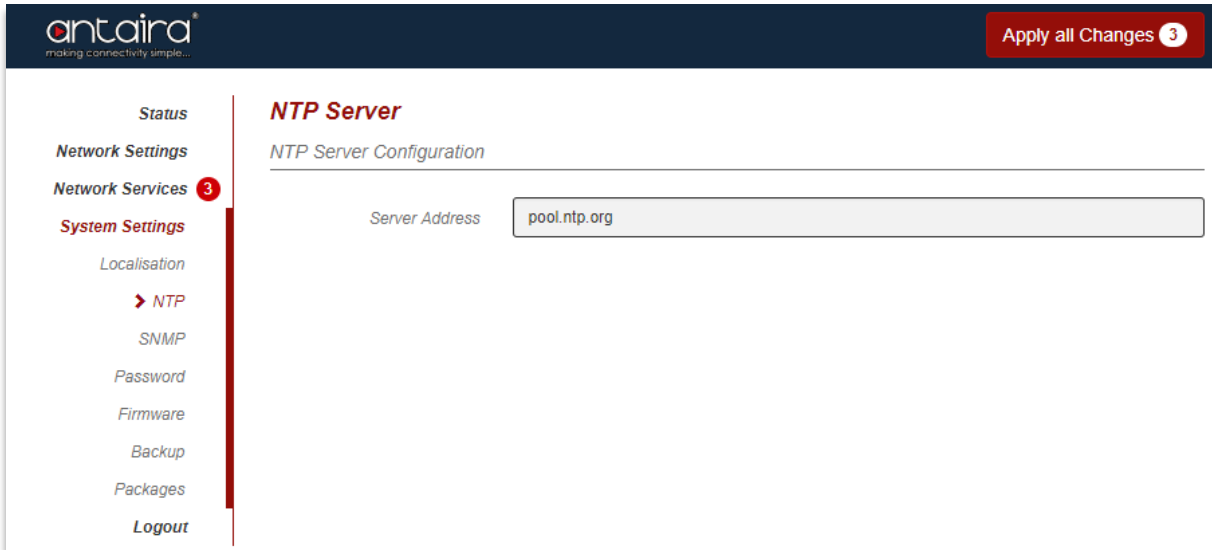

System Settings > Localization

Item	Description
Language	From the drop-down menu, choose the desired language.
Time Zone	From the drop-down menu, choose the desired time-zone.

5.2.   NTP

This page configures the Network Time Protocol Server.

System Settings > NTP

Item	Description
Server Address	Enter the name or IP Address of an NTP Server.

5.3.   SNMP

This page configures the Simple Network Management Protocol.

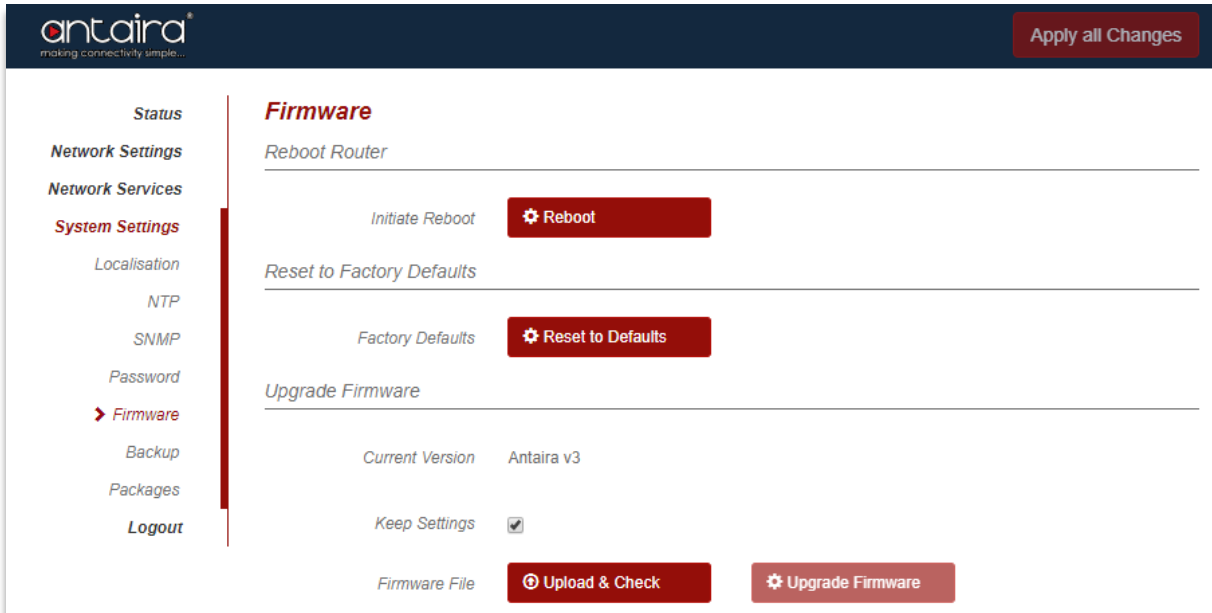| Item	Description
Access from WAN	Enable/Disable SNMP access from the WAN interface.
Access from LAN	Enable/Disable SNMP access from the LAN interface.
Device Location	Enter a device location.
Device Administrator	Enter an administrator email to receive SNMP alerts.
Device Name	Enter a device name.

5.4. Password

This page allows you to change the default Web User Interface password and session timeout.

System Settings > Password

Item	Description
Current Password	Click the lock icon to change the current password.
New Password	Enter a new password.
Re-Type Password	Re-enter the new password to confirm.
Timeout (Minutes)	Configure the session timeout in minutes. Default is 5 minutes.

5.5.   Firmware

The Antaira Access Point's firmware can be upgraded here. The device can also be rebooted and set to factory default settings.

System Settings > Firmware

Item	Description
Initiate Reboot	Reboots the Antaira Access Point.
Factory Defaults	Resets the Antaira Access Point to factory default settings.
Current Version	Displays the current firmware version.
Keep Settings	Choose to keep current settings when upgrading the firmware.
Firmware File	Click **Upload & Check** to load a new firmware. Click **Upgrade Firmware** to upgrade.

5.6.   Backup

Configurations can be downloaded as a backup file for later use or restoration. Restoring from a backup is also configured here.

Item	Description
Backup File: Download	Download configurations and all configuration files into a .tar.gz file.
Backup File: Select Config File	Select the configuration file to restore to.
Restore	Restore to the configuration file selected.

5.7.   Packages
5.7.1.   Installed Packages
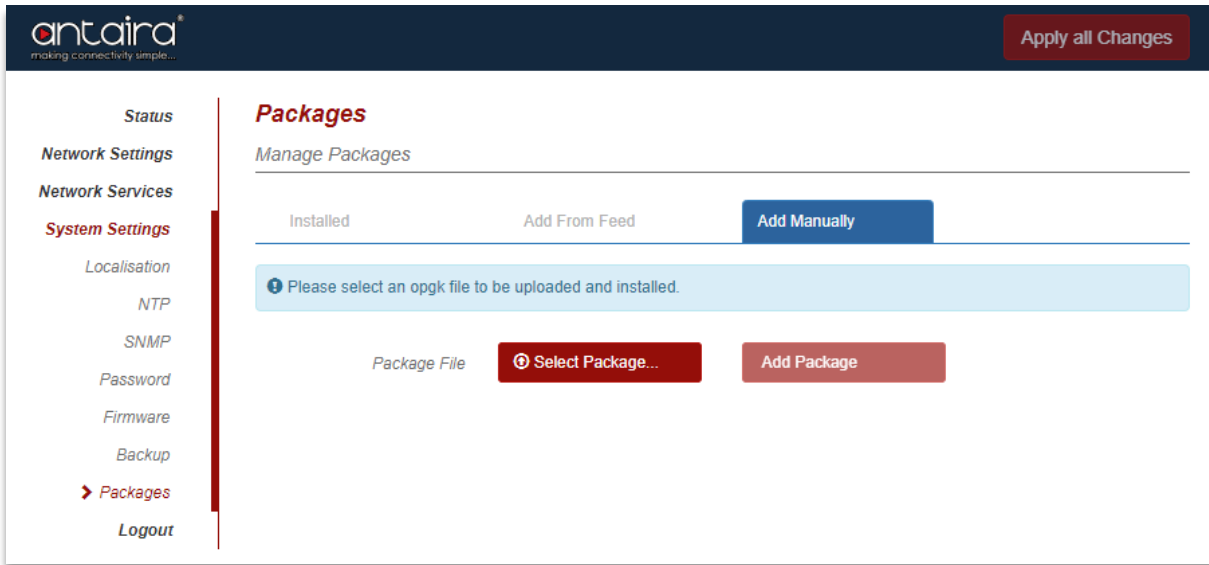

System Settings > Packages > Installed

Item	Description
Installed	

5.7.2.   Add from Feed
System Settings > Packages > Add From Feed

Item	Description
Add from Feed	

5.7.3. Add Manually

System Settings > Packages > Add Manually

Item	Description
Select Package	
Add Package	

5.8.   Logout

Click the Logout button to logout of the Antaira Access Point.