Table of Contents

Araknis X20 Series Access Points

Wi-Fi 6 Access Point User Manual

This manual details the web user interface and configuration of Araknis X20 series access points (APs)

First time setup tips

- This AP requires 802.3at (30W) PoE. Do not use 802.3af (15W) or a passive PoE injector as 15W is only enough to power the device, connect to OvrC, and broadcast an SSID with minimal throughput.
- For jobs with multiple APs, consider using OvrC to configure the SSIDs for all APs at once. See **Getting Started With OvrC Wi-Fi Management** for more information.
- All Araknis access points transmit the same default SSID, **araknis_initial**. If multiple access points are being installed in the same network, without using OvrC for SSID setup, power on and configure one AP at a time to avoid confusion about which access point you are connecting to.
- Araknis Networks recommends the use of MAC reservations, instead of static IP addresses.
- You must change the login credentials during initial setup.

Connecting to the AP

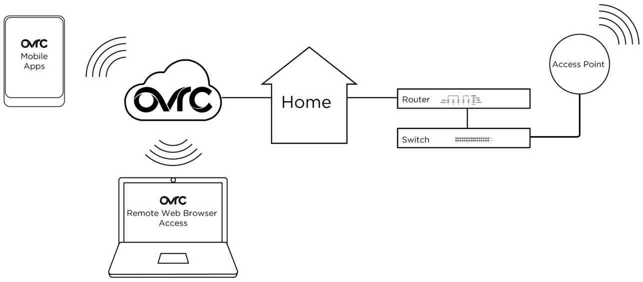
Araknis APs can be configured through OvrC or the local interface. The local interface is accessible using OvrC's webconnect feature, typing the AP's DHCP address into your browser's address bar, or using the AP's default IP address.

Configuring the AP in OvrC

OvrC provides Wi-Fi management, remote device management, real-time notifications, and intuitive customer management, using your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

To add this device to your OvrC account:

1. Connect the AP to the internet
2. Log into OvrC (**www.ovrc.com**)
3. Scan the site using an OvrC Pro device, or add the AP manually by entering the MAC address and Service Tag.
4. **Click here** for our article on *Getting Started With OvrC Wi-Fi Management*.

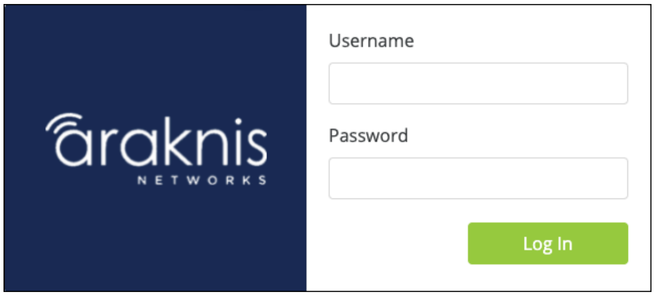


Logging into the Web Interface

1. Log into the AP using the default credentials:

Username	araknis
Password	araknis

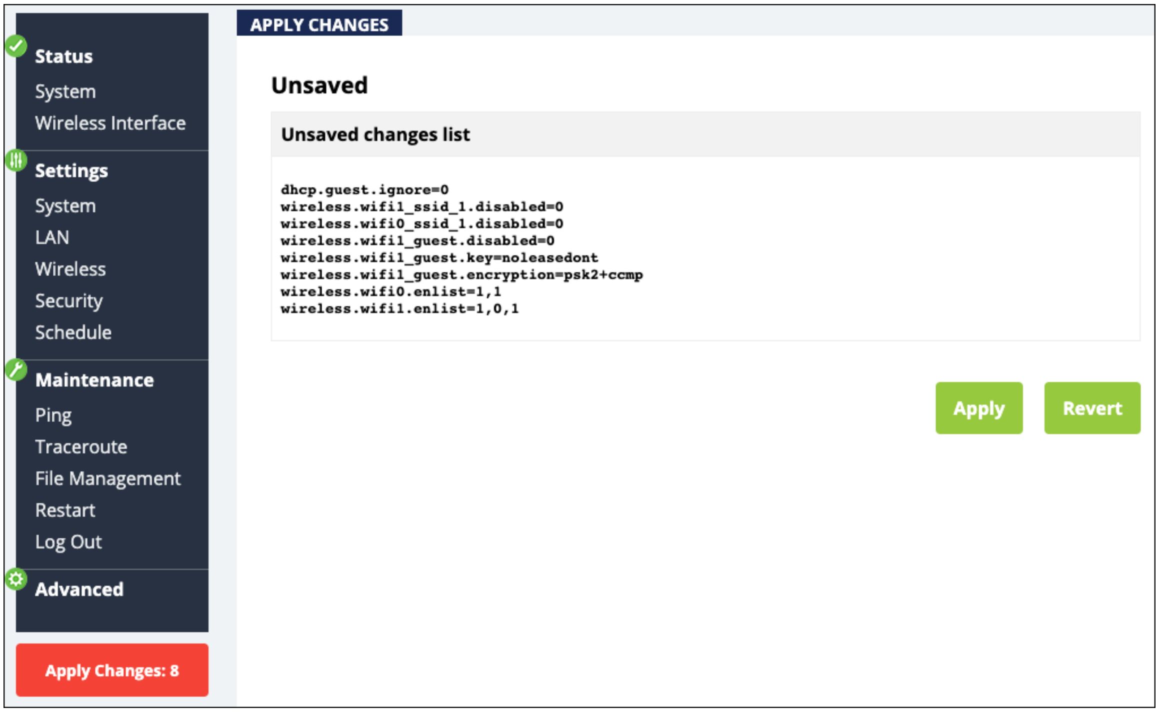
2. You must update the password after initial login.



Pro Tip: Strong passwords are long and unrelated to the client's public details. For example, thepepperonipizzas is stronger and easier to remember than P@ssword or thesmiths.

Saving and Applying Changes

1. Click the **Save** button after applying changes to a page. This holds the new settings in the Apply Changes field.
2. After all desired changes have been made, click the flashing **Apply Changes** button, at the bottom of the left menu, to review the new settings. Click **Apply** to make the changes or **Revert** to cancel the changes.



Unsaved

Unsaved changes list

```
dhcp.guest.ignore=0
wireless.wifi1_ssid_1.disabled=0
wireless.wifi0_ssid_1.disabled=0
wireless.wifi1_guest.disabled=0
wireless.wifi1_guest.key=noleasedont
wireless.wifi1_guest.encryption=psk2+ccmp
wireless.wifi0.enlist=1,1
wireless.wifi1.enlist=1,0,1
```

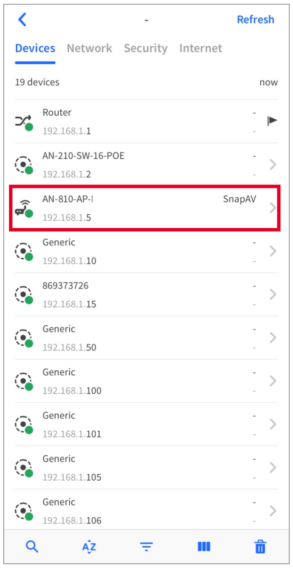
Note: Settings take effect after the progress bar reaches 100%.

Other Access Methods: DHCP IP Address

The WAP is configured to DHCP by default so that the DHCP server can assign an IP address when the AP is connected to the network (the DHCP server is usually the router). This address can be used for accessing the web interface.

Use one of these methods to find the IP address of the AP:

- Check the device list in OvrC.
- Check the client table on your router.
- Use a network scanner (e.g. Fing) to scan the network. The Araknis WAP manufacturer field displays SnapAV.
- See the highlighted field in the Fing screenshot to the right for an example of an Araknis device being identified.



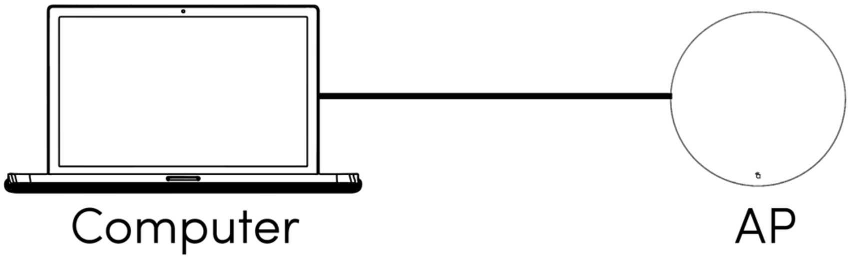
19 devices — now

Router 192.168.1.1	-	
AN-210-SW-16-POE 192.168.1.2	-	
AN-810-AP-I 192.168.1.5	SnapAV	
Generic 192.168.1.10	-	
869373726 192.168.1.15	-	
Generic 192.168.1.50	-	
Generic 192.168.1.100	-	
Generic 192.168.1.101	-	
Generic 192.168.1.105	-	
Generic 192.168.1.106	-	

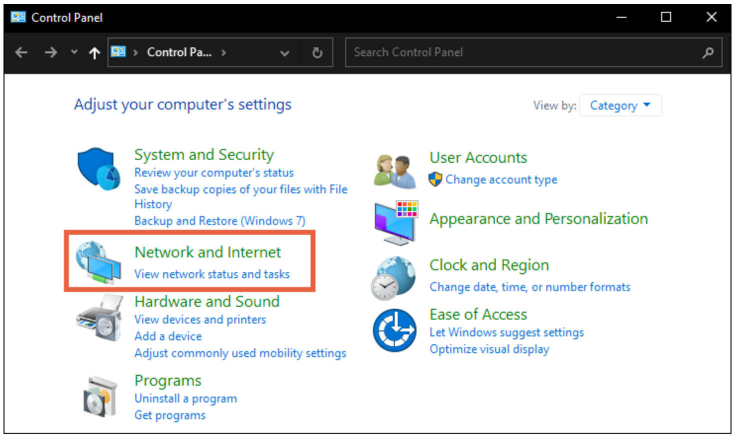
Accessing the AP Using the Default IP Address

If the AP is not given a DHCP address, or needs to be accessed while not connected to a network, you can configure your computer's network connection to access the AP using the default IP address, **192.168.20.253**.

Step 1: Connect your PC to the AP using an Ethernet cable.



Step 2: Open the Control Panel and click Network and Internet.



Control Panel

Control Pa... › Search Control Panel

Adjust your computer's settings

View by: Category ▾

System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)

Network and Internet
View network status and tasks

Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings

Programs
Uninstall a program
Get programs

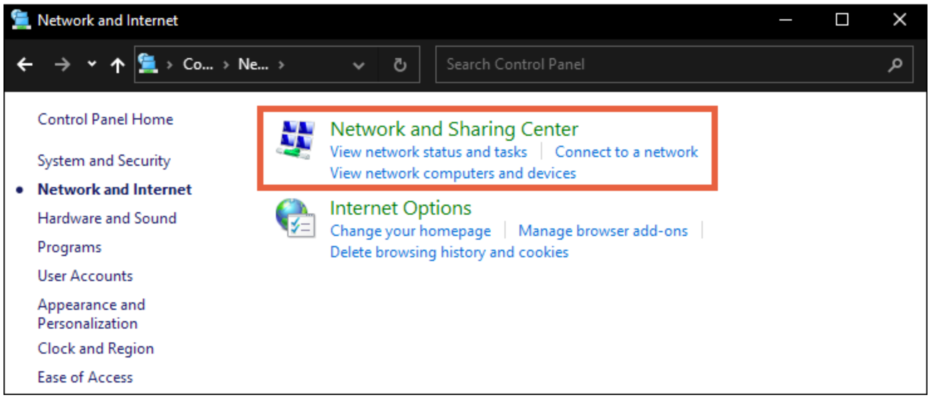
User Accounts
Change account type

Appearance and Personalization

Clock and Region
Change date, time, or number formats

Ease of Access
Let Windows suggest settings
Optimize visual display

Step 3: Click Network and Sharing Center.



Network and Internet

Co... › Ne... › Search Control Panel

Control Panel Home

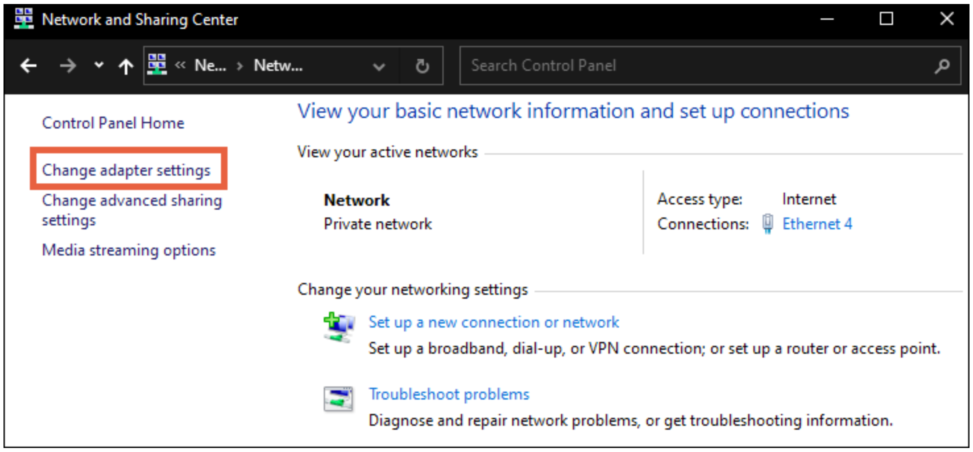
System and Security
- **Network and Internet**

Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access

Network and Sharing Center
View network status and tasks | Connect to a network
View network computers and devices

Internet Options
Change your homepage | Manage browser add-ons |
Delete browsing history and cookies

Step 4: Click Change adapter settings.



Network and Sharing Center

« Ne... › Netw... Search Control Panel

Control Panel Home

Change adapter settings
Change advanced sharing settings
Media streaming options

View your basic network information and set up connections

View your active networks

Network
Private network

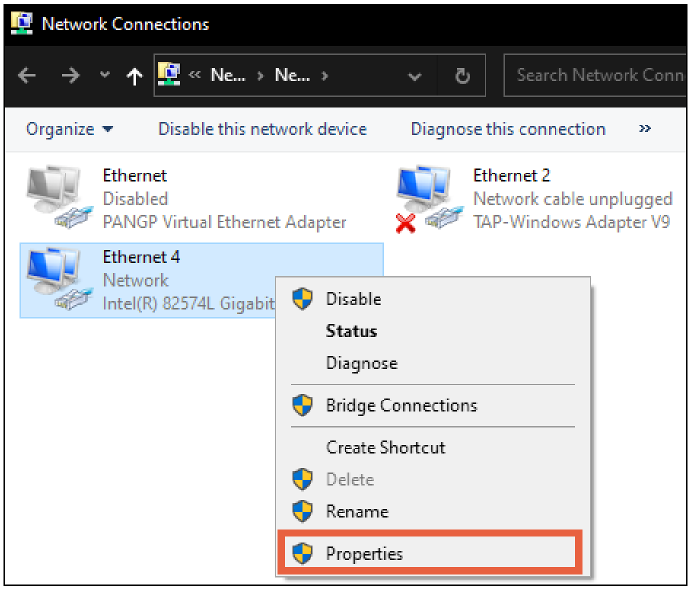
Access type: Internet
Connections: Ethernet 4

Change your networking settings

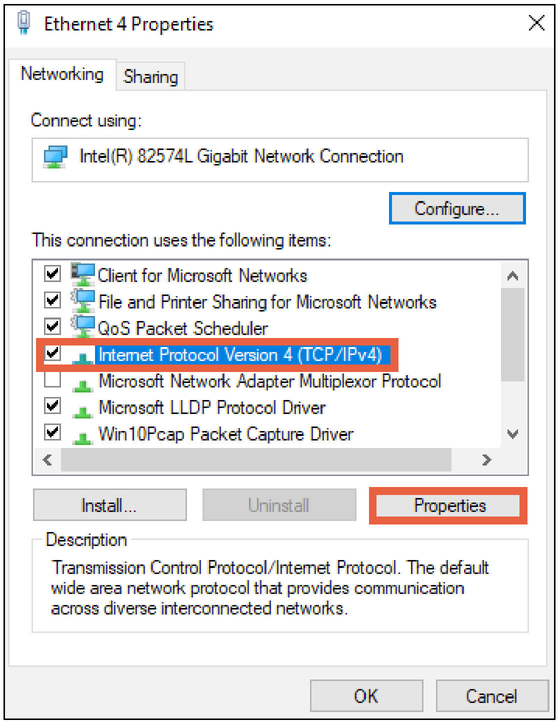
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Step 5: Right-click the icon for the wired network connection, then left-click **Properties**.



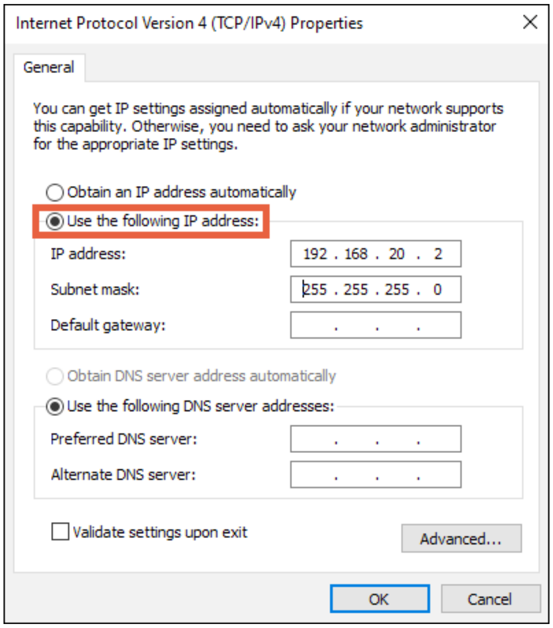
Step 6: Select Internet Protocol Version 4 (TCP/IPv4), then click **Properties**.


Ethernet 4 Properties
Networking
Sharing
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Win10Pcap Packet Capture Driver
Install...
Uninstall
Properties
Description
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Step 7: In the General tab, click Use the following IP address: and enter the IP address and subnet mask, then click OK.

IP Address	192.168.20.2
Subnet Mask	255.255.255.0



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 20 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

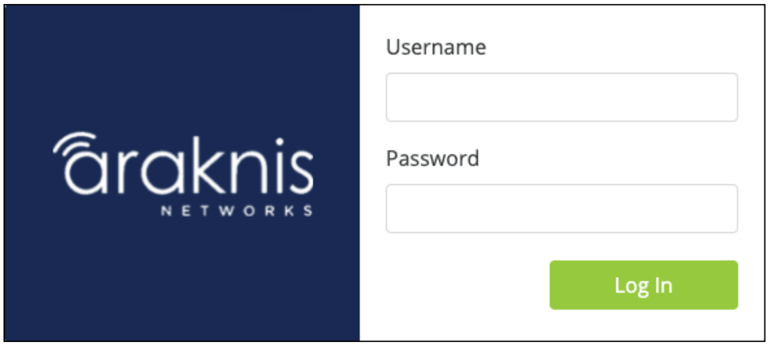
Preferred DNS server: . . .

Alternate DNS server: . . .

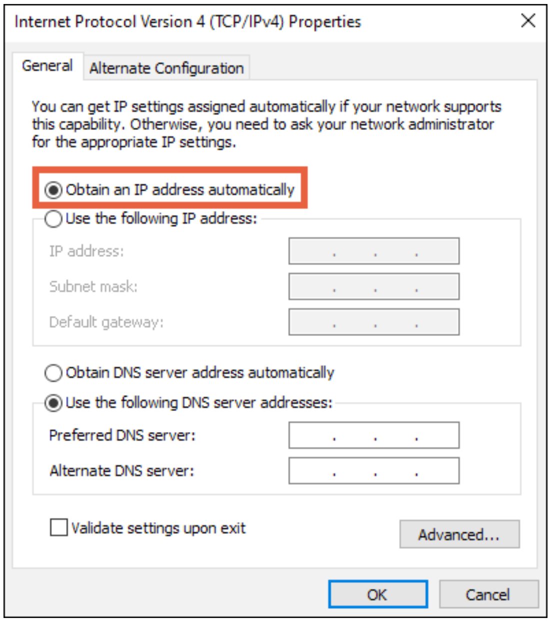
□ Validate settings upon exit

Step 8: Open a browser and navigate to https://192.168.20.253/. Log in using the default credentials:

Username	araknis
Password	araknis



Step 9: After configuring the AP, set your computer's IPv4 Properties back **to Obtain an IP address automatically**, then click **OK**.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

○ Obtain DNS server address automatically

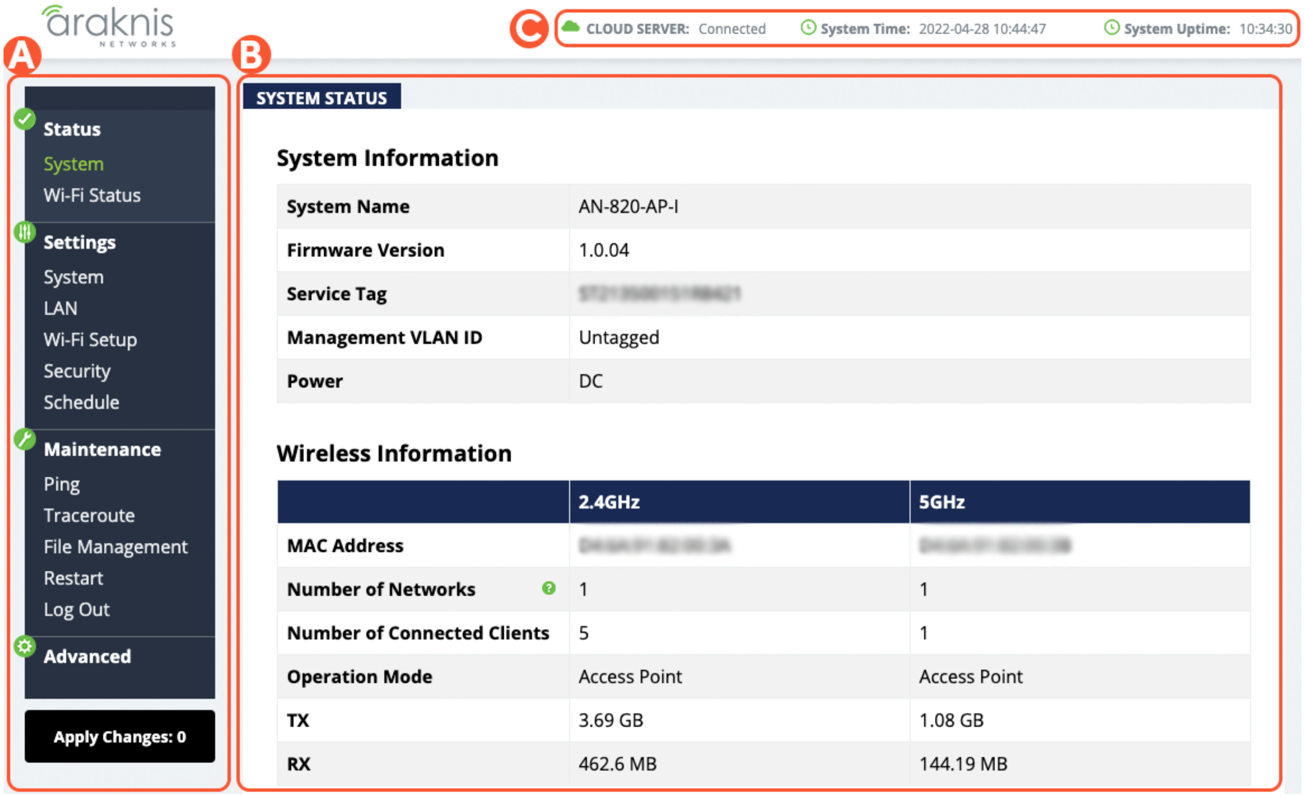
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

User Interface Overview



CLOUD SERVER: Connected System Time: 2022-04-28 10:44:47 System Uptime: 10:34:30

System Information

System Name	AN-820-AP-I
Firmware Version	1.0.04
Service Tag	[redacted]
Management VLAN ID	Untagged
Power	DC

Wireless Information

	2.4GHz	5GHz
MAC Address	[redacted]	[redacted]
Number of Networks	1	1
Number of Connected Clients	5	1
Operation Mode	Access Point	Access Point
TX	3.69 GB	1.08 GB
RX	462.6 MB	144.19 MB

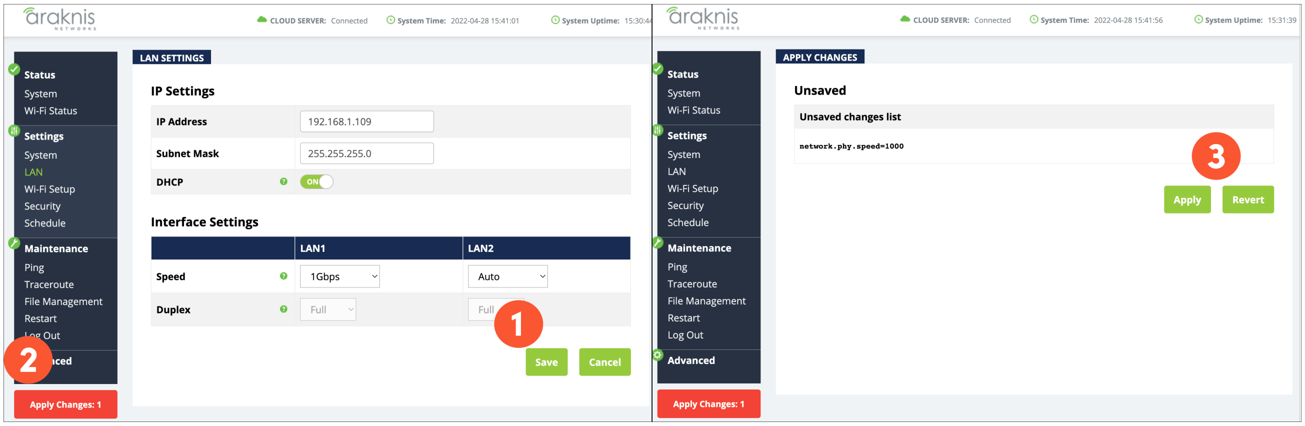
A. **Main Navigation Menu:** Use the sub-menus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the access point. Click **Apply Change**s to review and apply the changes saved in menus.

B. **Main Window:** The main window displays the currently selected sub-menu.

C. **Top Bar**: The top bar displays the current connection status to the OvrC server, the current internally-set system time, and the current system uptime in Days:Hours:Minutes.

Applying changes to the access point

1. After making changes to settings on a menu page, click the **Save** button on the menu to hold the new settings in the Apply Changes field.
2. After all desired changes have been made, click **Apply Changes** to review the new settings.
3. Click **Apply** to make the changes or Revert to cancel the changes.



CLOUD SERVER: Connected System Time: 2022-04-28 15:41:01 System Uptime: 15:30:44

LAN SETTINGS

IP Settings

IP Address	192.168.1.109
Subnet Mask	255.255.255.0
DHCP	ON

Interface Settings

	LAN1	LAN2
Speed	1Gbps	Auto
Duplex	Full	Full

CLOUD SERVER: Connected System Time: 2022-04-28 15:41:56 System Uptime: 15:31:39

APPLY CHANGES

Unsaved

Unsaved changes list

```
network.phy.speed=1000
```

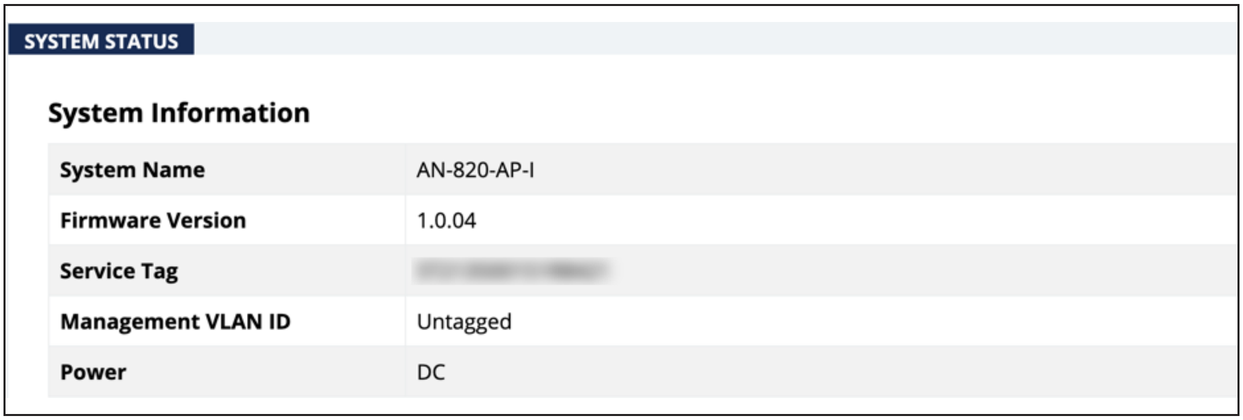
System Status

The initial page, after login, is the System Status. This page provides a real-time summary of the access point's system information. Use the screen to verify the settings and operation of your device.

System Information

Displays the current information about the AP's system settings.

Path: Status > System > System Information



System Information

System Name	AN-820-AP-I
Firmware Version	1.0.04
Service Tag	[redacted]
Management VLAN ID	Untagged
Power	DC

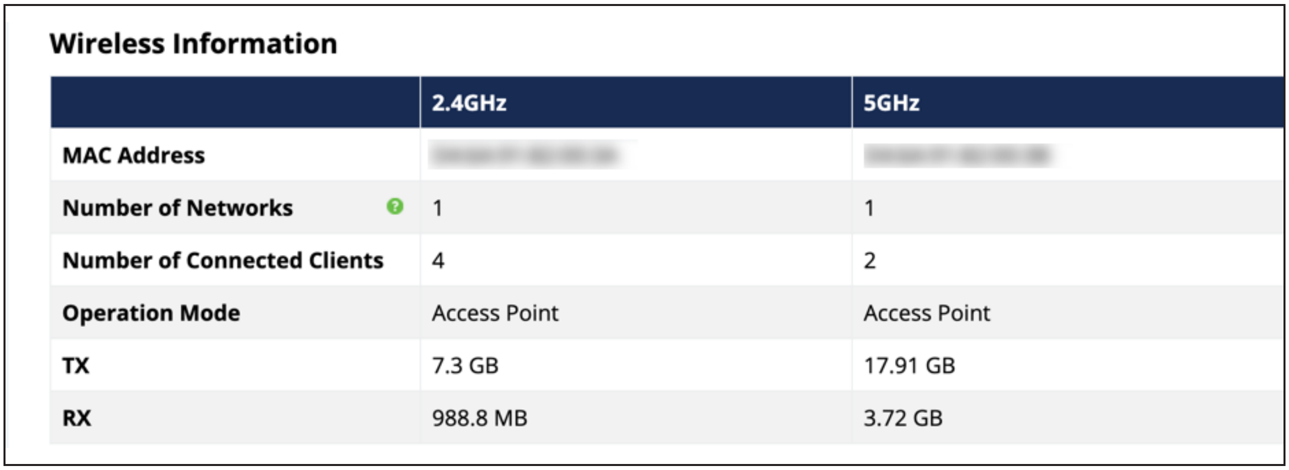
Table Fields

- **System Name:** The name assigned to the system. Used for configured name access.
- **Service Tag:** Internal tracking number used to track every product sold by Araknis Networks.
- **Firmware Version:** The urrent firmware version running on the access point.
- **Management VLAN ID:** The VLAN that must be used to access the web interface.

Wireless Information

Displays the current information about the wireless radio channel(s) in use.

Path: Status > System > Wireless Information



Wireless Information

	2.4GHz	5GHz
MAC Address	[redacted]	[redacted]
Number of Networks	1	1
Number of Connected Clients	4	2
Operation Mode	Access Point	Access Point
TX	7.3 GB	17.91 GB
RX	988.8 MB	3.72 GB

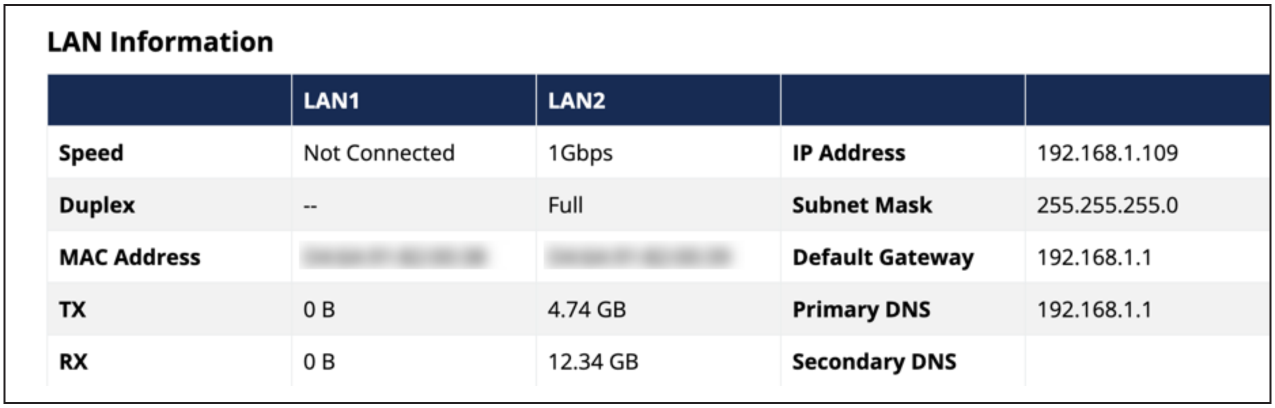
Table Fields

- **MAC Address:** The individual Media Access Control (MAC) address assigned to the 2.4GHz and 5GHz radio interfaces.
- **Number of Networks:** The number of active wireless networks (i.e. SSID's) configured on the radio interface.
- **Number of Connected Clients:** The number of currently connected wireless clients on all configured networks using the radio interface.
- **Operation Mode:** Indicates that the radio is configured as an access point.
- **TX:** The amount of data, in bytes, transmitted on the radio interface since the last power cycle.
- **RX:** The amount of data, in bytes, received on the radio interface since the last power cycle.

LAN Information

Displays the current LAN connection parameters.

Path: Status > System > LAN Information



LAN Information

	LAN1	LAN2		
Speed	Not Connected	1Gbps	**IP Address**	192.168.1.109
Duplex	--	Full	**Subnet Mask**	255.255.255.0
MAC Address	[redacted]	[redacted]	**Default Gateway**	192.168.1.1
TX	0 B	4.74 GB	**Primary DNS**	192.168.1.1
RX	0 B	12.34 GB	**Secondary DNS**	

Table Fields

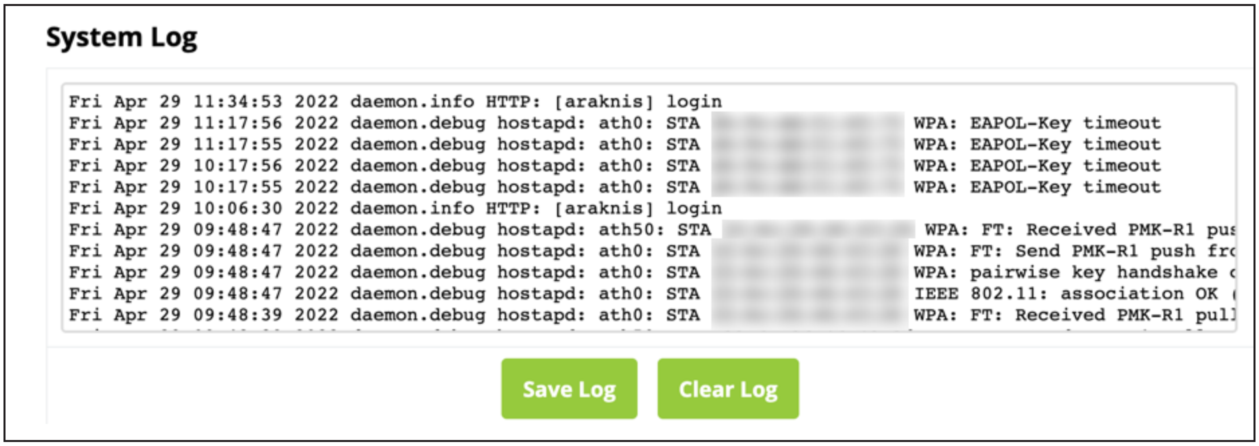
- **Speed:** Indicates negotiated LAN speed between the access point and the wired network.
- **Duplex:** Indicates the negotiated duplex setting between the access point and the wired network.
- **MAC address:** The MAC address assigned to the LAN port. LAN port 1 MAC address is always primary.
- **TX:** The amount of data, in bytes, transmitted over the wired network connection.
- **RX:** The amount of data, in bytes, received from the wired network connection.
- **IP Address:** The access point's IP address issued by the network router.
- **Subnet Mask:** The access point's subnet mask.
- **Default Gateway:** The IP address of the router that assigned the access point an IP address.

- **Primary DNS:** The primary DNS assigned to device.
- **Secondary DNS:** The secondary DNS assigned to the device.

System Log

The System Log records changes to configuration, connections, security conditions, and more.

Path: Status > System > System Log



```
Fri Apr 29 11:34:53 2022 daemon.info HTTP: [araknis] login
Fri Apr 29 11:17:56 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: EAPOL-Key timeout
Fri Apr 29 11:17:55 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: EAPOL-Key timeout
Fri Apr 29 10:17:56 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: EAPOL-Key timeout
Fri Apr 29 10:17:55 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: EAPOL-Key timeout
Fri Apr 29 10:06:30 2022 daemon.info HTTP: [araknis] login
Fri Apr 29 09:48:47 2022 daemon.debug hostapd: ath50: STA [redacted] WPA: FT: Received PMK-R1 pus
Fri Apr 29 09:48:47 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: FT: Send PMK-R1 push fro
Fri Apr 29 09:48:47 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: pairwise key handshake c
Fri Apr 29 09:48:47 2022 daemon.debug hostapd: ath0: STA [redacted] IEEE 802.11: association OK (
Fri Apr 29 09:48:39 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: FT: Received PMK-R1 pull
```

Options

- **Save Log:** Click to view the log as a text file or save the log for future reference.
- **Clear Log:** Click to permanently delete the contents of the System Log.

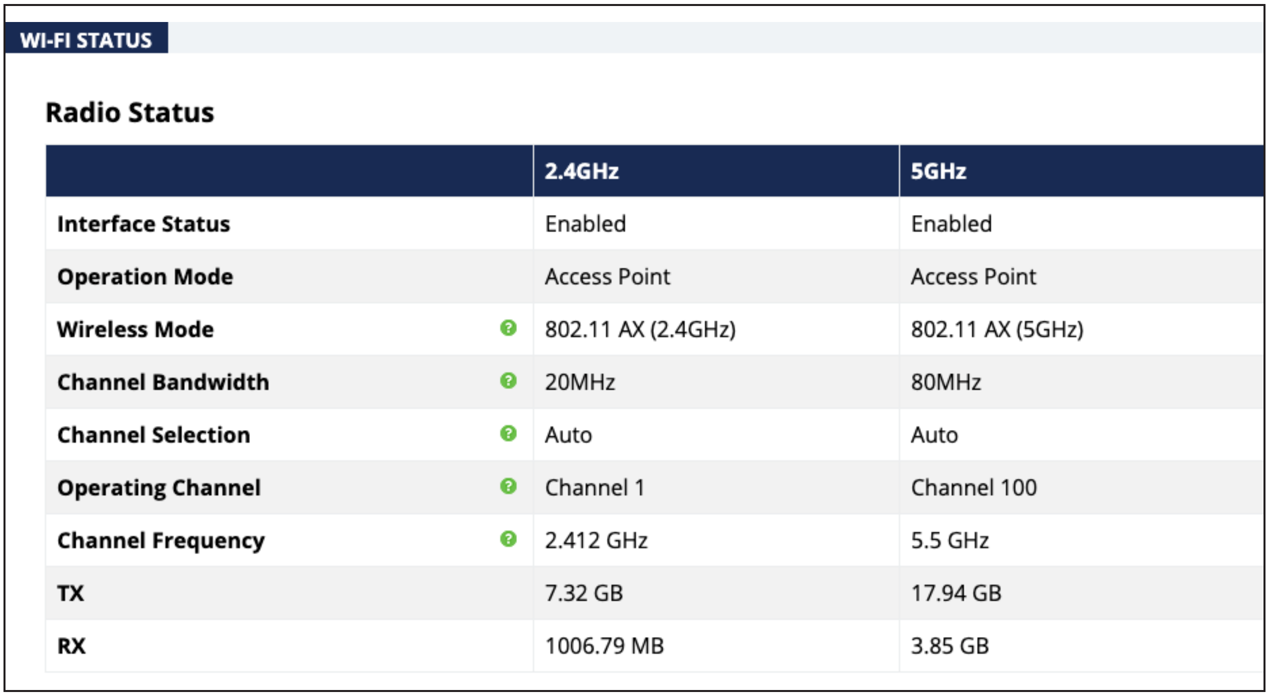
Wi-Fi Status

Provides a detailed look at the wireless settings and performance for radio status, settings, wireless network configuration, and connected client status.

Radio Status

Provides a detailed look at the radio settings and performance.

Path: Status > Wireless interface > Radio Status



WI-FI STATUS

Radio Status

	2.4GHz	5GHz
Interface Status	Enabled	Enabled
Operation Mode	Access Point	Access Point
Wireless Mode ?	802.11 AX (2.4GHz)	802.11 AX (5GHz)
Channel Bandwidth ?	20MHz	80MHz
Channel Selection ?	Auto	Auto
Operating Channel ?	Channel 1	Channel 100
Channel Frequency ?	2.412 GHz	5.5 GHz
TX	7.32 GB	17.94 GB
RX	1006.79 MB	3.85 GB

Table Fields

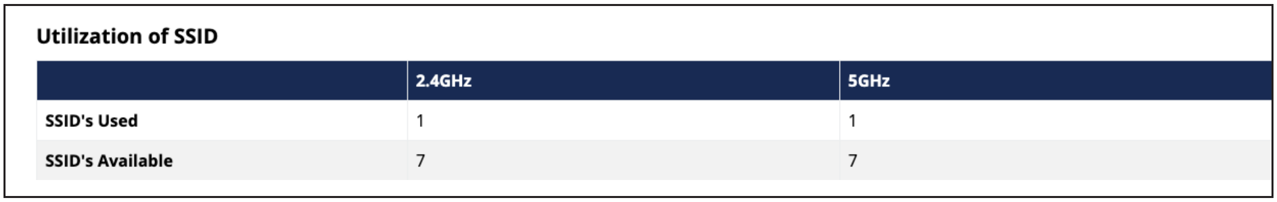
- **Interface Status:** Indicates whether the wireless antenna is enabled or disabled.
- **Operation Mode:** Indicates that the radio is configured as an access point.

- **Wireless Mode:** Indicates the Wi-Fi protocol(s) currently in use with the band frequency.
- **Channel Bandwidth:** Indicates the current channel bandwidth.
- **Channel Selection:** Indicates the current channel setting.
- **Operating Channel:** Indicates the current operating channel.
- **Channel Frequency:** Indicates the frequency of the operating channel.
- **TX:** The amount of data transmitted in bytes.
- **RX:** The amount of data received in bytes.

Utilization of SSID

Details the use and availability of the SSIDs configured in the AP.

Path: Status > Wireless interface > Wireless Network



Utilization of SSID

	2.4GHz	5GHz
SSID's Used	1	1
SSID's Available	7	7

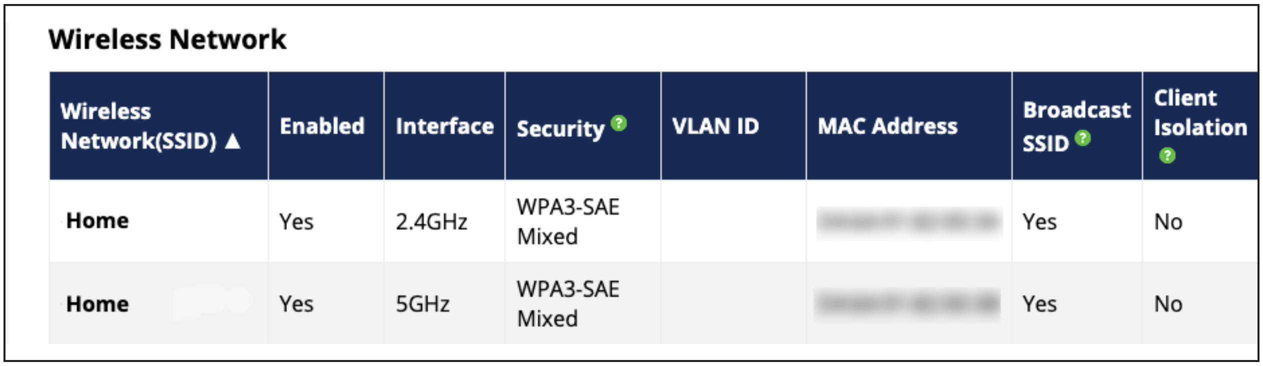
Table Fields

- **SSIDs Used:** The number of SSIDs currently configured in the AP.
- **SSIDs Available:** The number of SSIDs that can be configured in the AP.

Wireless Network

The Wireless Network table provides a detailed look at how the SSIDs are configured.

Path: Status > Wireless interface > Wireless Network



Wireless Network

Wireless Network(SSID) ▲	Enabled	Interface	Security	VLAN ID	MAC Address	Broadcast SSID	Client Isolation
Home	Yes	2.4GHz	WPA3-SAE Mixed		[redacted]	Yes	No
Home	Yes	5GHz	WPA3-SAE Mixed		[redacted]	Yes	No

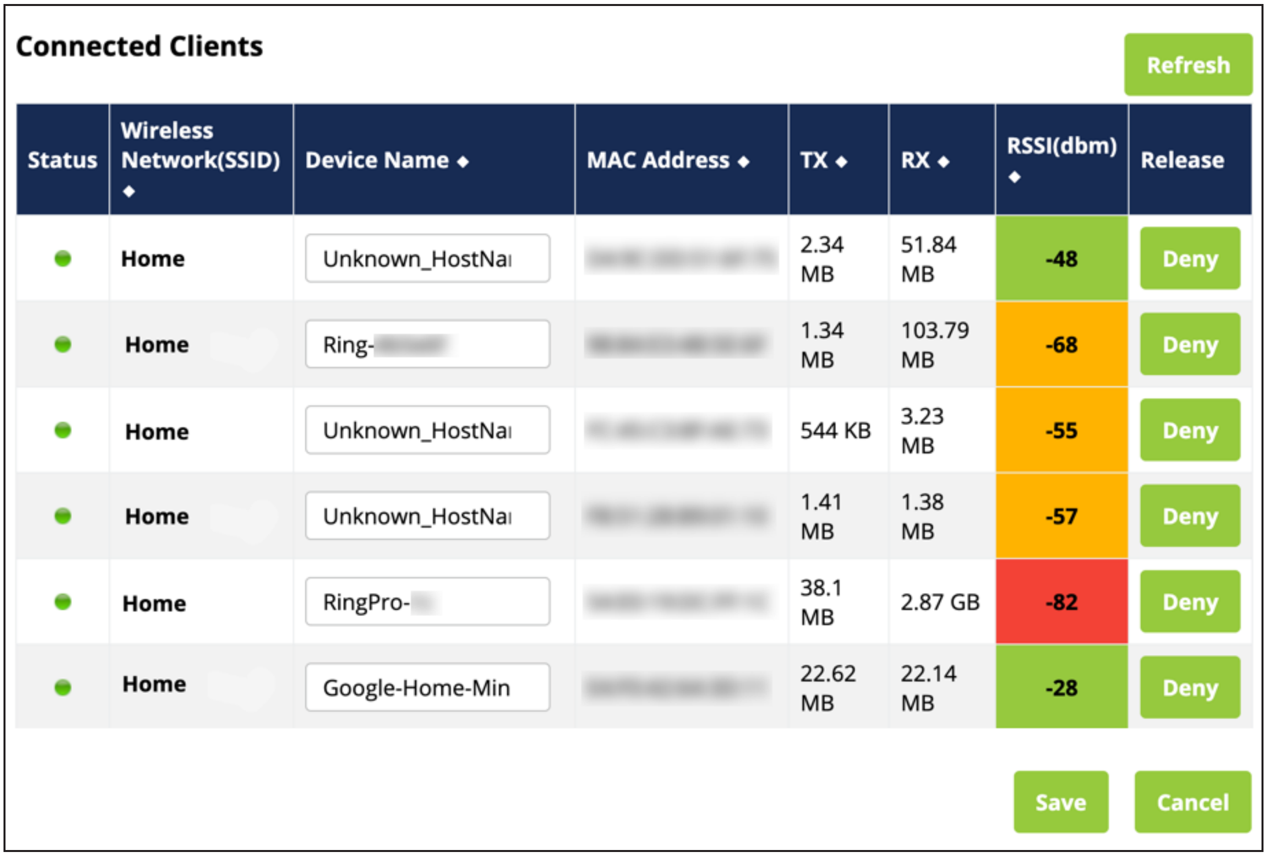
Table Fields

- **Wireless Network (SSID):** The SSIDs being transmitted by the access point.
- **Enabled:** Indicates whether the SSID is enabled or disabled.
- **Interface:** Indicates the operating frequency of the SSID.
- **Security:** Indicates the security mode selected for the SSID.
- **VLAN ID:** Indicates if the SSID is tagged with a VLAN ID.
- **MAC address:** The MAC address of the radio interface that's transmitting the SSID.
- **Broadcast SSID:** Indicates whether the SSID is visible to Wi-Fi devices and discovery tools.
- **Client Isolation:** Indicates whether or not client devices connected to different SSIDs can communicate with each other.

Connected Clients

The Connected Clients table provides details about the devices connected to any SSID on the access point.

Path: Status > Wireless interface > Connected Clients



Connected Clients

Status	Wireless Network(SSID) ◆	Device Name ◆	MAC Address ◆	TX ◆	RX ◆	RSSI(dbm) ◆	Release
●	Home	Unknown_HostNa	[redacted]	2.34 MB	51.84 MB	-48	Deny
●	Home	Ring-[redacted]	[redacted]	1.34 MB	103.79 MB	-68	Deny
●	Home	Unknown_HostNa	[redacted]	544 KB	3.23 MB	-55	Deny
●	Home	Unknown_HostNa	[redacted]	1.41 MB	1.38 MB	-57	Deny
●	Home	RingPro-[redacted]	[redacted]	38.1 MB	2.87 GB	-82	Deny
●	Home	Google-Home-Min	[redacted]	22.62 MB	22.14 MB	-28	Deny

Table Fields

- **Status:** Indicates whether the client is currently connected. Green indicates that the client is connected to the SSID.
- **Wireless Network (SSID):** Indicates the SSID the wireless client is connected to.
- **Device Name:** The name either pulled from or assigned to the wireless client.
- **MAC address:** Displays the MAC address of the connected wireless client.

- **TX:** The amount of data, in kilobytes, transmitted to the connected wireless client.
- **RX:** The amount of data, in kilobytes, received from the connected wireless client.
- **RSSI (dBm):** Displays the wireless signal strength between the access point and the connected client.

  The color of the table field represents the signal strength: green is strong, yellow is medium, and red is weak.
- **Release:** Click the Deny button to remove the client from the network.

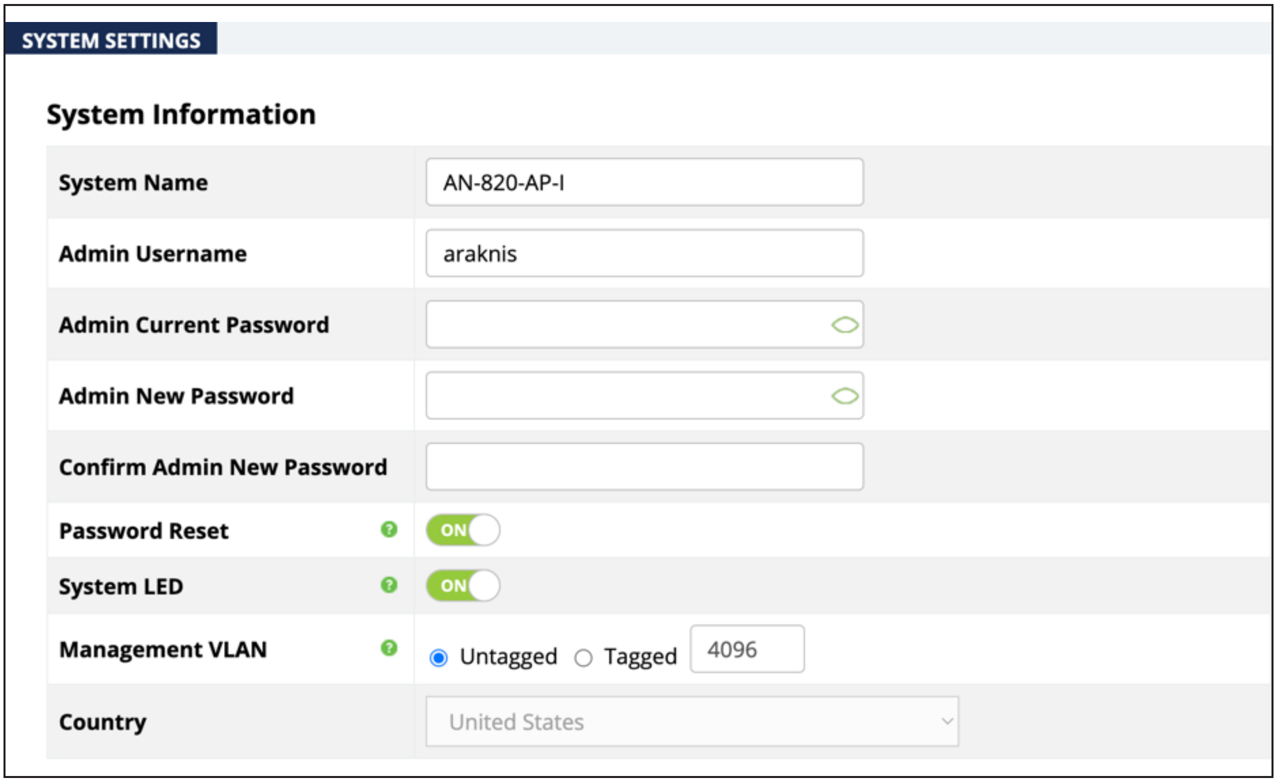
Note: The closer the RSSI (dBm) value is to 0, the stronger the signal is, and the closer to -100, the weaker the signal is.

System Settings

System Information

Use the System Information page to configure administration and access settings.

Path: Settings > System > System Information



SYSTEM SETTINGS

System Information

System Name	AN-820-AP-I
Admin Username	araknis
Admin Current Password	
Admin New Password	
Confirm Admin New Password	
Password Reset	ON
System LED	ON
Management VLAN	● Untagged ○ Tagged 4096
Country	United States

Configurable Settings

- **System Name:** Enter a meaningful name such as SmithHome or SmithBasement. Limited to 32 characters, including spaces.
- **Admin Username:** Enter a username for logging into the access point. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.
  Default: araknis

- **Admin Current Password:** Enter the current login password when changing the password.
  Default: araknis
- **Admin New Password**: Enter a new login password. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.
- **Confirm Admin New Password:** Enter the same password as above, to confirm.
- **Password Reset:** This toggle disables/enables the physical password reset button on the AP. Disabling this feature requires a full factory reset of the AP to reset the username/password.
- **System LED:** Turn the Status LED ON or OFF.
  Default: ON
- **Management VLAN:** The VLAN ID you must be connected to for access to the AP web interface.
- **Default:** Untagged

Caution: Changing the management VLAN could cause loss of to access to the web interface. Connect your computer to the new management VLAN or reset the AP to regain connectivity.

- **Country:** Select the country of the install location to comply with local standards.
- **Default:** United States

Note: This setting is only configurable on international models.

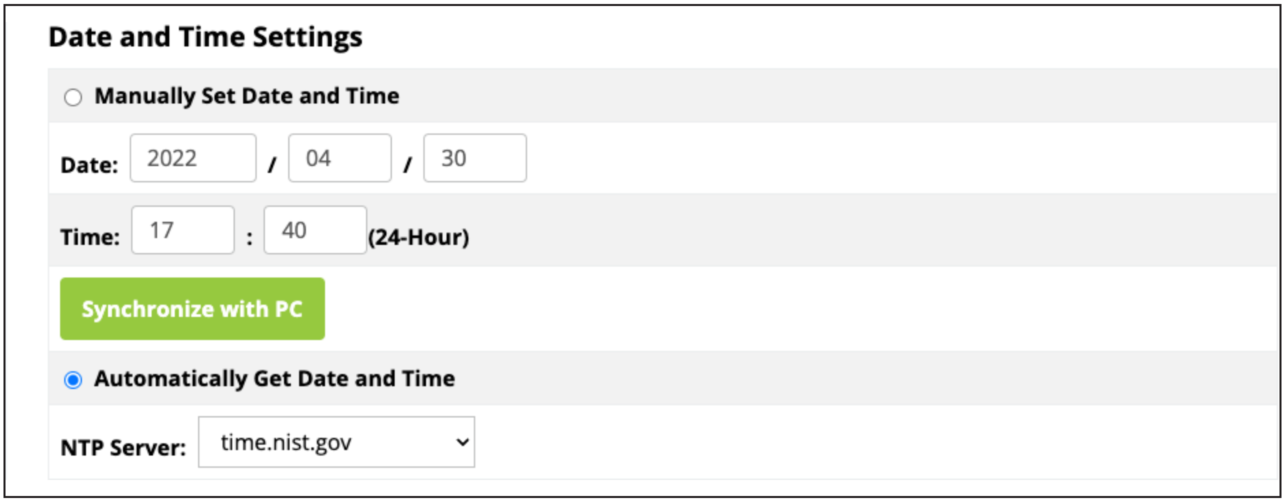
Click **Save**, then **Apply Changes** when you're finished with the configuration.

Date and Time Settings

Configure the system date and time settings that are displayed in the AP menus and logs.

Path: Settings > System > Date and Time Settings

Pro Tip: Use the default **Automatically Get Date and Time** setting. Manual configuration may not remain accurate after power outages or resets.



Date and Time Settings

○ Manually Set Date and Time

Date: 2022 / 04 / 30

Time: 17 : 40 (24-Hour)

● Automatically Get Date and Time

NTP Server: time.nist.gov

Configurable Settings

- **Manually Set Date and Time:** Select to manually set the date and time.
- **Date:** Enter the year, month and date (four digits for year; two digits for month, and two digits for date).
- **Time:** Enter the hour and minutes for the current time. Use a mobile device or satellite clock for accuracy.
- **Synchronize with PC:** Click this button to automatically sync the access point to the connected computer's clock.

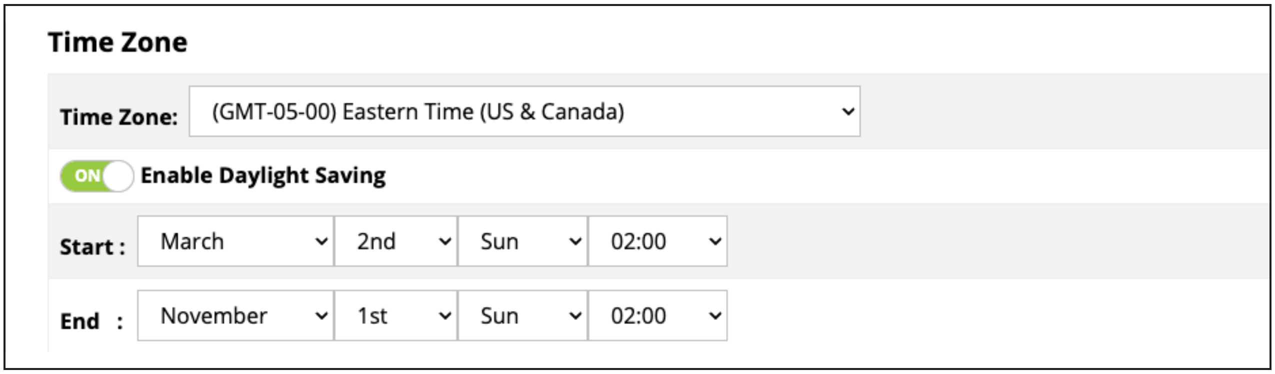
- **Automatically Get Date and Time:** Automatically get the date and time from a 3rd-party NTP server.
- **NTP Server:** Select an NTP (Network Time Protocol) Server to reference for the standard date and time.
  Default: time.nist.gov (recommended)

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Time Zone Settings

Configure the time zone and Daylight Saving settings for the install location.

Path: Settings > System > Date and Time Settings



Time Zone

Time Zone: (GMT-05-00) Eastern Time (US & Canada)

ON Enable Daylight Saving

Start : March | 2nd | Sun | 02:00

End : November | 1st | Sun | 02:00

Configurable Settings

- **Time Zone:** Select the appropriate time zone from the drop-down.
- **Enable Daylight Saving:** Select to enable.
- **Start:** Select the month, date, day and time Daylight Saving Time starts from the drop-downs.
- **End:** Select the month, date, day and time Daylight Saving Time ends from the drop-downs.

Note: Daylight Saving start and end can change from year to year. Be sure to update this information to avoid potential network errors.

Click **Save**, then **Apply Changes** when you’re finished with the configuration.

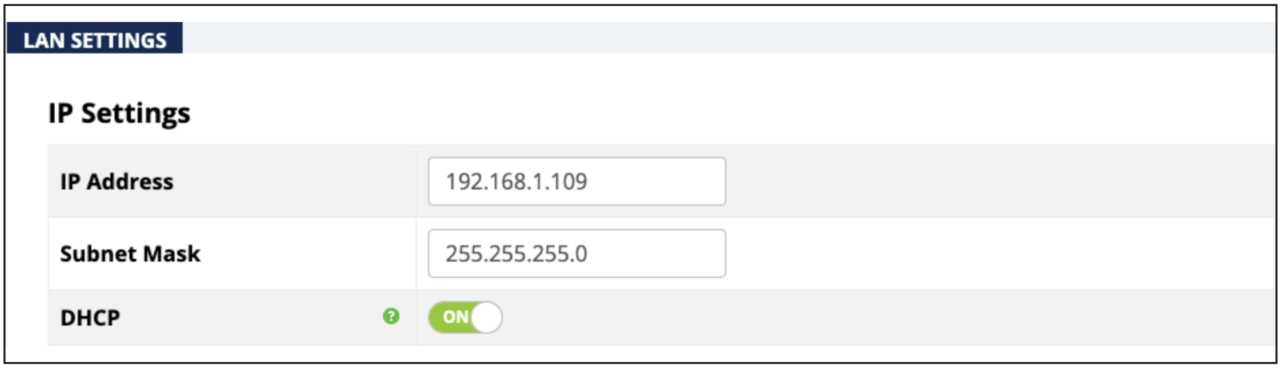
LAN Settings

IP Settings

Configure the AP’s IP address.

Pro Tip: Leave the IP Settings at the default DHCP enabled and make a MAC reservation in the router. If you prefer static IP addresses, use an IP address outside the router’s DHCP range.

Path: Settings > LAN > IP Settings



LAN SETTINGS

IP Settings

IP Address	192.168.1.109
Subnet Mask	255.255.255.0
DHCP	ON

Configurable Settings

- **IP Address:** Toggle DHCP to enter a static IP address for the device.
- **Subnet Mask:** Enter the subnet mask for the device.
- **Default:** 255.255.255.0
- **DHCP:** Allows the access point to receive a DHCP IP address from the network router, when enabled. Uncheck the box to configure a static IP address.
- **Default**: Enabled

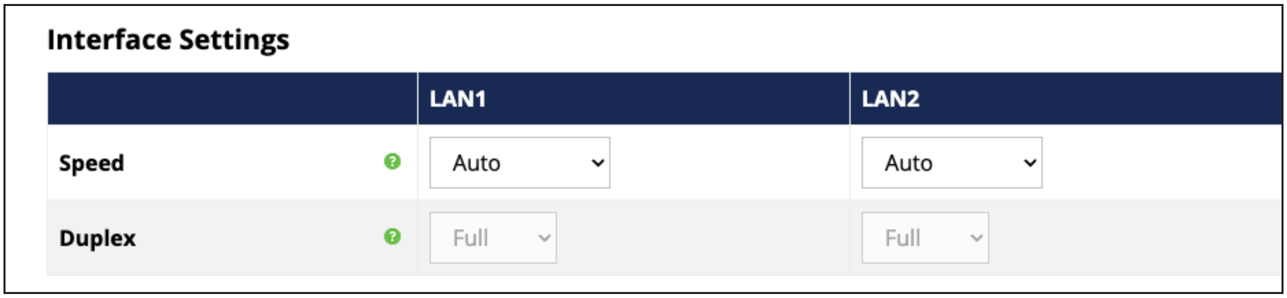
Click **Save**, then **Apply Changes** when you’re finished with the configuration.

Interface Settings

Configure the LAN speed and duplex settings for the LAN port(s).

Pro Tip: Leave these settings at their defaults unless you have a specific compatibility use case or for troubleshooting.

Path: Settings > LAN > Interface Settings



Interface Settings

	LAN1	LAN2
Speed ?	Auto	Auto
Duplex ?	Full	Full

Configurable Settings

- **Speed:** Select the LAN speed to Auto, 1Gbps, 100Mbps, 10Mbps, Disable (Disable turns the LAN Port OFF)
- **Default:** Auto
- **Duplex:** (10/100Mbps modes only) Select the duplex setting between the access point and the network router to Half or Full.
- **Default:** Full

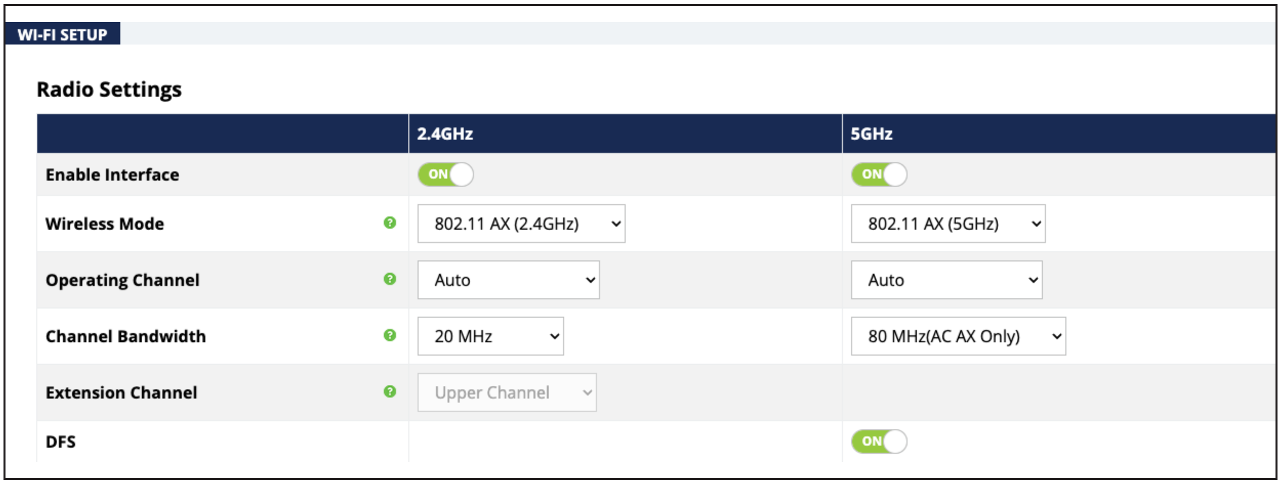
Click **Save**, then **Apply Changes** when you're finished with the configuration.

Wi-Fi Setup

Radio Settings

Configure the access point’s radio settings including wireless modes, operating channels, channel bandwidth, and extension channel.

Path: Settings > Wireless > Radio Settings



WI-FI SETUP

Radio Settings

	2.4GHz	5GHz
Enable Interface	ON	ON
Wireless Mode	802.11 AX (2.4GHz)	802.11 AX (5GHz)
Operating Channel	Auto	Auto
Channel Bandwidth	20 MHz	80 MHz(AC AX Only)
Extension Channel	Upper Channel	
DFS		ON

Configurable Settings

- **Enable Interface:** Toggle to enable or disable the radio interface.
- Default: Yes.
- **Wireless Mode:** Select the wireless mode for the radio.
  Default: 2.4GHz - 802.11 B/G/N/AX; 5GHz - 802.11 A/N, 802.11 AC/N, or 802.11 AX.
- **Operating Channel:** Select the desired Wi-Fi channel. Use a different channel than other APs on the network. On the 2.4GHz radio, there are only three non-overlapping channels: 1, 6 and 11. Select a channel as far away from close-numbered channels as possible.
  Default: Auto.

Pro Tip: In a multi-AP environment, put adjacent APs on channels as far apart as possible. A spectrum analyzer tool (such as Metageek's Chanalyzer Pro) is recommended for providing detailed information about possible channel interference.

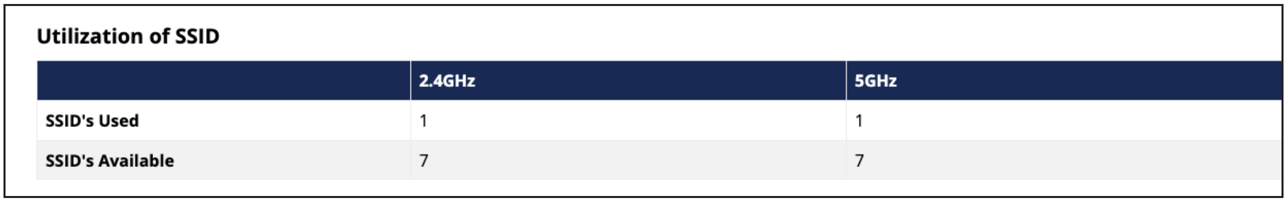
- **Channel Bandwidth:** Select the desired channel bandwidth. Smaller values allow greater range and larger values provide greater throughput. The combination setting allows the AP to decide.
  Default: 2.4GHz - 20MHz; 5GHz - 40MHz, 80Mhz.
- **Extension Channel:** Specify whether the channel extends above or below the normal 20MHz range. Only applies when the Channel Bandwidth is set higher than 20MHz.
  Default: 2.4GHz - Upper Channel; 5GHz - Lower Channel.
- **DFS:** Toggle to enable the use of DFS channels on the 5GHz radio interface.

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Utilization of SSID

Details the use and availability of SSIDs configured in the AP.

Path: Settings > Wireless > Utilization of SSID



Utilization of SSID

	2.4GHz	5GHz
SSID's Used	1	1
SSID's Available	7	7

Table Fields

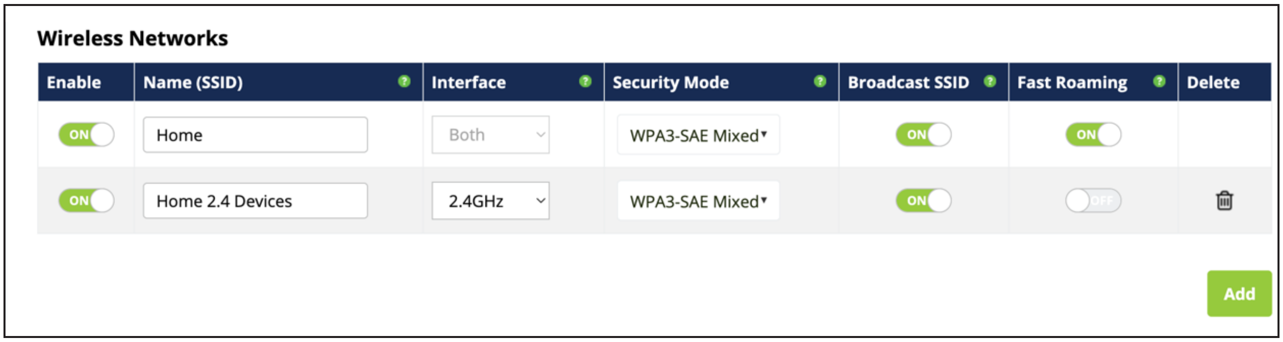
- **SSIDs Used:** The number of SSIDs currently in use by devices connected to the AP.
- **SSIDs Available:** The total number of SSIDs that can be configured on the AP.

Wireless Networks

Use the Wireless Networks menu to configure wireless networks (SSIDs) and their security settings.

Note: The default araknis_initial SSID settings are not secure and need to be changed.

Path: Settings > Wireless > Wireless Networks



Wireless Networks

Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Fast Roaming	Delete
ON	Home	Both	WPA3-SAE Mixed	ON	ON	
ON	Home 2.4 Devices	2.4GHz	WPA3-SAE Mixed	ON	OFF	🗑

Configurable Settings

- **Enable:** Select Yes to make the SSID available.

  Default: On.

- **Name (SSID):** Enter the network name for the network being configured.

  Default: araknis_initial (Blank when adding a new network).

- **Interface**: Select which channel frequencies should be broadcast. 2.4GHz, 5GHz, or Both.

  Default: Both, (2.4GHz when adding a network).

- **Security Mode:** Select a security mode from the drop-down to open the Wireless Security window. See section 10.5 - Wireless Security Options (SSID Encryption) (p.29) for wireless security setup options.

  Default: Open

- **Broadcast SSID:** Toggle whether or not to publicly display the SSID to nearby Wi-Fi devices.
  Default: Yes
- **Fast Roaming:** This feature allows client devices to seamlessly switch between multiple APs broadcasting the same SSID, based on the AP providing the best signal at any time. Read the below "Fast Roaming" on page 41 section for more information about this feature.
- **Add:** Click to add an SSID.
- **Delete:** Click to delete the SSID. The first SSID cannot be deleted.

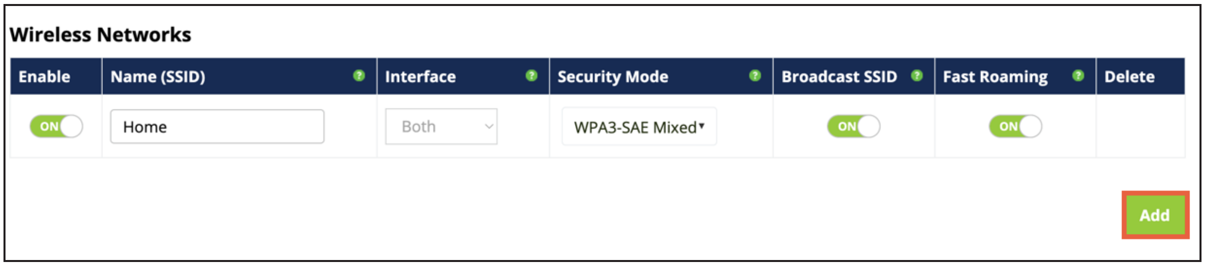
Click **Save**, then **Apply Changes** when you’re finished with the configuration.

Note: Client Isolation and Band Steering can be found at Advanced > Wireless Settings > Wireless Network Settings.

How to Configure a New SSID

Wi-Fi configuration varies depending on the installation site and devices being used on the network. To learn more about general setup, click here for our Wi-Fi Best Practices.

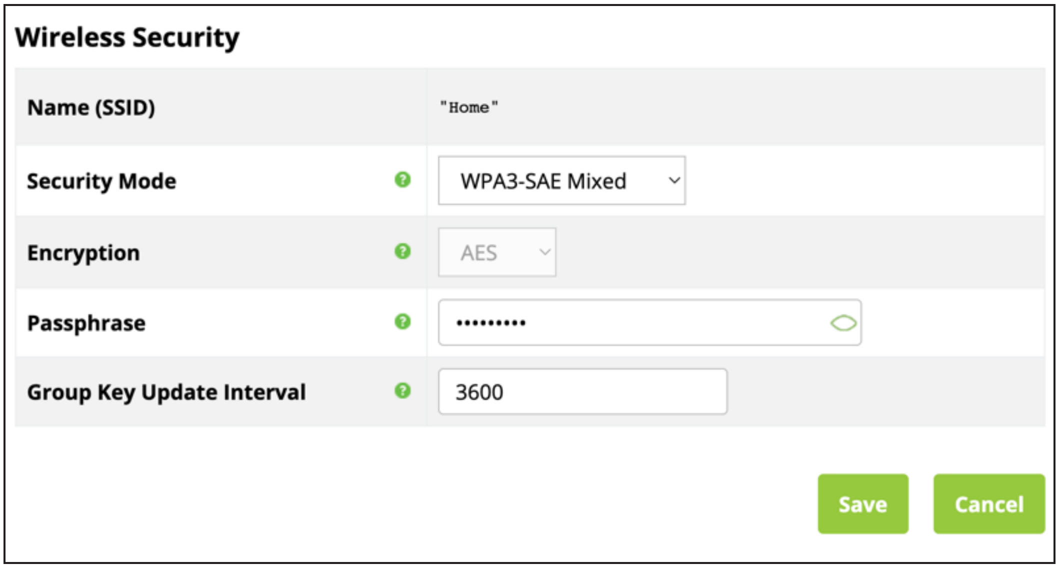
1. From the Wireless Settings page, scroll to the Wireless Networks menu.
2. Click **Add** if you are creating a new SSID, otherwise modify the settings for the default SSID.



Wireless Networks

Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Fast Roaming	Delete
ON	Home	Both	WPA3-SAE Mixed	ON	ON	

3. Enter a **Name** for the SSID.
4. Use the **Interface** drop-down to select 2.4 GHz, 5 GHz, or both frequencies. We recommend using **Both** unless requirements specify a certain frequency.
5. Select a **Security Mode** from the drop-down to open the Wireless Security window. The settings vary depending on the chosen mode. Refer to the proper section and configure the wireless settings as desired, then click **Save** to return to the main screen.
   - **Open**– Not recommended. Anyone that can find or see the SSID can connect.
   - **WPA2-PSK, WPA-PSK Mixed, WPA3, and WPA3-SAE Mixed Configuration**



Wireless Security

Name (SSID)	"Home"
Security Mode	WPA3-SAE Mixed
Encryption	AES
Passphrase	•••••••••
Group Key Update Interval	3600

- **Name (SSID):** The name of the SSID being configured.
- **Security Mode:** Displays the current selected mode. You can select a different encryption mode from the drop-down.
- **Encryption**: WPA2-PSK. WPA3, and WPA3-SAE use AES. WPA-PSK uses Both (TKIP+AES).
- **Passphrase**: Enter a passphrase for the wireless network being configured. If using the ASCII format, the password must be 8-63 characters in length. If using HEX, the password must be 64 HEX characters in length.

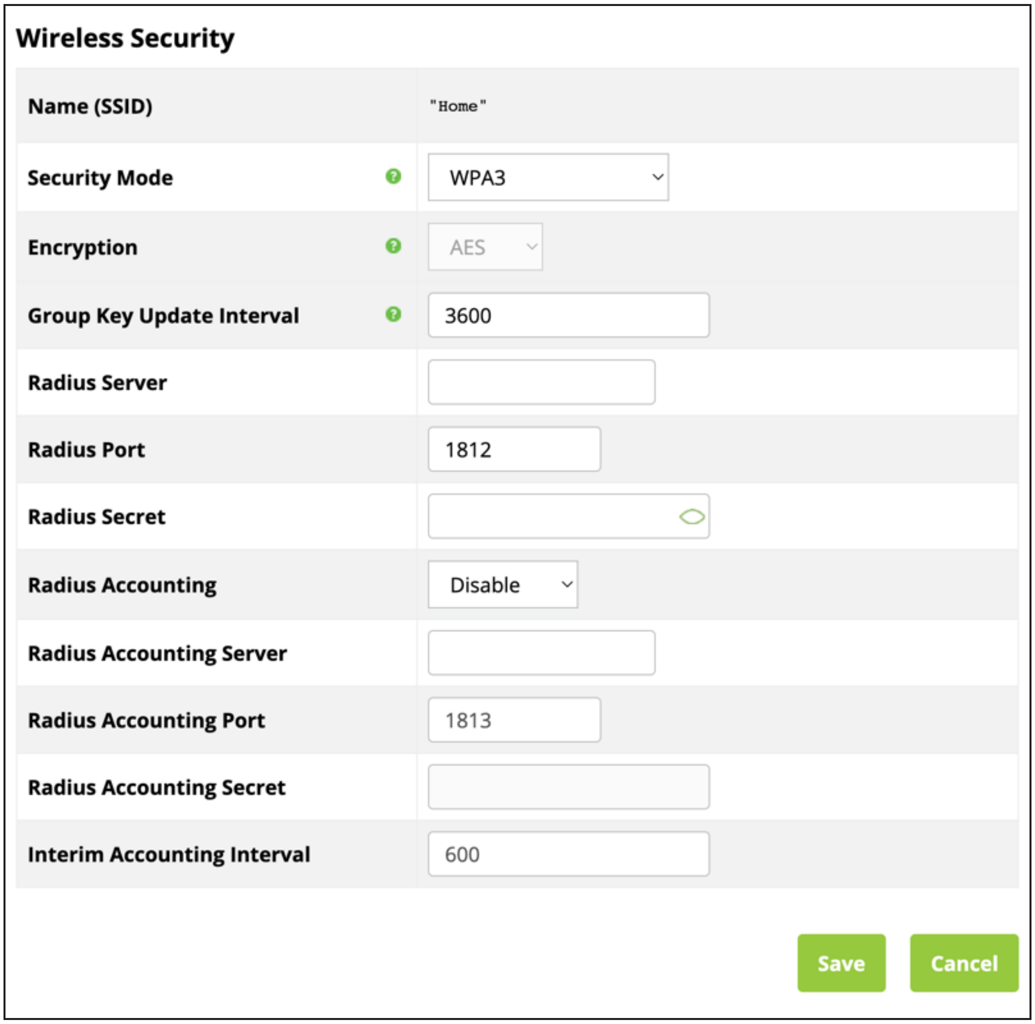
  Default: Blank
- **Group Key Update Interval:** Enter a value to specify how often, in seconds, the Group key changes. This value can be anywhere between 30-3600 seconds.

  Default: 3600 (60 minutes)

Click **Save** or **Cancel**.

- **WPA, WPA2, WPA Mixed, and WPA3 Configuration**

Note: For RADIUS setup, refer to the server instructions provided by the manufacturer



Wireless Security

Name (SSID)	"Home"
Security Mode	WPA3
Encryption	AES
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

- **Name (SSID):** The name of the SSID being configured.
- **Security Mode:** Displays the current selected mode. You can select a different encryption mode from the drop-down.
- **Encryption:** WPA. WPA2, and WPA3 use AES. WPA-PSK uses Both (TKIP+AES).

- **Group Key Update Interval:** Enter a value to specify how often, in seconds, the Group key changes. This value can be anywhere between 30-3600 seconds.

  Default: 3600 (60 minutes)

- **Radius Server:** Enter the radius server's IP address.
- **Radius Port:** Enter the radius server's connection port number.

  Default: 1812 (This is a dedicated TCP/UDP port and typically should not be changed.)

- **Radius Secret:** Enter the radius server's connection secret.

  Default: Blank

- **Radius Accounting:** Use the drop-down to enable or disable radius accounting.

  Default: Disable

- **Radius Accounting Server:** Enter the radius accounting server's IP address.
- **Radius Accounting Port:** Enter the radius accounting server connection port number.

  Default: 1813 (This is a dedicated TCP/UDP port and typically should not be changed.)

- **Radius Accounting Secret:** Enter the radius accounting server's connection secret.

  Default: Blank

- **Interim Accounting Interval:** Enter a value for how often accounting data will be sent, in seconds. This value can be anywhere between 60-600 seconds.

  Default: 600 (10 minutes)

Click **Save** or **Cancel**.

Pro Tip: We recommend using WPA3-SAE Mixed. If you have a device that does not support this encryption type, use WPA2-PSK.

6. If you do not want the SSID to be visible in device lists, toggle **Broadcast SSID** off. This requires users to manually enter the SSID to connect.
7. If there are multiple APs in the project, toggle **Fast Roaming** on so that client devices can seamlessly switch between APs with the same SSID being broadcast. Read the below *Fast Roaming* section for more information about this feature.
8. Click **Save**, a the bottom of the page, then **Apply Changes** for the new SSID to be written to the AP's configuration.

Fast Roaming

This powerful feature, known in Araknis products as Fast Roaming, is essential for building reliable Wi-Fi networks with multiple access points. After a client joins a Wi-Fi network, they don't always stay close to the AP they originally connected to.

Without Fast Roaming, the client remains connected to one AP until signal is lost, then find a new connection. Fast Roaming tells the client when to move the connection, then makes the switch with minimal delay. This keeps clients on the fastest and most reliable AP at all times.

Installation Notes and Frequently Asked Questions

- **Can these new-generation X20 APs be used compatibly with the old gen (x00 and x10) APs?**

  No.

- **How do I configure the locations of APs for the best performance?**

  Use a site analyzer tool to determine ideal AP locations. For the best performance, use more APs closer together and reduce the transmit power some to avoid interference (Advanced Wireless Settings).

- **Does it matter what operating channel is used?**

  If you aren't using the Auto Operating Channel selection, use a different wireless radio channel in each AP to lower the amount of interference each device encounters.

- **How do I set up Guest Networks with Fast Roaming enabled?**

  The guest network feature is not ideal for use with Fast Roaming since each AP creates a new DHCP server for clients connected to that SSID. Instead, create a separate VLAN and assign SSIDs for guest use. See the knowledgebase article Araknis Access Point Guest SSID VLAN Setup for instructions.

- **Is this a proprietary technology for Araknis Networks?**

  No. Fast Roaming utilizes the standard IEEE 802.11r and 802.11k to negotiate hand-off with the client. Only clients that support 802.11r/k are able to perform best in this environment.

- **Do any other AP brands that support Hand-off work with Araknis Fast Roaming?**

  We don't guarantee compatibility with any other brands, but will list them if we find any that are.

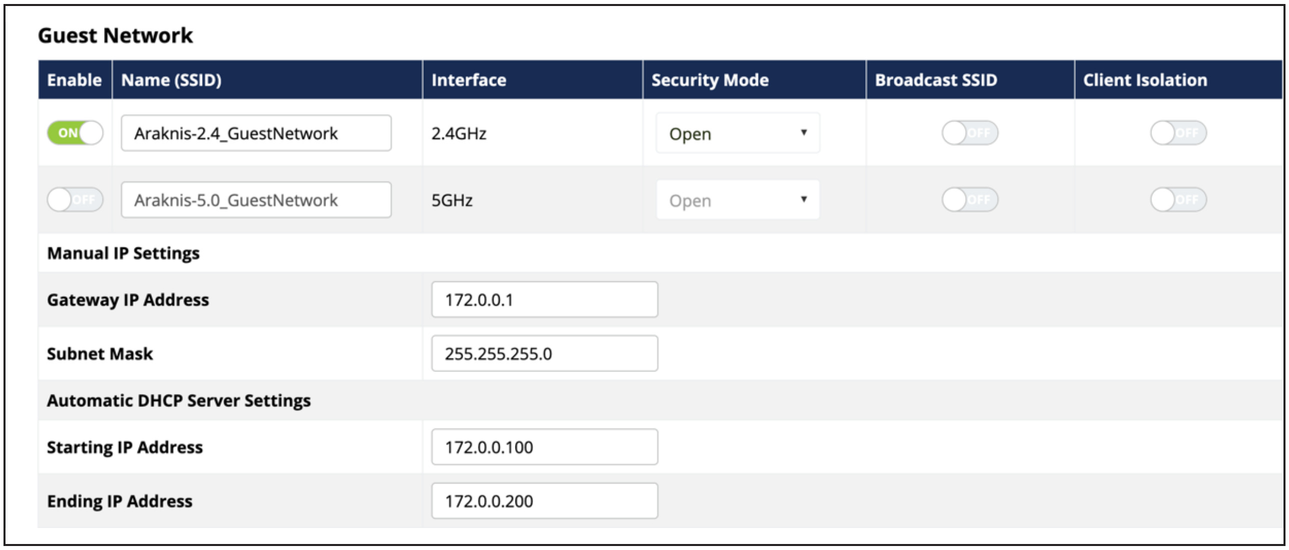
- **Does any equipment NOT work with Fast Roaming/Hand-off?**

  Gen 1 Apple iOS products, a number of IoT devices in the market, as well as certain printers - particularly older generation won't work. Most newer iOS devices work correctly.

Guest Network Configuration

Used to give guests limited wireless network access by using different security credentials and SSIDs.

Path: Settings > Wireless > Guest Network



Guest Network

Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation
ON	Araknis-2.4_GuestNetwork	2.4GHz	Open	OFF	OFF
OFF	Araknis-5.0_GuestNetwork	5GHz	Open	OFF	OFF

Manual IP Settings

Gateway IP Address	172.0.0.1
Subnet Mask	255.255.255.0

Automatic DHCP Server Settings

Starting IP Address	172.0.0.100
Ending IP Address	172.0.0.200

Configurable Settings

- **Enable:** Check the box to enable a guest network.

  Default: Disabled

- **Name (SSID):** Enter a name for the guest network.

  Default: Araknis-2.4_GuestNetwork

- **Interface:** Displays the wireless radio used for the guest network (2.4 or 5.0 GHz).

- **Security Mode:** Select a security mode for the SSID. guest networks are limited to Open, WPA2-PSK, WPA2-PSK Mixed, WPA3-SAE, and WPA3-SAE Mixed encryption modes.

  Default: Open

- **Broadcast SSID:** Select whether or not to publicly display the SSID to nearby Wi-Fi devices Default: Not selected
- **Channel Isolation:** Check the box to prevent communication between wireless clients on different SSIDs of the guest network.

  Default: Selected
- **Gateway IP Address:** Enter the guest network gateway IP address.

  Default: 192.168.200.1
- **Subnet Mask:** Enter the subnet mask for the guest network gateway.

  Default: 255.255.255.0
- **Starting IP Address:** Enter the lowest IP address available for the guest network.

  Default: 192.168.200.100
- **Ending IP Address:** Enter the highest IP address available for the guest network.

  Default: 192.168.200.200
- **WINS Server IP:** Enter the IP address for the WINS server for the guest network.

  Default: 0.0.0.0

Click **Save**, then **Apply Changes** when you're finished with the configuration.

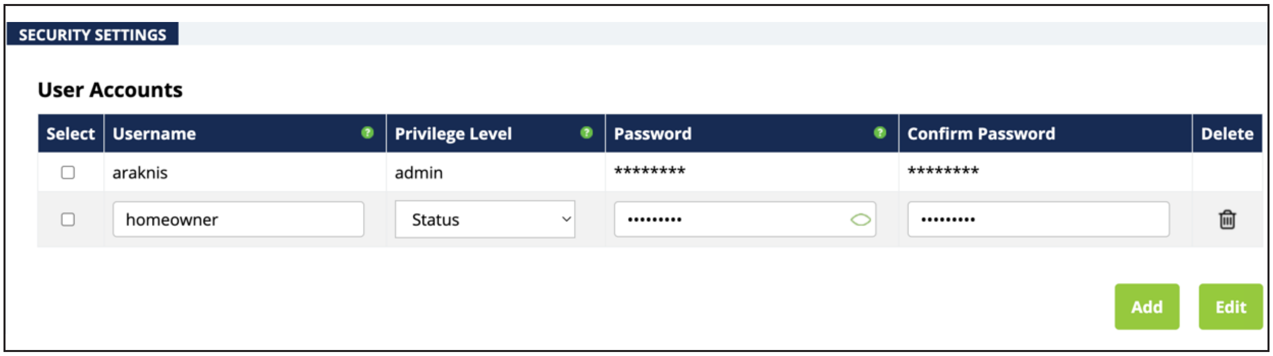
Pro Tip: If you're using guest networks across multiple APs we suggest you use VLANs. Read the knowledgebase article Araknis Access Point Guest SSID VLAN Setup for instructions.

Security Settings

User Accounts

Configure who can log into the access point and what level of privilege they have.

Path: Settings > Security > User Accounts



SECURITY SETTINGS

User Accounts

Select	Username	Privilege Level	Password	Confirm Password	Delete
□	araknis	admin	********	********	
□	homeowner	Status	•••••••••	•••••••••	🗑

Configurable Settings

- **Select:** Click to edit the selected table entry.

  Default: Not selected

- **Username:** Select the username, then click the Edit button to enter or change a username for logging into the access point. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.

  Default: araknis (Blank when adding a new account)

- **Privilege Level:** Select a privilege level of device management for the user. The first user is always the admin, which cannot be changed. New users can access the Status or Status+Settings.

  Default: Status+Settings when adding a new account)

- **Password**: Enter a new login password using letters, numbers, or punctuation. Limited to 32 characters, including spaces.

  Default: araknis (Blank when adding a new account)

- **Confirm Password:** Confirm the new login password by entering same password as above.

  Default: araknis (Blank when adding a new account)

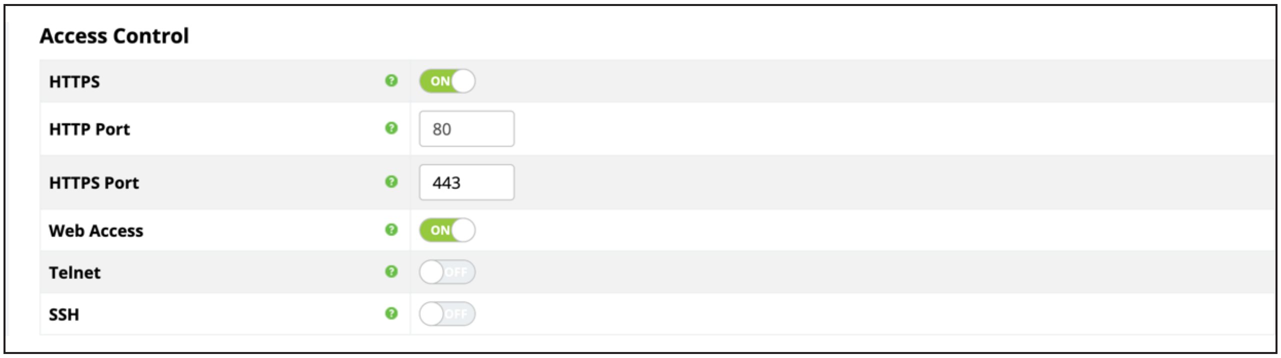
- **Delete:** Click the icon to delete a specific user account.
- **Add:** Click to add a new user account.
- **Edit:** Click the **Select** check box, in the left column of a user account, then click **Edit** to modify the account.

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Access Control

Configure how the access point's web interface can be accessed.

Path: Settings > Security > Access Control



Access Control

HTTPS	ON
HTTP Port	80
HTTPS Port	443
Web Access	ON
Telnet	OFF
SSH	OFF

Configurable Settings

- **HTTPS:** Toggle access to the AP using HTTP secure protocol.

  Default: On

Note: If you turn off HTTPS, clear your browser cache before trying to access the access point again. If you're using Mozilla Firefox, you may need to manually remove the "s" from the URL.

- **HTTP Port:** Enter the HTTP access port to connect to the AP.

  Default: 80

- **HTTPS Port:** Enter the HTTPS acces port to connect to the AP.

  Default: 443

Note: If you change the HTTP or HTTPS ports you must enter the port at the end of the URL. Example: 192.168.1.20:704

Pro Tip: If you're using port forwarding to access the AP remotely, assign a unique port number.

- **Web Access:** Select Enable or Disable to enable or disable the ability to modify the device via Web Browser.

  Default: On

Caution: Disabling web access causes loss of connection to the web interface. If this occurs, restoring the AP to the factory defaults by pressing the Reset button for more than 20 seconds. Let go when the LED flashes red.

- **Telnet:** Toggle the ability to use a telnet session to modify the device using the command line interface (CLI).

  Default: Off

- **SSH:** Toggle the ability to modify the device via a command line interface (CLI) using a secure channel.

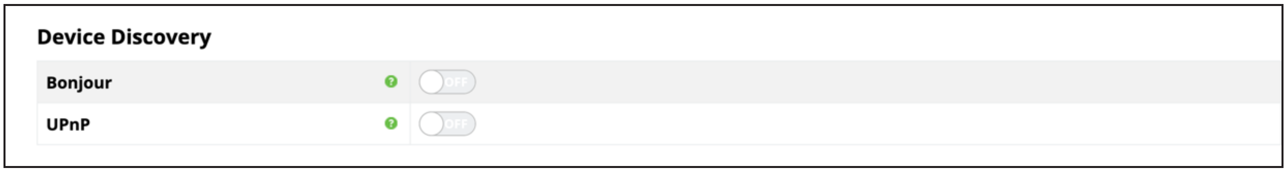
  Default: Off

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Device Discovery

Configure how or if the access point can search for and connect to network devices using Bonjour and/or UPnP.

Path: Settings > Security > Access Control



Device Discovery

Bonjour	OFF
UPnP	OFF

Configurable Settings

- **Bonjour:** Toggle on to allow the access point to search for and connect to network devices running Apple iOS and OS X. Bonjour can also be used on devices running a Microsoft OS.

  Default: Off

- **UPnP:** Toggle the ability to search for and connect to network devices using UPnP (Universal Plug and Play).

  Default: Off

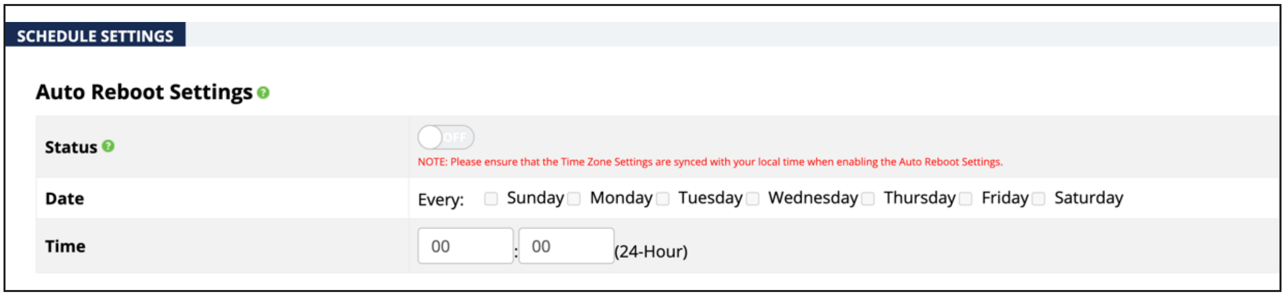
Click **Save**, then **Apply Changes** when you're finished with the configuration.

Schedule

Auto Reboot Settings

The AP can be set to reboot at specified times on a daily or weekly schedule. Rebooting the AP can improve network performance by keeping the system memory clear and ending unnecessary connections.

Path: Settings > Schedule > Auto Reboot Settings



SCHEDULE SETTINGS

Auto Reboot Settings

Status	OFF NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Auto Reboot Settings.
Date	Every: □ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday
Time	00 : 00 (24-Hour)

Configurable Settings

- **Status:** Toggle Auto Reboot on or off.

  Default: Off

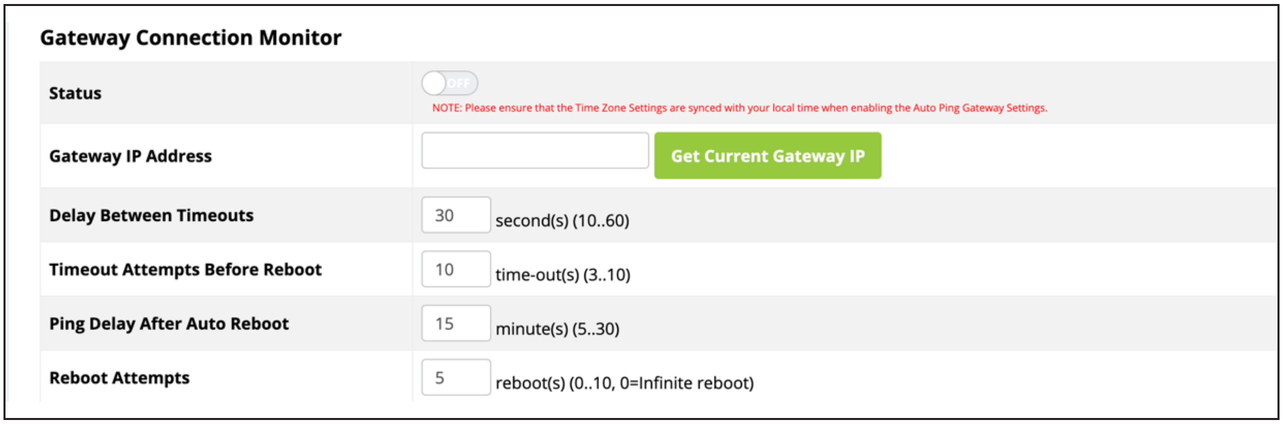
- **Date:** Check the boxes for the day(s) AP should reboot.
- **Time:** Enter the time for the reboot to take place in 24 hour format. (00:00=midnight; subtract 12 hours from 24 hour time for standard time 17:00-12:00=5:00pm)

Click **Save**, then **Apply Changes** when you’re finished with the configuration.

Gateway Connection Monitor

Configures the AP to ping the gateway, and if the ping results fall outside the desired settings, restart the AP.

Path: Settings > Schedule > Gateway Connection Monitor



Gateway Connection Monitor

Status	OFF NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Auto Ping Gateway Settings.
Gateway IP Address	Get Current Gateway IP
Delay Between Timeouts	30 second(s) (10..60)
Timeout Attempts Before Reboot	10 time-out(s) (3..10)
Ping Delay After Auto Reboot	15 minute(s) (5..30)
Reboot Attempts	5 reboot(s) (0..10, 0=Infinite reboot)

Configurable Settings

- **Status:** Toggle Auto Reboot on or off.

  Default: Off

- **Gateway IP Address:** Enter the gateway IP address to be pinged, usually the router.

- **Delay Between Timeouts:** Enter how many seconds the AP waits to try a new ping after a timeout.

  Default: 30 seconds

- **Timeout Attempts Before Reboot:** Enter how the number of timeouts that must occur before rebootoing the AP.

  Default: 10

- **Ping Delay After Auto Reboot:** Enter how many minutes before the AP pings again after it reboots.

  Default: 15 minutes

- **Reboot Attempts:** Enter the number of reboots before the AP stops monitoring the gateway.

  Default: 5

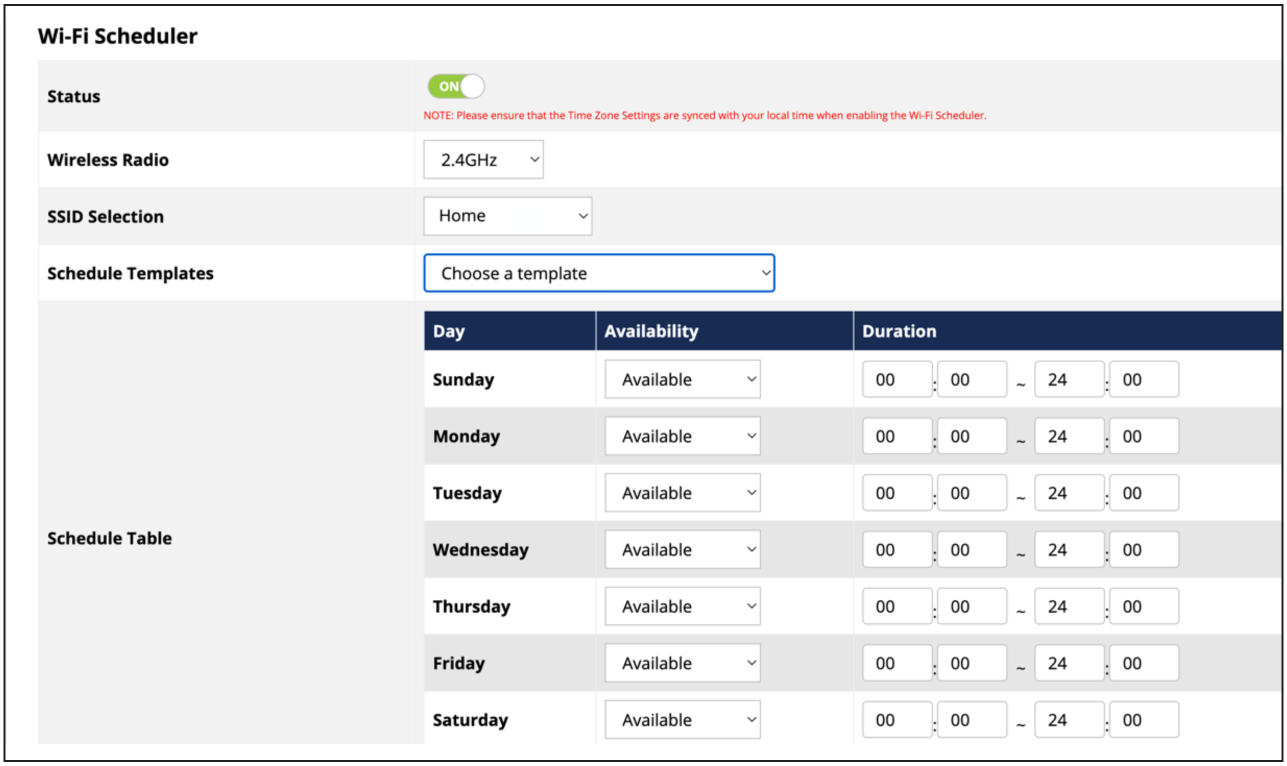
Click **Save**, then **Apply Changes** when you're finished with the configuration.

Wi-Fi Scheduler

The Wi-Fi Scheduler is used to configure when wireless networks are available for use.

The scheduler is based on a 24-hour clock (00:00 = 12:00AM, the start of a given day)

Path: Settings > Schedule > Wi-Fi Scheduler.



Wi-Fi Scheduler

Status	ON NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Wi-Fi Scheduler.
Wireless Radio	2.4GHz
SSID Selection	Home
Schedule Templates	Choose a template
Schedule Table	

Day	Availability	Duration
Sunday	Available	00 : 00 ~ 24 : 00
Monday	Available	00 : 00 ~ 24 : 00
Tuesday	Available	00 : 00 ~ 24 : 00
Wednesday	Available	00 : 00 ~ 24 : 00
Thursday	Available	00 : 00 ~ 24 : 00
Friday	Available	00 : 00 ~ 24 : 00
Saturday	Available	00 : 00 ~ 24 : 00

Configurable Settings

- **Status:** Toggle the Wi-Fi Scheduler on or off.

  Default: Off

- **Wireless Radio:** Select the 2.4GHz or 5GHz radio interface to be scheduled.

  Default: 2.4GHz.

- **SSID Selection:** Select one of the below templates:

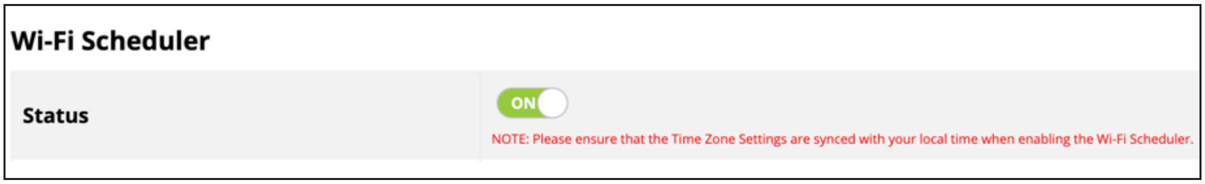
- **Schedule Templates:** Create different Wi-Fi schedules using the templates detailed below:
    - **Always Available:** The wireless network is always on. 00:00-24:00.
    - **Available 8-17 Daily:** 08:00-17:00. The wireless network is on at 8:00AM and off at 5:00PM.
    - **Available 8-17 Daily Except Weekends:** 08:00-17:00. The wireless network is on at 8:00AM and off at 5:00PM Monday-Friday and always off on Saturday and Sunday.
    - **Custom Schedule:** Allows custom configuration of the Wi-Fi Schedule using the Schedule Table settings.
- **Day:** The day of the week being configured.
- **Availability:** Select whether the device is Available for the set duration, or Unavailable for the specified day.
- **Duration:** The time the schedule starts and ends, using the 24 hour format. 00:00 = midnight. Subtract 12 hours from 24 hour time to get the standard time. For example: 17:00-12:00 = 5:00PM.

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Wi-Fi Scheduler Configuration Example

In this example, the 2.4GHz SSID, **Market 2**, needs to be available during the hours of 8AM to 6PM Monday through Friday, 10AM to 5PM on Saturdays, and unavailable the rest of the week.

1. Toggle the **Status** to on.

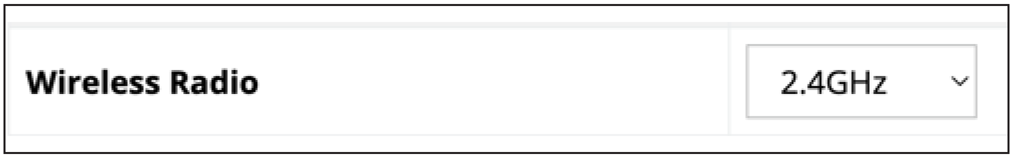


Wi-Fi Scheduler

Status: ON

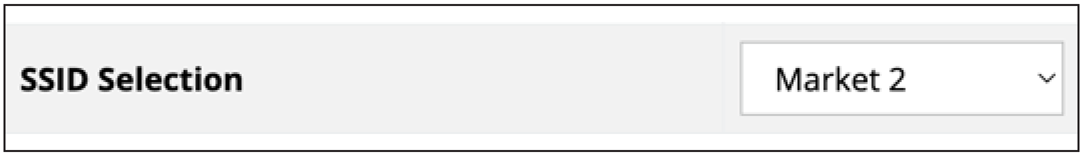
NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Wi-Fi Scheduler.

2. Use the **Wireless Radio** drop-down to select the **2.4GHz** radio.



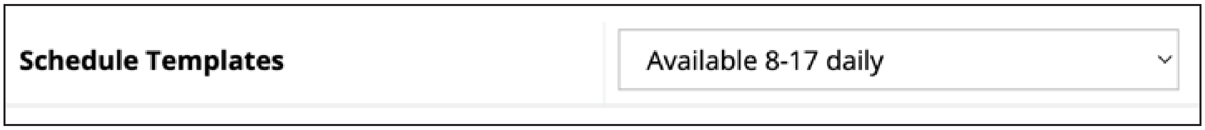
Wireless Radio	2.4GHz

3. Use the **SSID Selection** drop-down to select the previously created, **Market 2**, SSID.



SSID Selection	Market 2

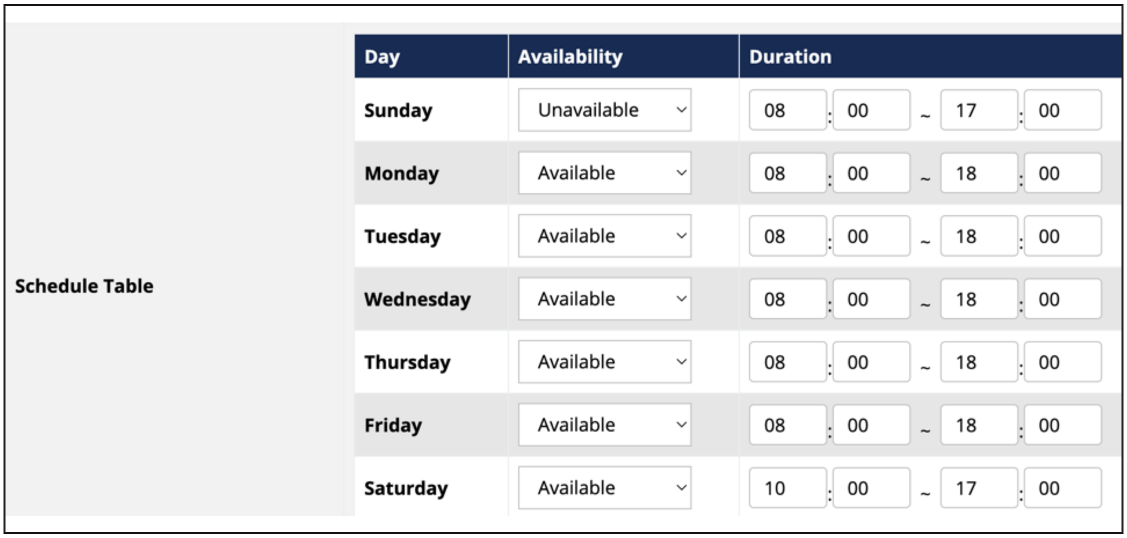
4. Select an option from the **Schedule Templates** drop-down. In this example, select **Available 8-17 Daily**, since this template is closest to the schedule needed.



Schedule Templates	Available 8-17 daily

5. Modify the **Schedule Table** to work on the desired schedule. In this example, the following changes:

- Sunday: Set to **Unavailable** so that no access is available the entire day.
- Monday-Friday: Modify the duration to **08:00 – 18:00** (8AM-6PM)
- Saturday: Modify the duration to **10:00 – 17:00** (10AM-5PM)



Schedule Table

Day	Availability	Duration
Sunday	Unavailable	08 : 00 ~ 17 : 00
Monday	Available	08 : 00 ~ 18 : 00
Tuesday	Available	08 : 00 ~ 18 : 00
Wednesday	Available	08 : 00 ~ 18 : 00
Thursday	Available	08 : 00 ~ 18 : 00
Friday	Available	08 : 00 ~ 18 : 00
Saturday	Available	10 : 00 ~ 17 : 00

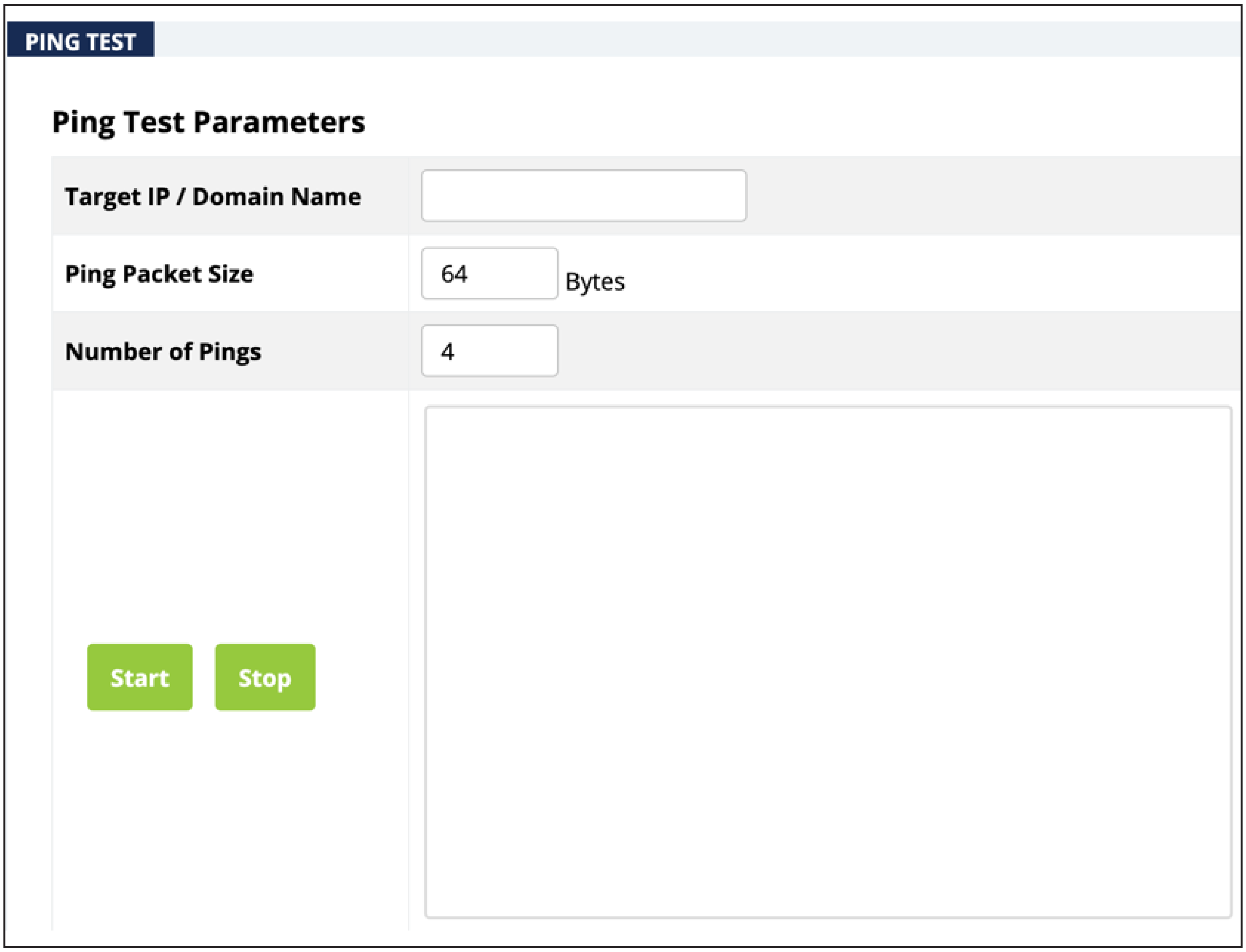
6. Click **Save**, then **Apply Changes** when you’re finished with the configuration.

Maintenance

Ping Test

Use a ping test to determine whether a particular IP address can be reached.

Path: Maintenance > Ping



PING TEST

Ping Test Parameters

Target IP / Domain Name	
Ping Packet Size	64 Bytes
Number of Pings	4

How to Run a Ping Test

1. Enter the **Target IP address** or **Domain Name** of the device or web page you want to communicate with.

2. Enter the **Ping Packet Size** for the test. The maximum size allowed is 65535 bytes.

   Default: 64 bytes.

3. Enter the **Number of Pings** you want the test to run.

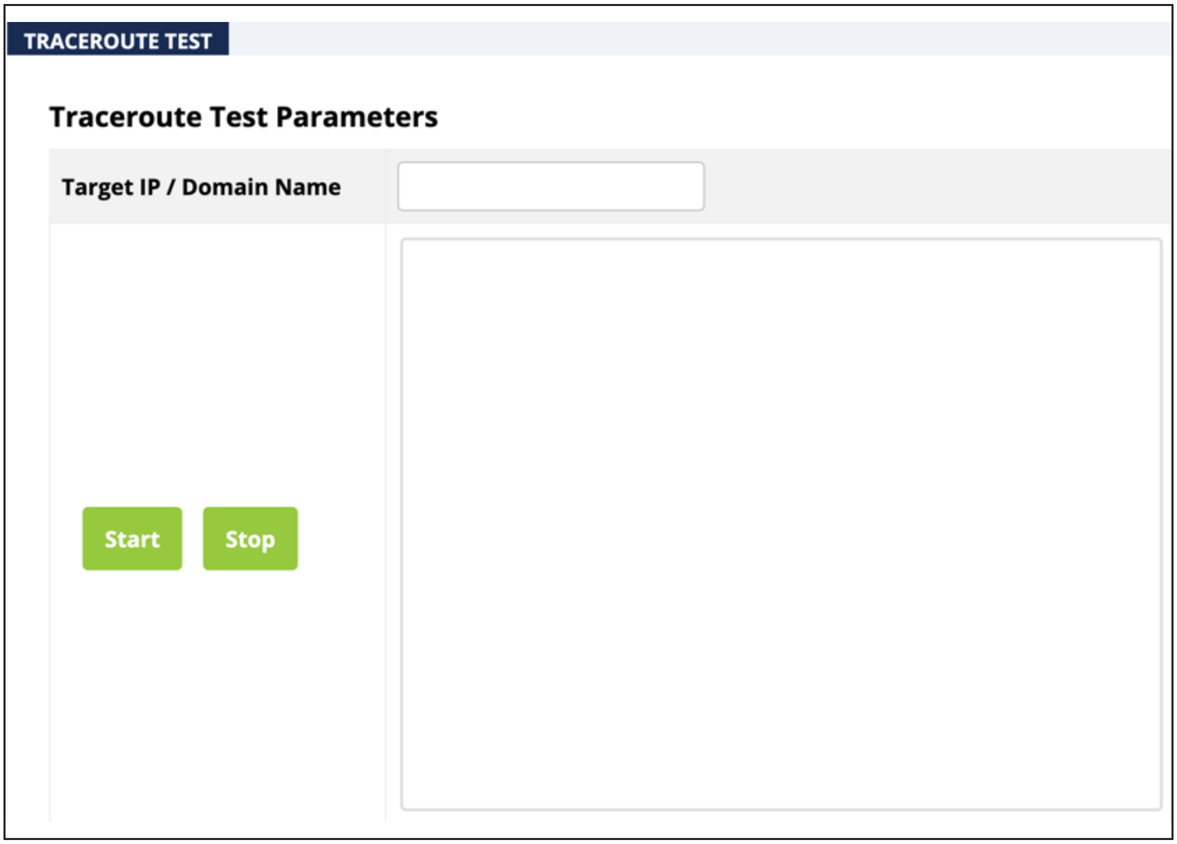
   Default: 4

4. Click the **Start** button to start the test. Click **Stop** to manually end the test.

Traceroute Test

Traceroutes display the route and delay time for data packets to/from a destination on the network.

Path: Maintenance > Traceroute



How to Run a Traceroute Test

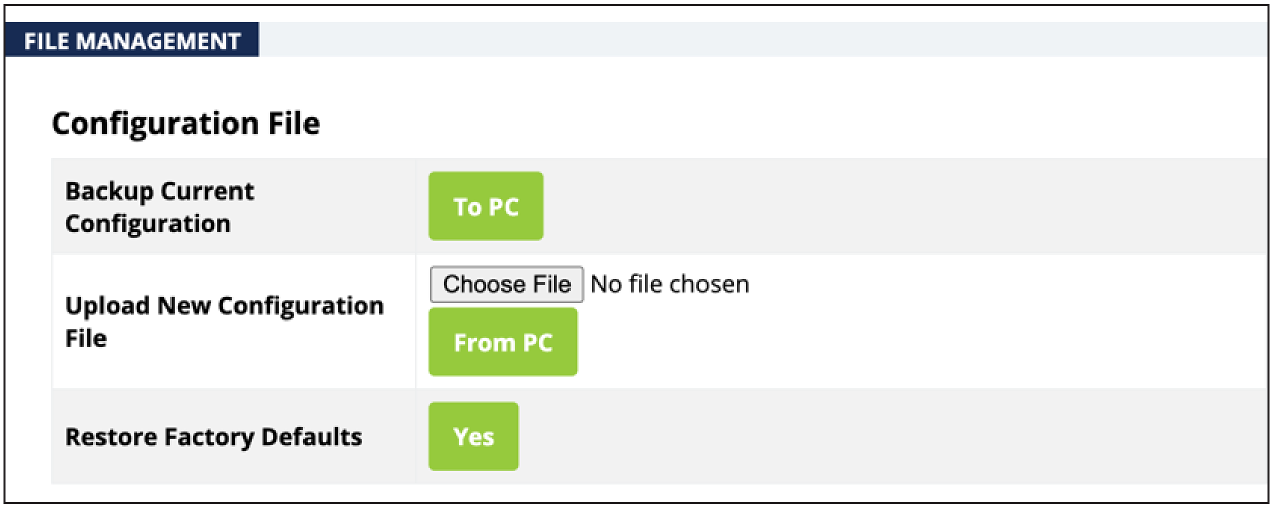
1. Enter the **Target IP address** or **Domain Name** of the device or web page that you want to see the network path used to communicate.
2. Click the **Start** button to see the test results in the text field on the right. You can click the **Stop** button to manually end the test.

File Management

Use the File Management page to back up or restore settings and apply firmware updates.

Configuration File

Path: Maintenance > File Management > Configuration File



FILE MANAGEMENT

Configuration File

Backup Current Configuration	To PC
Upload New Configuration File	Choose File No file chosen From PC
Restore Factory Defaults	Yes

How to Back Up the Configuration

1. Click the **To PC** button and select a location to save the file.
2. Give the file a meaningful name and save it to your computer.

How to Upload a Configuration File

1. Click the **Choose File** button and select a configuration file (.tar file) saved to your computer. The file name appears to the right of the Choose File button.

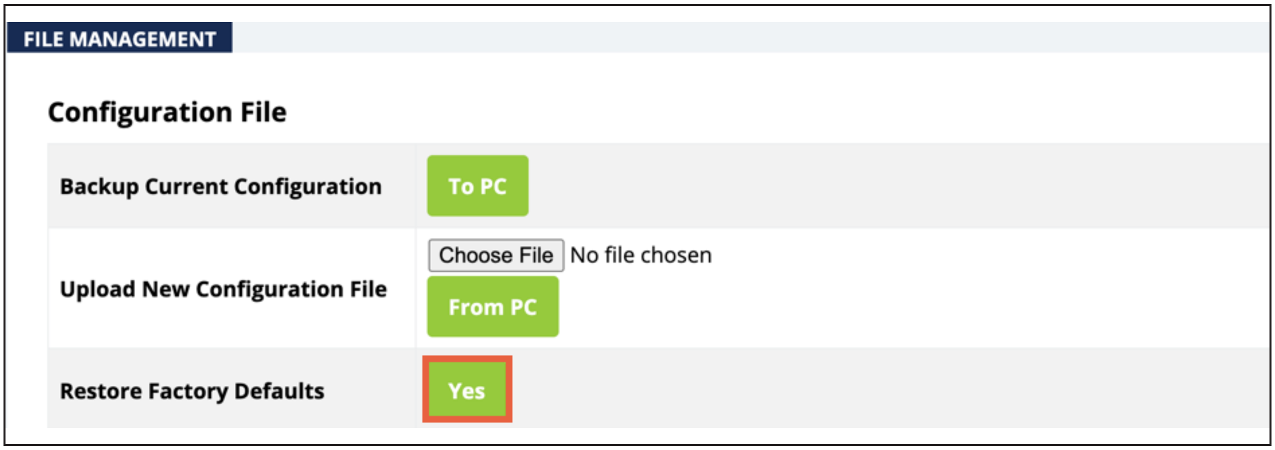
2. Click the **From PC** button to upload the configuration file. You'll see a loading page as the configuration is applied to the AP. When complete, the Araknis login page appears.

3. Log in and confirm the configuration settings were applied properly.

How to Factory Default the Access Point

Use the File Management page to restore the factory default settings.

Path: Maintenance > File Management > Configuration File



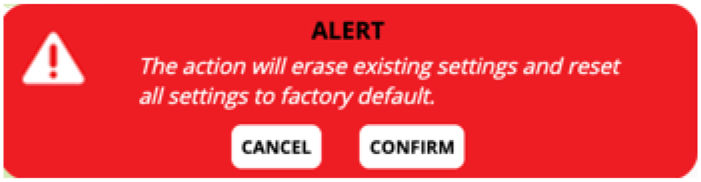
FILE MANAGEMENT

Configuration File

Backup Current Configuration	To PC
Upload New Configuration File	Choose File No file chosen From PC
Restore Factory Defaults	Yes

Caution: All of the current settings will be permanently lost if they're not backed up.

1. Click the **Yes** button to restore the access point to factory default settings, which opens a red alert message.



ALERT

The action will erase existing settings and reset all settings to factory default.

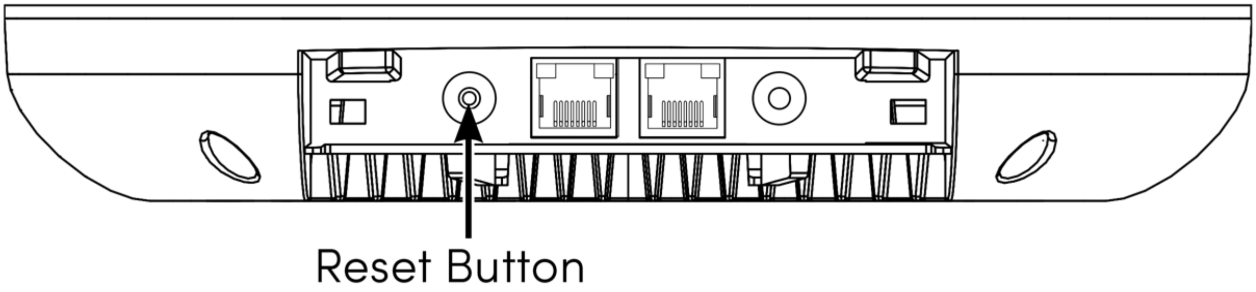
2. Click **Confirm** to restore factory defaults. A loading page pops up while the AP restores the factory defaults. When complete, the login window appears.

3. Enter the default username and password. (araknis; araknis) and configure the AP like new, or upload a configuration file.

How to Perform a Hardware Factory Default

Press and hold the Reset button for more than 20 seconds. Release the button when the LED blinks red.

Allow two to four minutes for the AP to restart and load the factory default settings, then log into the AP using the default username and password (araknis; araknis) and configure the AP like new, or upload a configuration file.



Reset Button Action	LED State	Description
Hold the reset button for 1-9 seconds	Blinking Green	Restarts the AP
Hold the reset button for 10-19 seconds*	Blinking Orange	Only resets the username and password
Hold the reset button for more than 20 seconds	Blinking Red	Resets the AP to factory defaults

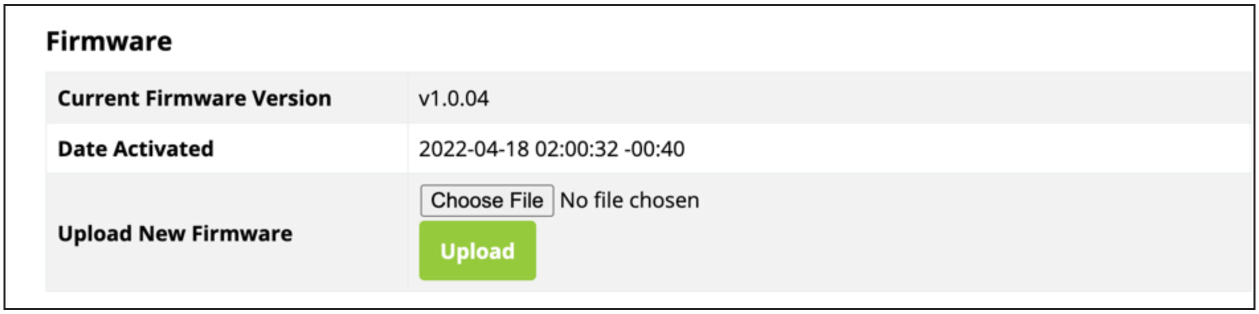
*This action is only available when the Reset Password toggle is disabled in the web interface.

How to Manually Update the Firmware

The Firmware menu shows the Current Firmware Version and the date it was installed (Date Activated.)

Path: Maintenance > File Management > Firmware

1. Download the firmware file from the product page and save it in an easy to find location on your computer.
2. Click **Choose File** and select the firmware file you saved to your computer. The firmware file's name appears next to the Choose File button.
3. Click **Upload** and wait for the loading bar to complete,then click the **Upgrade** button. A new window appears with a countdown (in seconds) as to when the AP will be available again. Once complete, the login window appears.
4. Enter the username and password, then navigate to **Maintenance** > **File Management** > **Firmware** and confirm the new firmware version.

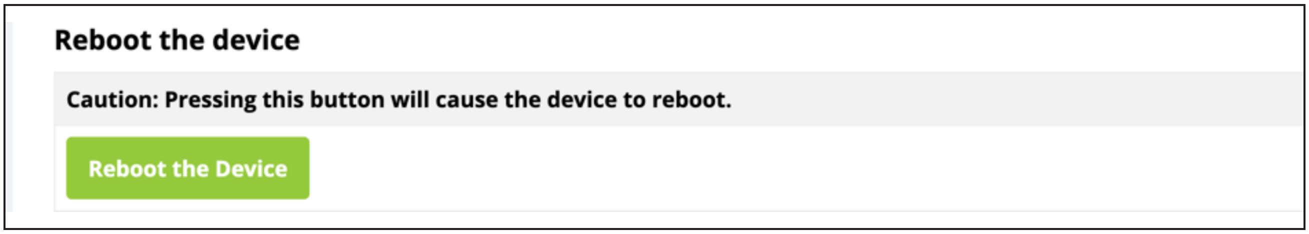


Firmware

Current Firmware Version	v1.0.04
Date Activated	2022-04-18 02:00:32 -00:40
Upload New Firmware	Choose File No file chosen Upload

Restarting the AP

Path: Maintenance > Restart



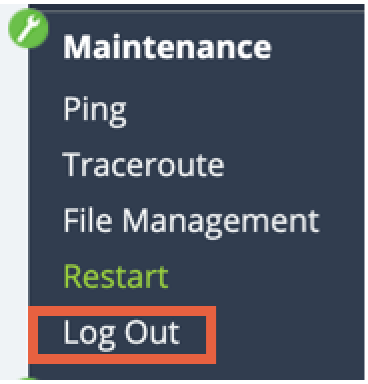
Reboot the device

Caution: Pressing this button will cause the device to reboot.

Click the **Reboot the Device** button. You'll get a confirmation message and be presented with the login screen when the AP restarts.

Logging Out of the AP

Path: Maintenance > Logout



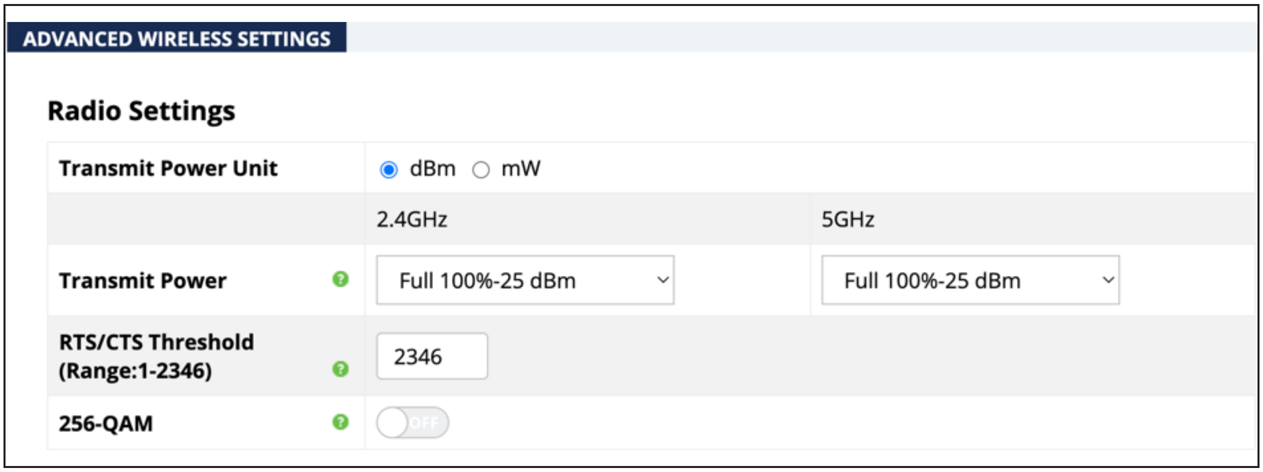
Log out of the AP to change the user currently logged in.

Advanced Wireless Settings

Radio Settings

Configure the transmit power for the radio interfaces,unit of measurement, RTS/CTS Threshold, and 256-QAM.

Path: Advanced > Wireless Settings > Radio Settings



ADVANCED WIRELESS SETTINGS

Radio Settings

Transmit Power Unit	● dBm ○ mW	
	2.4GHz	5GHz
Transmit Power	Full 100%-25 dBm	Full 100%-25 dBm
RTS/CTS Threshold (Range:1-2346)	2346	
256-QAM	OFF	

Configurable Settings

- **Transmit Power Unit:** Select the preferred unit of measure. dBm or mW.

  Default: dBm.

- **Transmit Power:** Select a setting from the drop-down to set the radio power. Higher power improves performance but can cause interference with other access points in close range on the same channel.

  A higher coverage range also corresponds with lower throughput (i.e. to achieve the highest transmit power, the connection must run at the lowest data rate). Set this value as low as possible (for adequate coverage) to get the maximum wireless speed/data throughput.

Values are in dBm or mW, based on the Transmit Power Unit setting.

Default: Full 100%-25 dBm

- **RTS/CTS Threshold (Range: 1-2346):** Enter a value for the threshold package size for RTS/CTS (request to send/clear to send). A lower number increases the frequency that the packets are sent and consumes more bandwidth.

  Default: 2346

- **256-QAM:** Can be toggled on to improve throughput performance on 2.4GHz band, but only fo compatible client devices.

  Default: Off

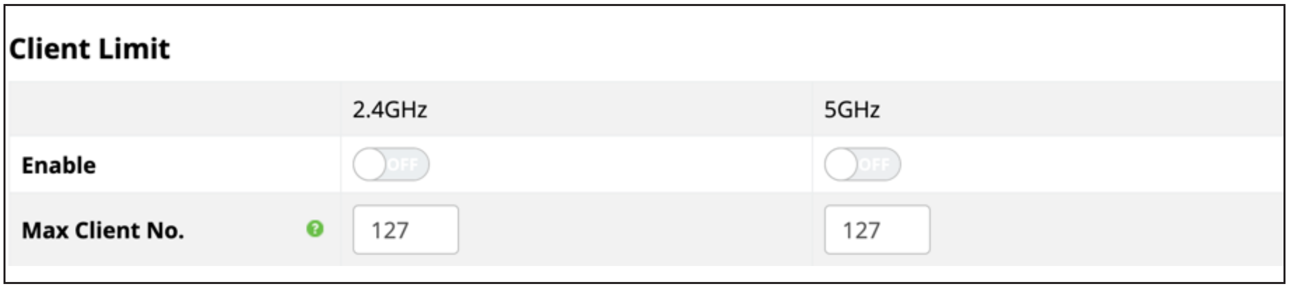
Pro Tip: Do not toggle 256-QAM on unless you have a specific use case.

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Client Limit

Configure the maximum amount of client devices that can connect to individual radio interfaces.

Path: Advanced > Wireless Settings > Client Limit



Client Limit

	2.4GHz	5GHz
Enable	OFF	OFF
Max Client No.	127	127

Configurable Settings

- **Enable:** Toggle on to enforce a Client Limit, by channel.

  Default: Off.

- **Max Client No.:** Set the maximum number of clients (between 1 and 127) that can be connected to a channel at a given time.

  Default: 127.

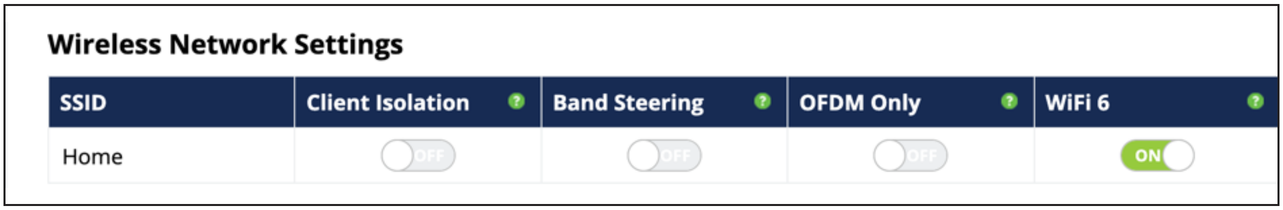
Pro Tip: We recommend a network design that allows each access point to handle 30 client devices at any given time.

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Wireless Network Settings

Turn on more advanced features for specific SSIDs.

Path: Advanced > Wireless Settings > Wireless Network Settings



Wireless Network Settings

SSID	Client Isolation	Band Steering	OFDM Only	WiFi 6
Home	OFF	OFF	OFF	ON

Configurable Settings

- **Client Isolation:** Toggle on to prevent client devices connected to this SSID from communicating to client devices connected to a different SSID.
- **Band Steering:** Toggle on to help move client devices to the radio interface with the strongest signal. Connected devices can still move between 2.4GHz and 5GHz channels, but the device must choose when to do so.

Note: Band Steering can only be turned on for SSIDs set to Both channels.

- **OFDM Only:** Turn OFDM (Orthogonal Frequency Division Multiplexing) on to prevent 2.4GHz legacy 802.11b devices from connecting to the SSID. OFDM disables CCK (Complimentary Code Keying) rates of 1, 2, 5.5, and 11 and provides maximum throughput for 802.11 g devices.

Note: OFDM Only can only be turned on if the SSID is set to Both or the 2.4GHz Wireless Mode is configured for B/G/N, B/G, or AX.

- **WiFi6:** Turn this feature off to allow incompatible Wi-Fi 5 devices to connect to the SSID. Wi-Fi 6 devices cannot use OFDMA and Target Wake Time (TWT).

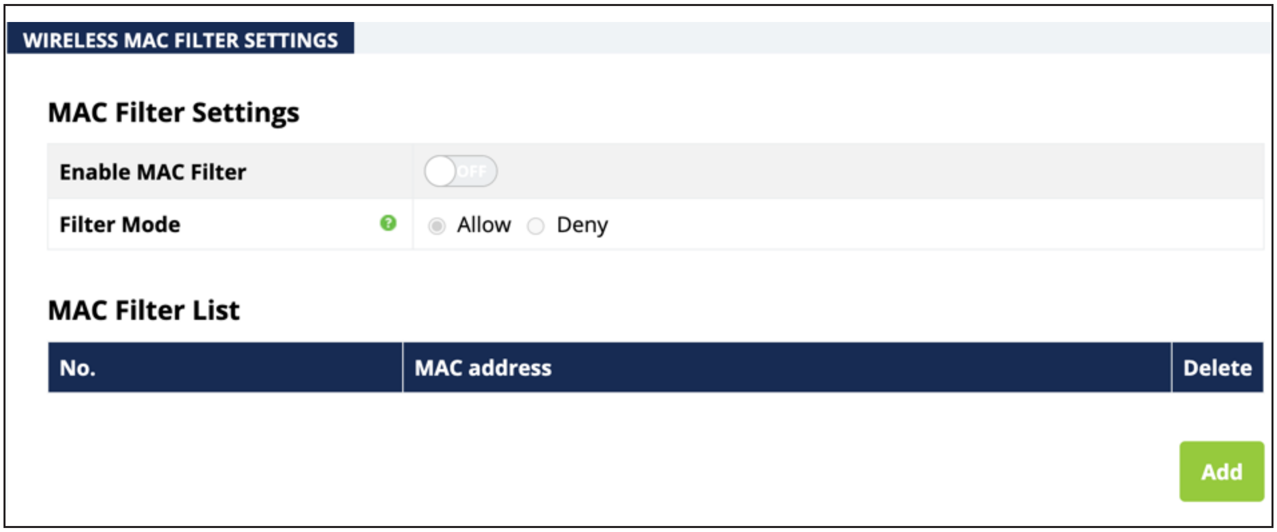
Note: WiFi6 can only be turned on if the interface mode is set to AX.

Click **Save**, then **Apply Changes** when you're finished with the configuration.

Wireless MAC Filter Settings

The Wireless MAC Filter determines if wireless client devices can access the wireless network by entering their MAC address in the filter list.

Path: Advanced > MAC Filter > MAC Filter Settings



WIRELESS MAC FILTER SETTINGS

MAC Filter Settings

Enable MAC Filter	OFF
Filter Mode	● Allow ○ Deny

MAC Filter List

No.	MAC address	Delete

How to Configure the Mac Filter

1. Toggle **Enable MAC Filter** to on.
2. Set the **Filter Mode** to Allow or Deny. Each selection populates a different list.

Selecting **Allow** shows the list of MAC addresses that can connect to the access point.

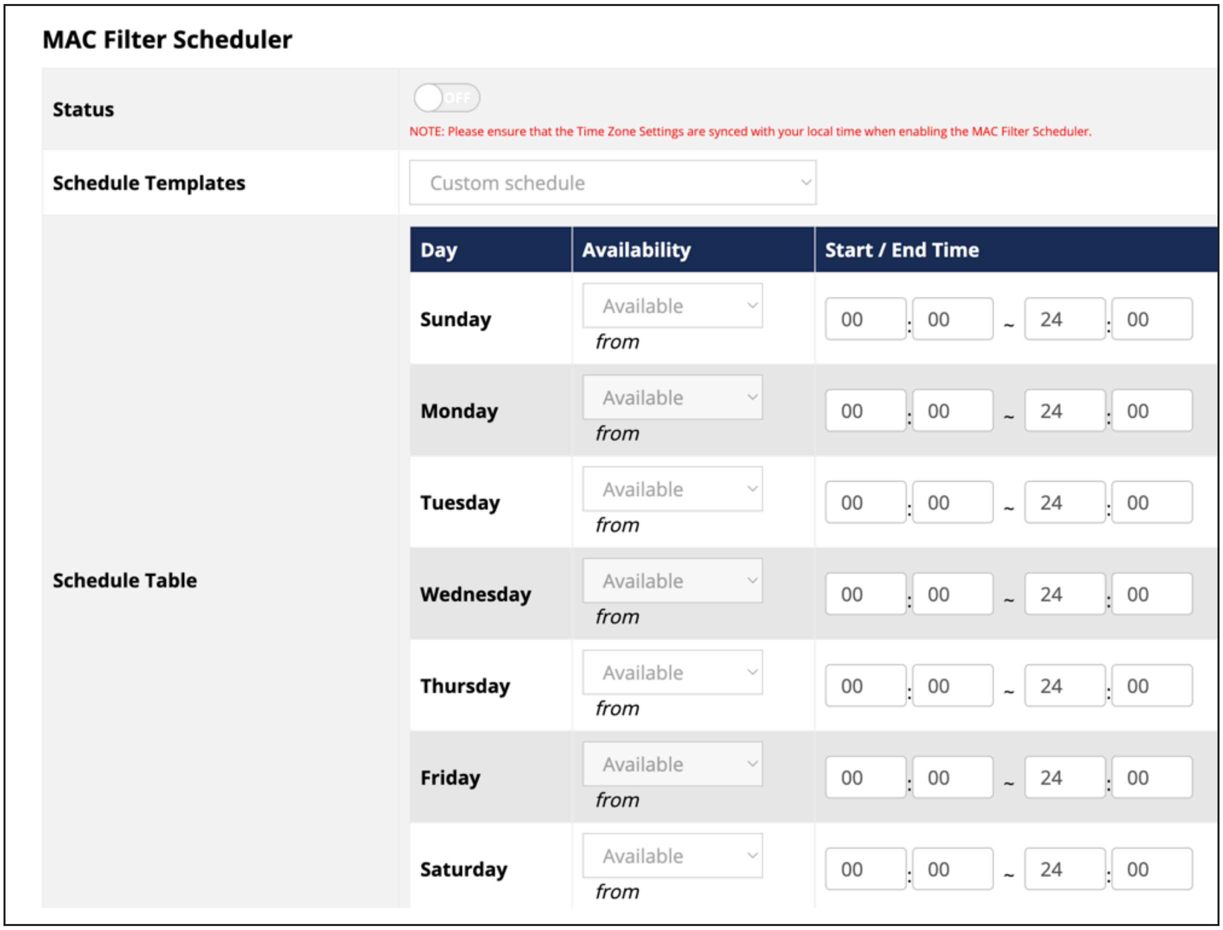
Selecting **Deny** shows the list of MAC addresses that cannot connect to the access point.

3. Click the **Add** button to add a MAC address to the list. If you've made a mistake, you can Delete the entry.
4. Click **Save**, then **Apply Changes** when you're finished with the configuration.

MAC Filter Scheduler

Use the MAC Filter Scheduler to only enforce the MAC filter during specific times.

Path: Advanced > MAC Filter > MAC Filter Scheduler



MAC Filter Scheduler

Status	OFF NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the MAC Filter Scheduler.
Schedule Templates	Custom schedule
Schedule Table	

Day	Availability	Start / End Time
Sunday	Available *from*	00 : 00 ~ 24 : 00
Monday	Available *from*	00 : 00 ~ 24 : 00
Tuesday	Available *from*	00 : 00 ~ 24 : 00
Wednesday	Available *from*	00 : 00 ~ 24 : 00
Thursday	Available *from*	00 : 00 ~ 24 : 00
Friday	Available *from*	00 : 00 ~ 24 : 00
Saturday	Available *from*	00 : 00 ~ 24 : 00

How to Configure the MAC Filter Scheduler

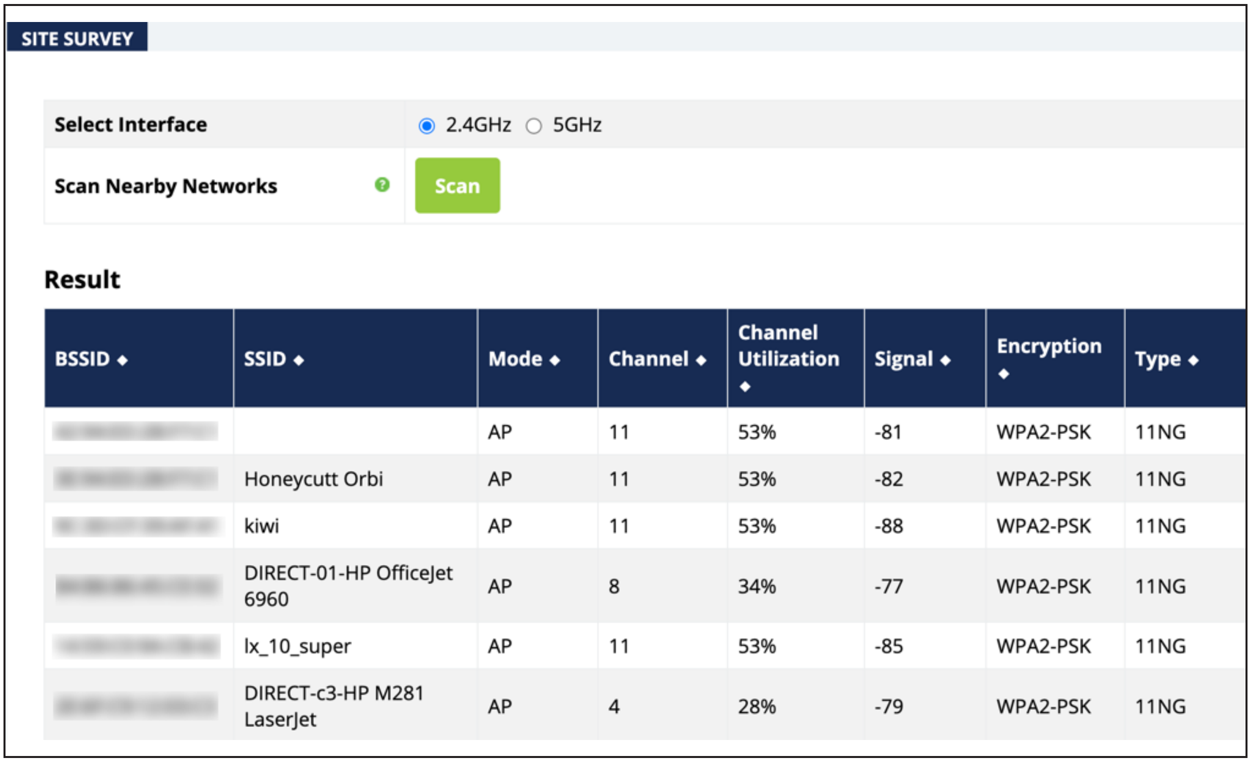
1. Toggle the **Status** to On.
2. Use the **Schedule Templates** to select one of the templates detailed below:
   - **Always Available:** The MAC Filter is always on. 00:00-24:00.
   - **Available 8-17 Daily:** 08:00-17:00. The MAC Filter is on at 8:00AM and off at 5:00PM.
   - **Available 8-17 Daily Except Weekends:** 08:00-17:00. The MAC filter is on at 8:00AM and off at 5:00PM Monday-Friday and always off on Saturday and Sunday.
   - **Custom Schedule:** Select to manually configure each day and time of the MAC Filter Schedule, using the Schedule Table settings.
3. To modify the template, use the **Availability** drop-down, next to the Day, to select whether the MAC Filter is Available (on) for the set duration, or Unavailable (off) for the specified day.
4. Enter or modify the **Start** and **End Time**, using the 24 hour format. 00:00 = midnight. Subtract 12 hours from 24 hour time to get the standard time. For example: 17:00-12:00 = 5:00PM.
5. Click **Save**, then **Apply Changes** when you're finished with the configuration.

Site Survey

The access point provides a convenient on-board Wi-Fi detection tool commonly known as a Wi-Fi sniffer that can be used to detect the presence of other 2.4GHz and 5GHz wireless networks.

The Site Survey displays the modes, channels, security settings, signal strengths, encryptions, and types can be identified. Use this information during setup to avoid conflicts with other wireless networks in the surrounding area.

Path: Advanced > Site Survey



SITE SURVEY

Select Interface	● 2.4GHz ○ 5GHz
Scan Nearby Networks	Scan

Result

BSSID ◆	SSID ◆	Mode ◆	Channel ◆	Channel Utilization ◆	Signal ◆	Encryption ◆	Type ◆
[redacted]		AP	11	53%	-81	WPA2-PSK	11NG
[redacted]	Honeycutt Orbi	AP	11	53%	-82	WPA2-PSK	11NG
[redacted]	kiwi	AP	11	53%	-88	WPA2-PSK	11NG
[redacted]	DIRECT-01-HP OfficeJet 6960	AP	8	34%	-77	WPA2-PSK	11NG
[redacted]	lx_10_super	AP	11	53%	-85	WPA2-PSK	11NG
[redacted]	DIRECT-c3-HP M281 LaserJet	AP	4	28%	-79	WPA2-PSK	11NG

How to Perform a Site Survey

To perform a Site Survey, select the radio Interface to scan for, then click **Scan**.

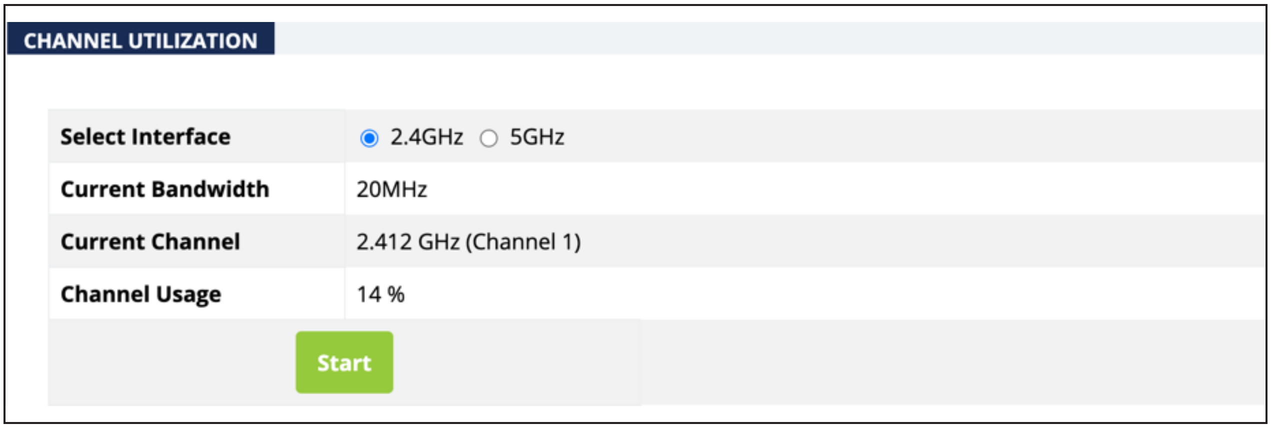
Reading the Results

- **BSSID:** Basic Service Set Identification. Indicates the MAC address of a detected 2.4GHz or 5GHz neighboring wireless device.
- **SSID:** Service Set Identifier. Indicates the network name of a wireless network that a specific device is connected to.
- **Mode:** Indicates if the detected device is being used as an AP or repeater.
- **Channel:** Indicates the channel a specific device is transmitting on.
- **Channel Utilization:** Indicates how much 802.11 traffic the AP is measuring from the device.The percentage is the amount of time the device keeps the channel busy.
- **Signal:** Displays the signal strength of the detected wireless signal perceived by the AP. Measured in RSSI (Received Signal Strength Indicator).
- **Encryption:** Indicates the security mode encryption of the detected device.
- **Type:** Indicates the wireless mode of the detected device.

Channel Utilization

Use the Channel Utilization tool to measure how much 802.11 traffic the AP is measuring in the surrounding area. The higher the percentage, the busier the channel is. A high percentage means it is difficult to communicate on the channel being scanned.

Path: Advanced > Channel Utilization



CHANNEL UTILIZATION

Select Interface	● 2.4GHz ○ 5GHz
Current Bandwidth	20MHz
Current Channel	2.412 GHz (Channel 1)
Channel Usage	14 %

How to Scan for Channel Utilization

Select a radio Interface, then click the **Start** button.

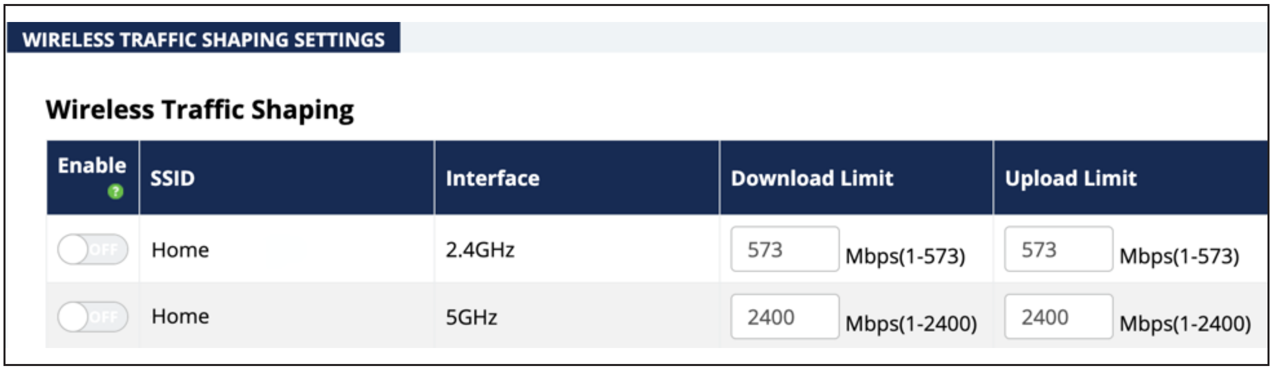
Reading the Results

- **Current Bandwidth:** Indicates the channel bandwidth of the selected radio interface.
- **Current Channel:** Indicates the radio interface selected, and the channel the AP is using.
- **Channel Usage:** Displays the current channel utilization.

Wireless Traffic Shaping

Use traffic shaping to set upload and download limits for specific SSIDs and their radio broadcasts to wireless network saturation and reduce latency.

Path: Advanced > Traffic Shaping



WIRELESS TRAFFIC SHAPING SETTINGS

Wireless Traffic Shaping

Enable	SSID	Interface	Download Limit	Upload Limit
OFF	Home	2.4GHz	573 Mbps(1-573)	573 Mbps(1-573)
OFF	Home	5GHz	2400 Mbps(1-2400)	2400 Mbps(1-2400)

Wireless Traffic Shaping Configuration

1. Toggle the **Enable** switch to On for the SSID and wireless interface you want to impose a limit on.
2. Enter a **Download Limit**, in Mbps, between 1-573 for 2.4GHz interfaces and 1-2400 for 5Ghz.
3. Enter an **Upload Limit**, in Mbps, between 1-573 for 2.4GHz interfaces and 1-2400 for 5Ghz.
4. Click **Save**, then **Apply Changes** when you're finished with the configuration.

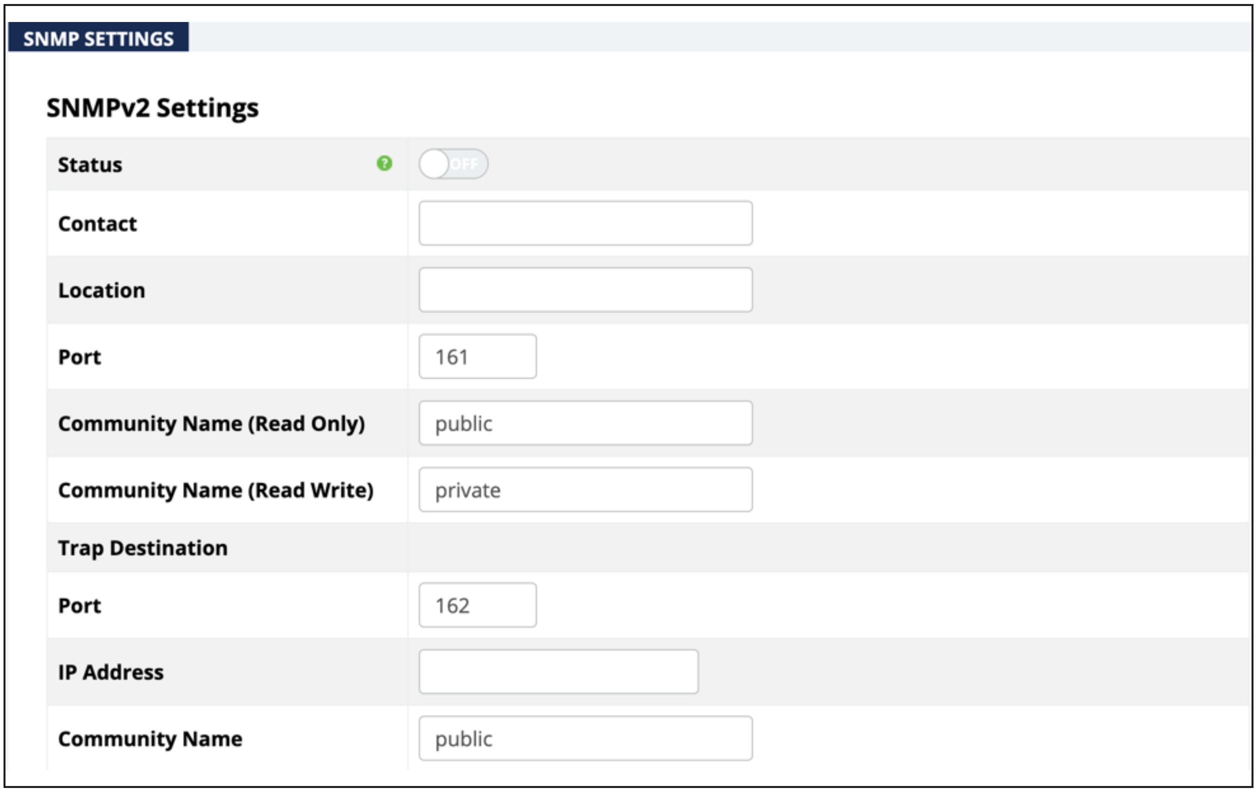
SNMP

Simple Network Management Protocol (SNMP) is an IP network protocol used to monitor network devices, audit network usage, detect network faults or inappropriate access, and, configure remote devices.

SNMPv2 Settings

Note: Refer to the SNMP server documentation while configuring these settings.

Path: Advanced > SNMP > SNMPv2



SNMP SETTINGS

SNMPv2 Settings

Status	OFF
Contact	
Location	
Port	161
Community Name (Read Only)	public
Community Name (Read Write)	private
Trap Destination	
Port	162
IP Address	
Community Name	public

Configurable Settings

- **Status:** Toggle on or off.

  Default: Off

- **Contact:** Enter the name of the person managing the SNMPv2 server.

  Default: Blank

- **Location:** Enter the physical location of the SNMPv2 server.

  Default: Blank

- **Port:** Enter the port number for SNMPv2 ‘listening’.

  Default: 161 (This is a dedicated TCP/UDP port and typically should not be changed.)

- **Community Name (Read Only):** Enter the password for SNMPv2 read only access.

  Default: Public. ‘Public’ is a typical default of SNMP v2 devices for Read Only.

- **Community Name (Read Write):** Enter the password for SNMPv2 read/write access.

  Default: Private.

- **Trap Destination:** An SNMPv2 Trap is a notification of a network event, like a fault or security issue. The Trap Destination is typically the IP address of the SNMP server where trap messages should be sent.

- **Port:** Enter the SNMPv2 port number for ‘receiving traps’.

  Default: 162 (This is a dedicated TCP/UDP port and typically should not be changed.)

- **IP Address:** Enter the IP address of the SNMPv2 server that’s receiving SNMP traps.

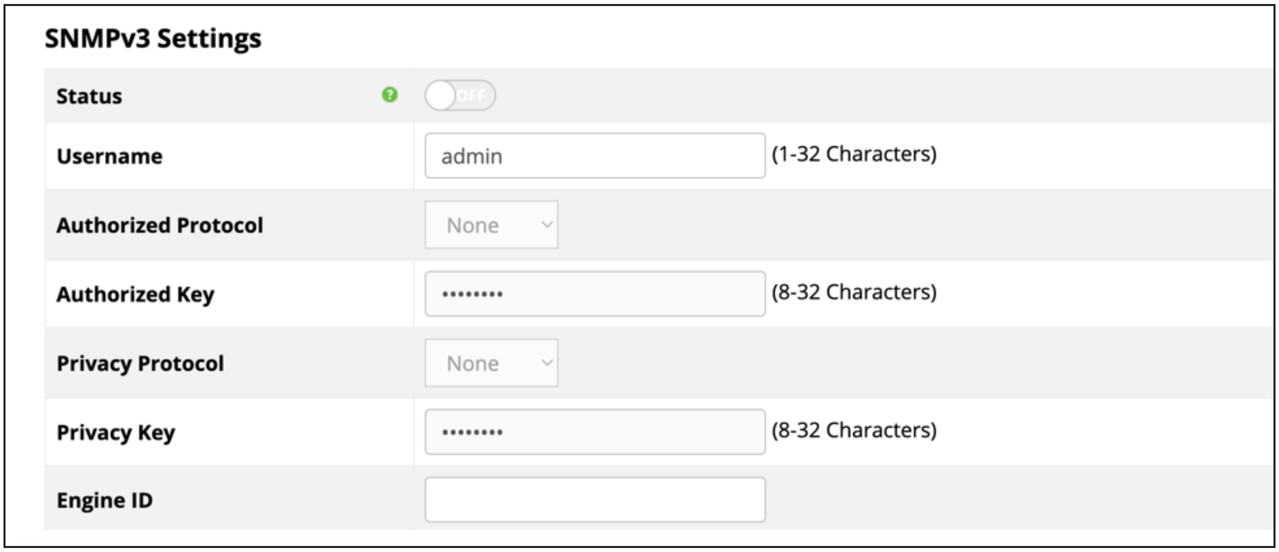
- **Community Name:** Enter the password for the SNMPv2 trap community.

Click **Save**, then **Apply Changes** when you’re finished with the configuration.

SNMPv3 Settings

Note: Refer to the SNMP server documentation while configuring these settings.

Path: Advanced > SNMP > SNMPv3



SNMPv3 Settings

Status	OFF
Username	admin (1-32 Characters)
Authorized Protocol	None
Authorized Key	•••••••• (8-32 Characters)
Privacy Protocol	None
Privacy Key	•••••••• (8-32 Characters)
Engine ID	

Configurable Settings

- **Status:** Toggle on or off.

  Default: Off

- **Username:** Enter a username for SNMPv3 implementation. RANGE: 1-31 Characters.

  Default: admin.

- **Authorized Protocol:** Use the drop-down to select MD5, SHA, or None.

  Default: MD5

- **Authorized Key:** Enter an authentication key to act as an electronic signature, when authenticating SNMPv3 messages. RANGE: 8-32 Characters.

  Default: 12345678

- **Privacy Protocol:** Use the drop-down to select DES or None.

Default: DES

- **Privacy Key:** Enter a Privacy Key to act as an encryption for the data within a SNMPv3 message. RANGE: 1-8 Characters.

  Default: 12345678

- **Engine ID:** Enter an Engine ID to identify where a SNMPv3 message is coming from.

  Default: Blank

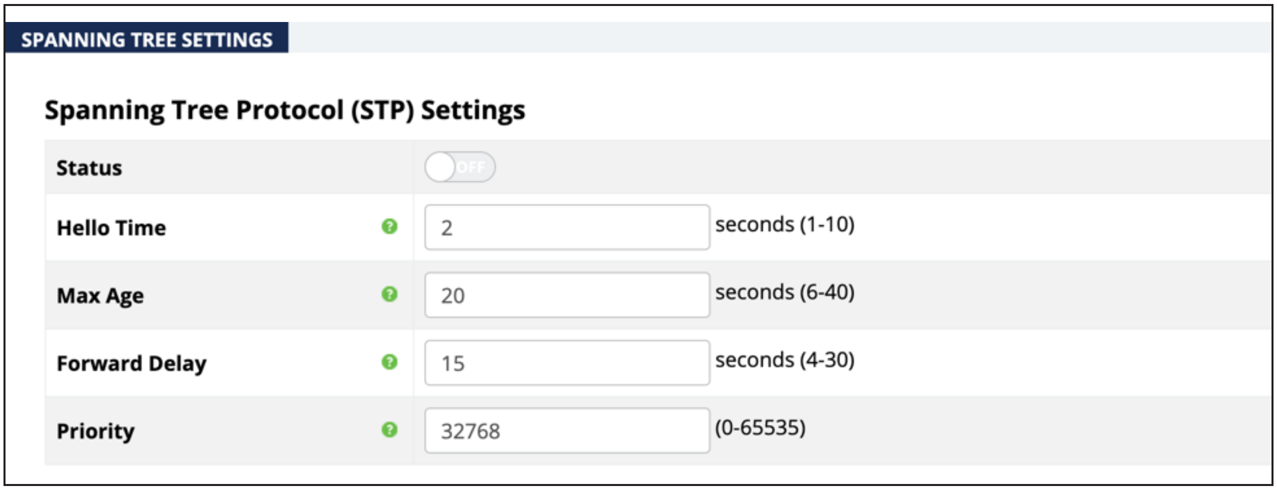
Click **Save**, then **Apply Changes** when you're finished with the configuration.

Spanning Tree Settings

Spanning Tree is an IP network protocol that prevents loops caused by multiple active paths between switches or bridges on the network. Read Understanding Spanning Tree & Best Practices for more information.

Caution: Do not enable Spanning Tree unless you have a specific use case for it. Support has received a number of calls because of unnecessary STP implementation.

Path: Advanced > Spanning Tree



SPANNING TREE SETTINGS

Spanning Tree Protocol (STP) Settings

Status	OFF	
Hello Time	2	seconds (1-10)
Max Age	20	seconds (6-40)
Forward Delay	15	seconds (4-30)
Priority	32768	(0-65535)

Configurable Settings

- **Status:** Toggle STP on or off.

  Default: Off

- **Hello Time:** Enter a value between 1-10 seconds. This setting determines how often, in seconds, the access point sends a Hello Message to the network switches and bridges to assess the network topology.

  Default: 2 seconds

- **Max Age:** Enter a duration between 6-40 seconds.

- This setting determines how long the access point waits for a Hello Message from another switch or bridge. If no message is received within the set duration, the device switch or bridge is considered offline and a new STP route is configured.

  Default: 20 seconds.

- **Forward Delay:** Enter a value between 4-30 seonds. This setting determines the length of time the access point 'listens' to the network and either retains the current topology or generates a new topology, based on network switch or bridge status.

  Default: 4 seconds.

- **Priority:** Enter a value for between 0-65535. This setting helps to determine which bridge is the root bridge, which is the switch that controls the main route that network traffic is routed through to avoid network loops.

  Default: 32768.

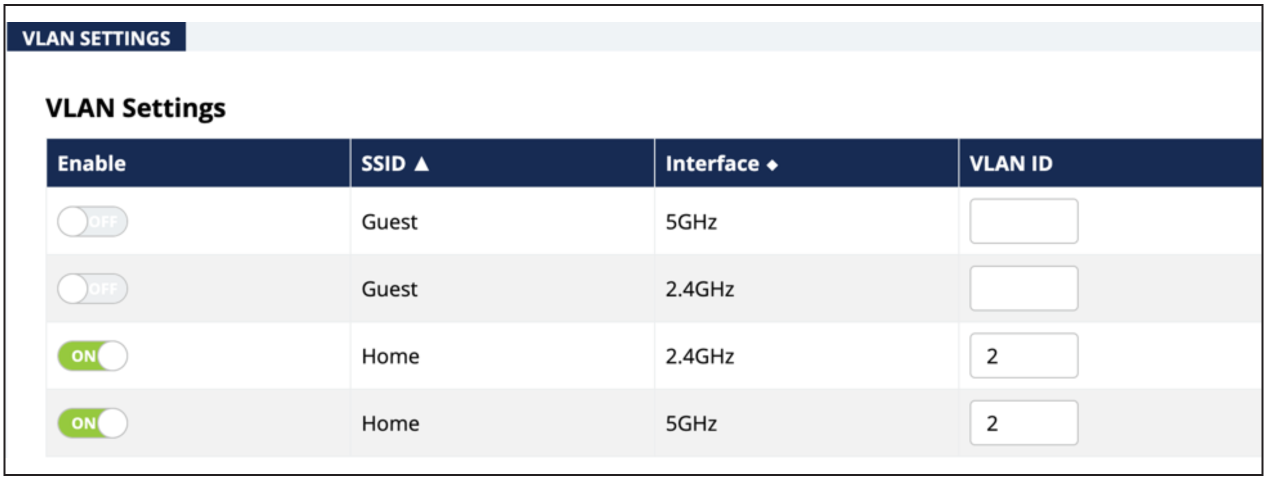
Click **Save**, then **Apply Changes** when you're finished with the configuration.

VLANs

Use this menu to tag an SSID with a VLAN ID. The most common use case is for more advanced guest network configurations. Read Araknis Access Point Guest SSID VLAN Setup for instructions.

Caution: Do not tag an SSID with the default VLAN ID of the network. This causes the access point to lock up and may require a factory default to regain access.

Path: Advanced > VLANs



VLAN Settings

Enable	SSID ▲	Interface ◆	VLAN ID
OFF	Guest	5GHz	
OFF	Guest	2.4GHz	
ON	Home	2.4GHz	2
ON	Home	5GHz	2

How to Tag an SSID with a VLAN ID

1. Click the **Enable** toggle next the SSID and radio interface you want to tag. If you do not see the SSID you wish to tag, verify that the SSID is enabled under **Settings** > **Wi-Fi Setup**.
2. Enter the **VLAN ID** in the SSID row that you want to tag.
3. Click **Save**, then **Apply Changes** when you're finished with the configuration.

Technical Support

For chat and telephone, visit **snp1.co/techsupport** • Email: **TechSupport@SnapOne.com**. Visit**snp1.co/tc** for discussions, instructional videos, news, and more.

Warranty and Legal Notices

Find details of the product's Limited Warranty and other resources such as regulatory notices and patent and safety information, at **snapone.com/legal** or request a paper copy from Customer Service at **866.424.4489**.

Snap One makes no claim that the information contained herein covers all installation scenarios and contingencies, or product use risks. Information within this specification subject to change without notice.

230620

200-AN-520_820-AP-A