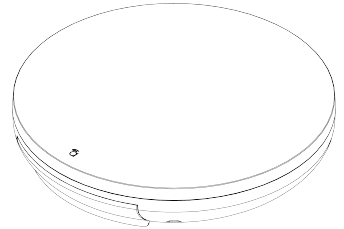

AN-x30-AP-I Wi-Fi 7 Wireless Access Point

Welcome to Araknis Networks™

Thank you for choosing an Araknis™ Wi-Fi 7 Wireless Access Point (AP). With a circular housing, an easy mounting system, convenient PoE power, and the latest Wi-Fi 7 wireless technologies, these products are ideal as staples in both residential and commercial applications.



Features

- Wi-Fi 7 Certified
- Sleek circular design

AN-830-AP-I & AN-830-AP-I-1: High-performance 4x4 6GHz radio

- 1× 10 Gigabit LAN port w/PoE-IN
- 1× Gigabit LAN port (data only)

AN-530-AP-I & AN-530-AP-I-1: 2x2 6 GHz radio

- 1× 10 Gigabit LAN port w/PoE-IN
- OvrC-enabled

Installing Wi-Fi 7

Before you deploy Wi-Fi 7, there's some information you'll want to know to set your customers' expectations and deliver a successful deployment.

What does Wi-Fi 7 add?

- 6 GHz expansion for a cleaner spectrum that doesn't support legacy devices.
- 320 MHz doubles the channel width for higher throughput in low-interference environments.
- WPA3 encryption. 6 GHz does not support WPA2.
- 4K-QAM increases data density by almost 20% compared to 1024-QAM, at strong signal levels.
- Multi-Link Operation (MLO) enables a client device to use multiple bands simultaneously. This provides a more reliable connection and lower latency. This requires the client device to support MLO.
- Standard Power provides a higher 6 GHz transmit power in supported regulatory domains.
- Multi-gig edge expectations with a strong signal.

 **Note:** MLO and Standard Power are coming soon to the AN-x30 series access points.

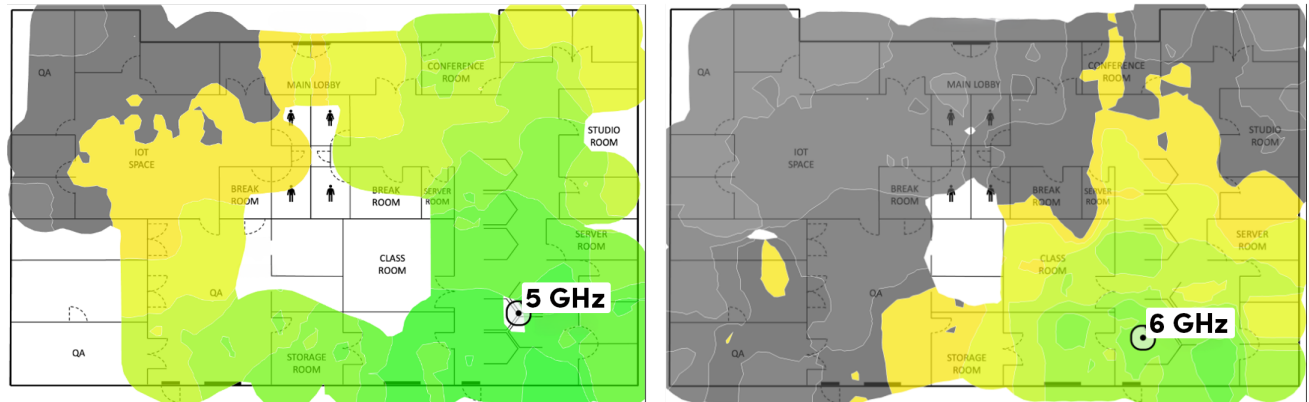
Wi-Fi 7 requirements

- Multi-gig switching at 2.5 Gbps+. Clients won't notice the speed without a 2.5 Gbps internet service, a 2.5 Gbps modem, router, and switch.
- Cat6/6A cables. 6A is required for 10 Gbps.
- A PoE (802.3bt) budget that supports 60W per AP.
- Client devices that support Wi-Fi 6E/7.

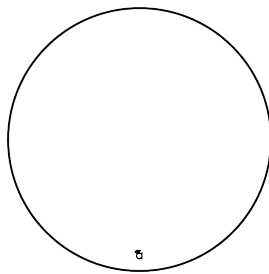
Expectations and deployment

6 GHz is ideal for same-room or line-of-sight applications. It has a shorter propagation range and does not penetrate building materials well. Expect to add 1.5 more access points compared to 2.4 and 5 GHz only installations.

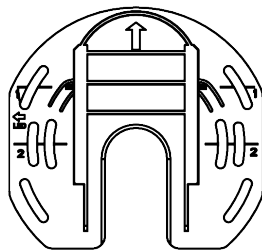
2.4 and 5 GHz broadcasts are critical for full coverage, but you will most likely need to turn the 2.4 GHz broadcast off in some access points to reduce interference.



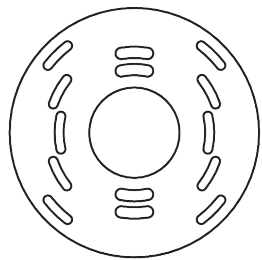
Box contents



Access point (AP)



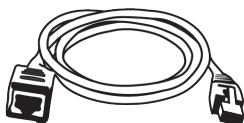
Mounting bracket



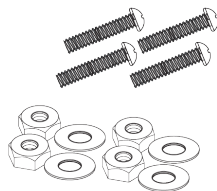
Tile ceiling backing
plate



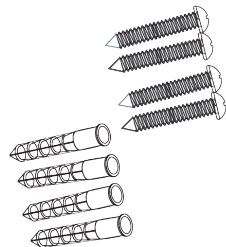
Quick Start Guide QR
card



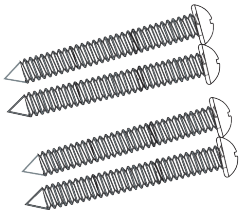
Male-to-female
category jumper cable



Tile ceiling mounting
hardware



Drywall mounting
hardware



Wood surface mounting
hardware

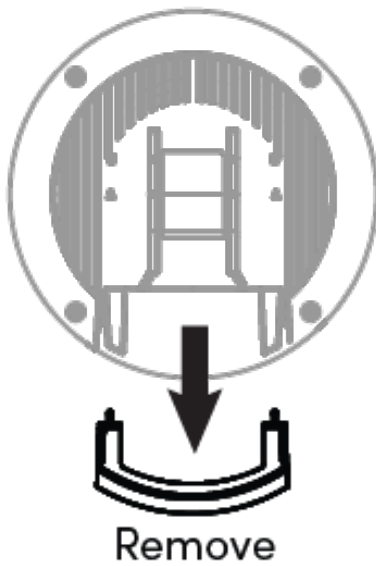
 **Note:** This guide uses the 830 AP for illustrative purposes.

Installing the AN-530-AP-I

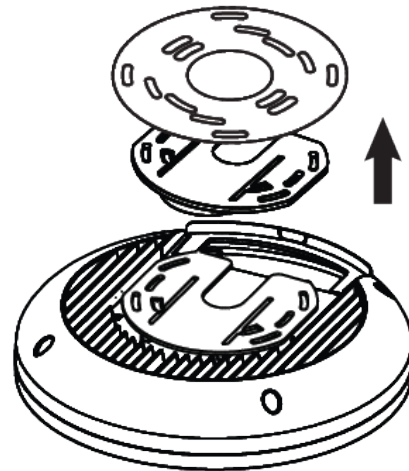
Keep in mind that the access point has an operating temperature of 50°C when choosing a mounting location.

 **Pro Tip:** Use the ceiling back plate on top of acoustic ceiling tiles to prevent the mounting nuts from pulling through the tile.

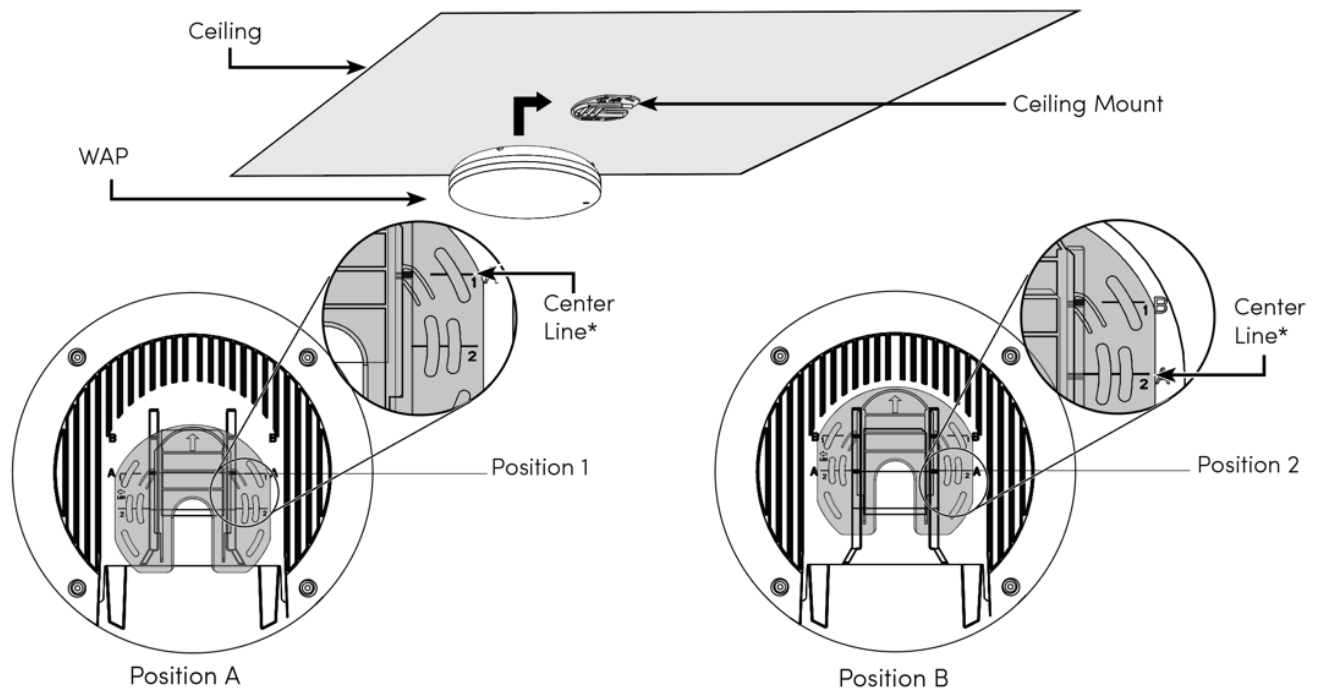
Removing the cable bay cover



Attaching the AP to the ceiling mount



Positioning the ceiling mount

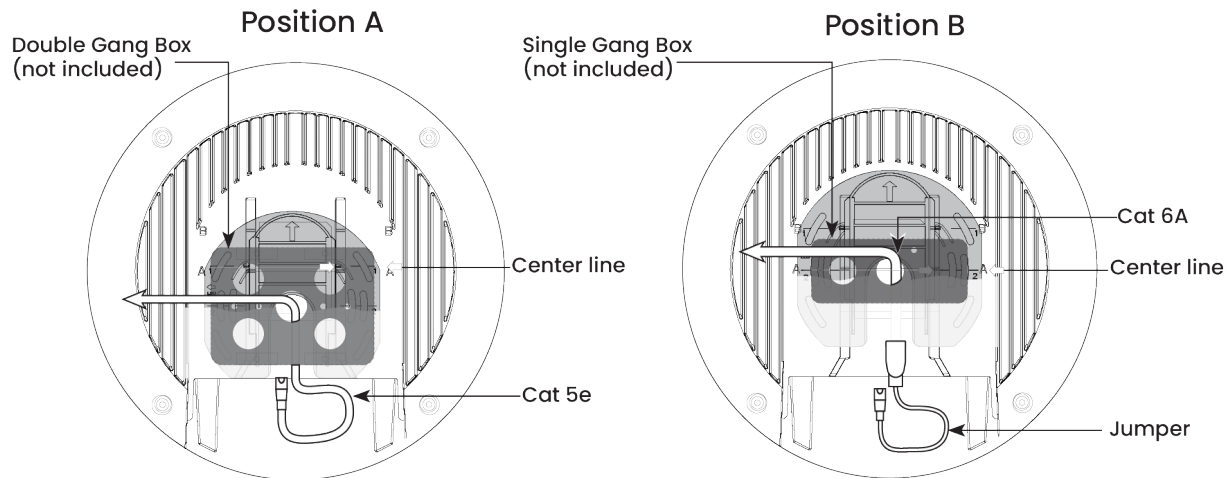


* The center line of the bracket is not necessarily the center line of the AP when it's being installed.
Use the above guide to understand the center line of the AP when installing the bracket.

Using the jumper cable

You can mount your access point to the electrical box in one of two positions, shown below. These options are provided to provide cable bend relief for cables of different lengths and thicknesses.

The illustrations do not reflect pre-install steps. Run the wire or jumper prior to connecting the access point.



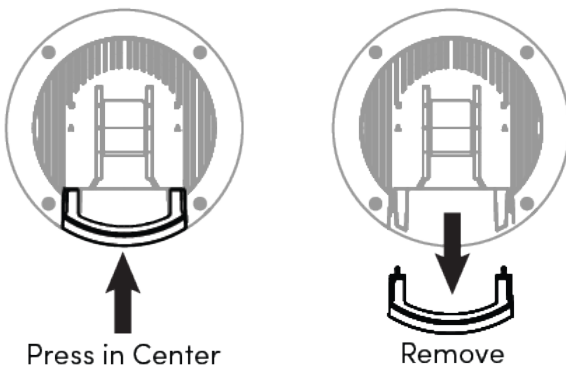
Note: Use the jumper cable when using Cat 6A in Position B.

Installing the AN-830-AP-I

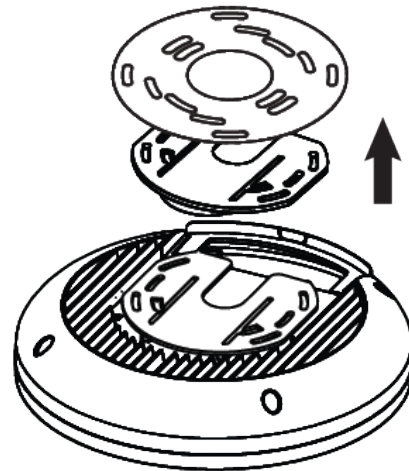
Keep in mind that the access point has an operating temperature of 50°C when choosing a mounting location.

 **Pro Tip:** Use the ceiling back plate on top of acoustic ceiling tiles to prevent the mounting nuts from pulling through the tile.

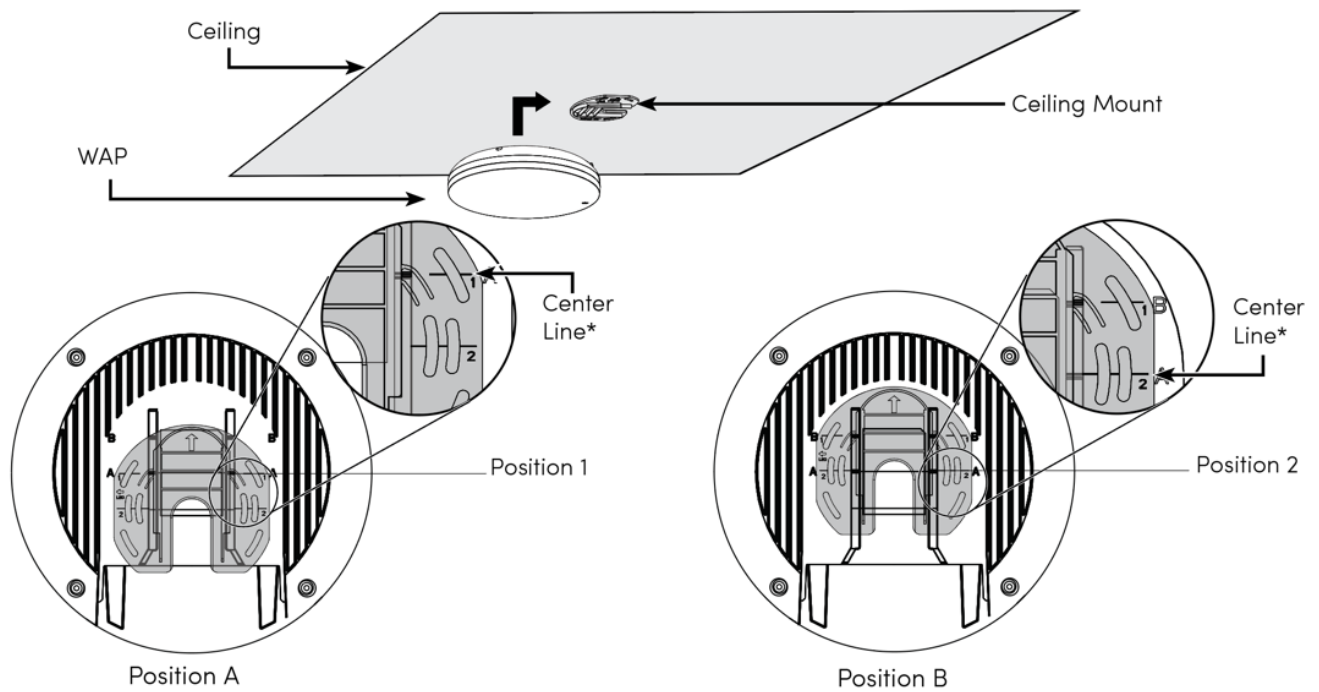
Removing the cable bay cover



Attaching the AP to the ceiling mount



Positioning the ceiling mount



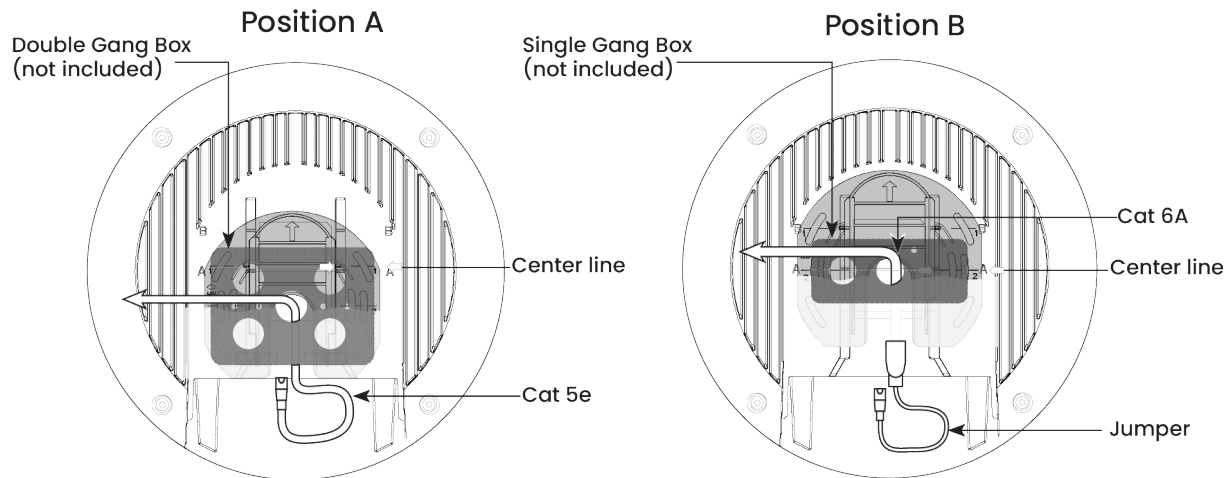
* The center line of the bracket is not necessarily the center line of the AP when it's being installed.

Use the above guide to understand the center line of the AP when installing the bracket.

Using the jumper cable

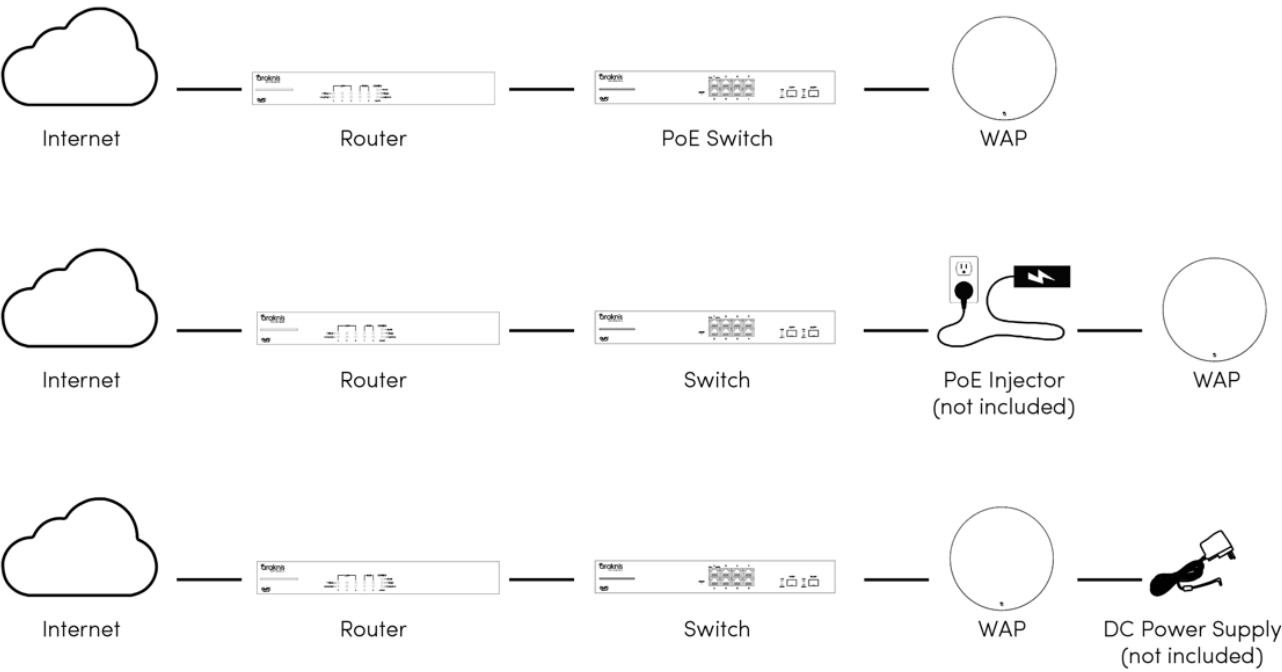
You can mount your access point to the electrical box in one of two positions, shown below. These options are provided to provide cable bend relief for cables of different lengths and thicknesses.

The illustrations do not reflect pre-install steps. Run the wire or jumper prior to connecting the access point.



Note: Use the jumper cable when using Cat 6A in Position B.

Connections



Connecting to the AP

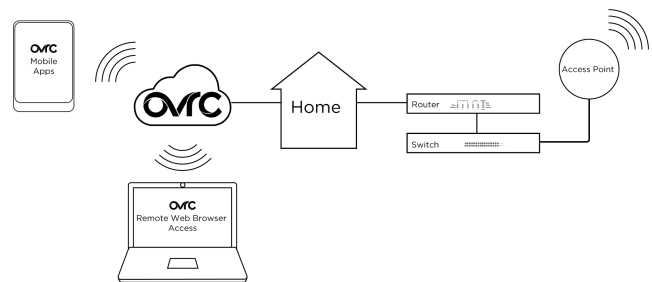
Araknis APs can be configured through OvrC or the local interface. The local interface is accessible using OvrC's webconnect feature, typing the AP's DHCP address into your browser's address bar, or using the AP's default IP address.

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*.

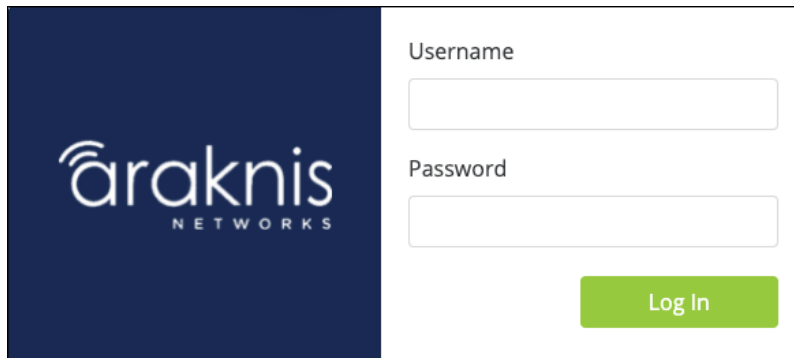


Logging into the Web Interface

1. Log into the AP using the default credentials:

Username	araknis
Password	araknis

2. You must update the password after initial login.

The image shows the login interface for Araknis Networks. On the left is a dark blue vertical bar with the 'araknis NETWORKS' logo in white. To the right of this bar is a white login form. The form has two input fields: 'Username' and 'Password'. Below the 'Password' field is a green 'Log In' button.

Username

Password

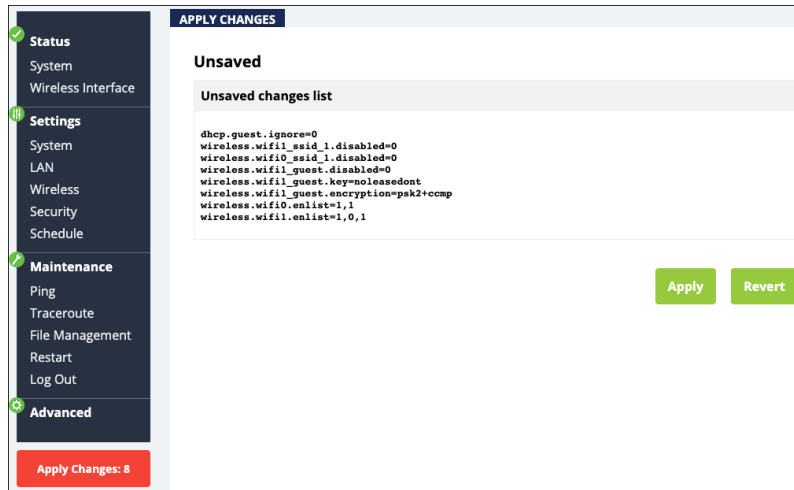
Log In



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.



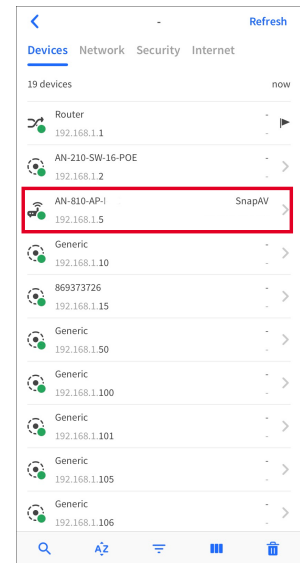
Note: Settings take effect after the progress bar reaches 100%.

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:

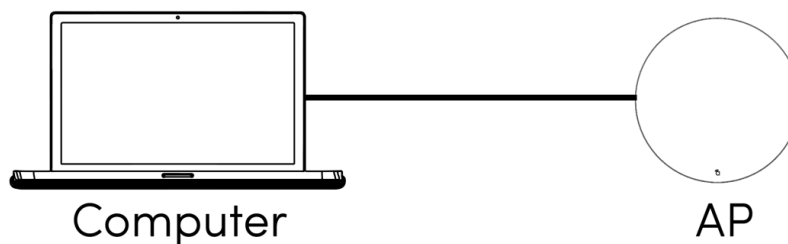
- Check the device list in OvrC.
- Check the client table on your router.
- Use a network scanner (e.g. Fing) to scan the network. The Araknis WAP manufacturer field displays SnapAV.
- See the highlighted field in the Fing screenshot to the right for an example of an Araknis device being identified.



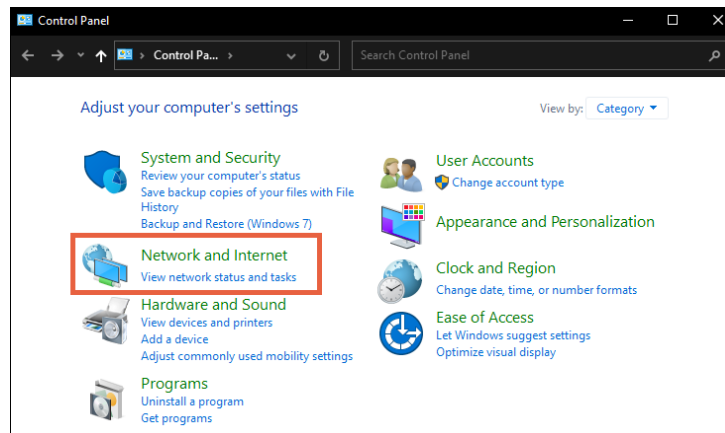
Accessing the AP Using the Default IP Address

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**.

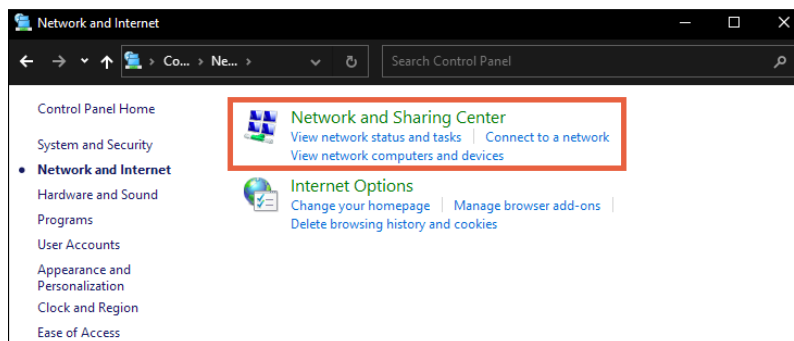
Step 1: Connect your PC to the AP using an Ethernet cable.



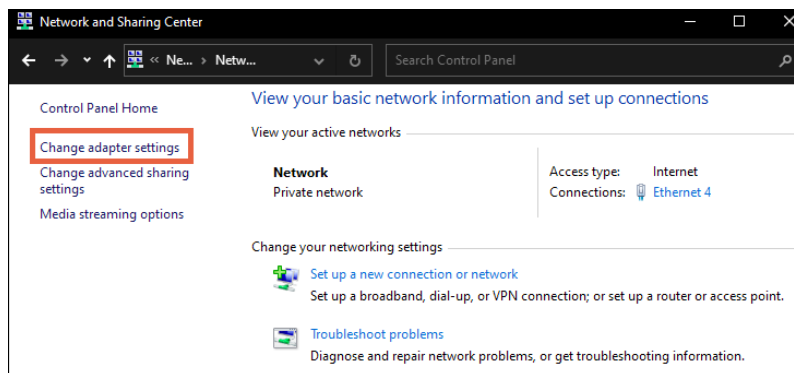
Step 2: Open the Control Panel and click Network and Internet.



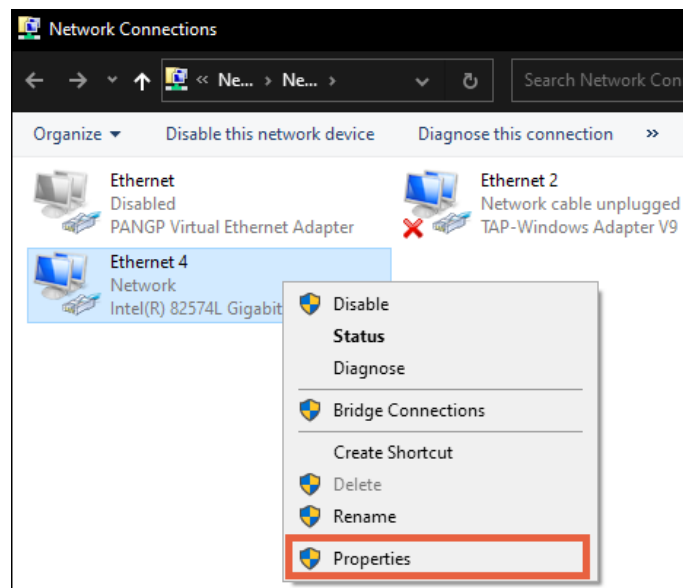
Step 3: Click Network and Sharing Center.



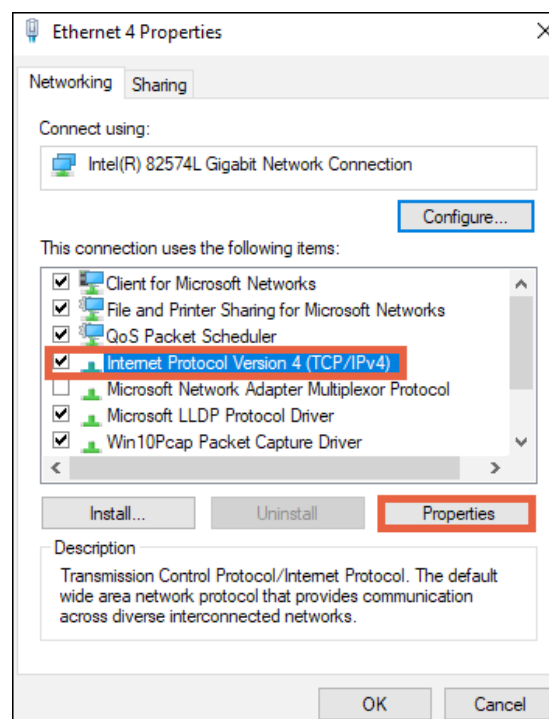
Step 4: Click Change adapter settings.



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**.



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

Advanced...

OK Cancel

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

Username	araknis
Password	araknis

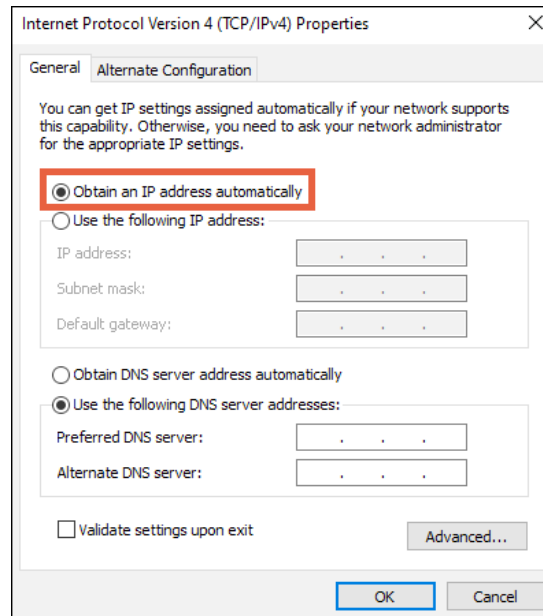
araknis NETWORKS

Username

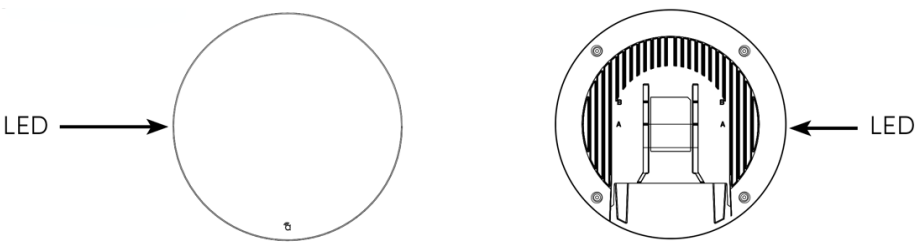
Password

Log In

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



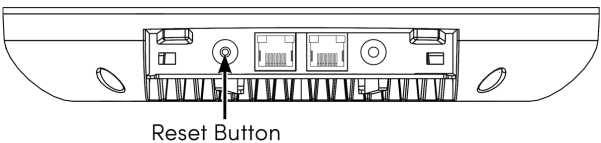
LED behaviors



AP State	LED Behavior	Description
Operational States	No LED	The AP is not powered on.
	Solid White	The AP is in the uboot stage of the startup process.
	Blinking White	The AP is at the kernel stage of the startup process.
	Solid Blue	The AP started correctly and is running in an operational state.
	Blinking Blue	The AP is operational but is underpowered.
Error States	Blinking Orange	The AP is not connected to the internet.
	Blinking Green	The AP is updating it's firmware.
	Solid Orange	The AP failed a firmware update and needs to be recovered.
	Solid Red	The AP is non-functional.

Reset procedures

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.

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.

System Information

Displays the current information about the access point's system settings.

Path: Status > System > System Information

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 current firmware version running on the access point.
- **Management VLAN ID:** The VLAN that must be used to access the web interface.

System Information	
System Name	AN-530-AP-I
Firmware Version	2.0.00
Service Tag	ST25
Management VLAN ID	Untagged
Power	PoE++ (bt)

Wireless Information

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

Path: Status > System > Wireless Information

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 (SSIDs) 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.

Wireless Information			
	2.4GHz	5GHz	6GHz
MAC Address	14:3F:C3: [REDACTED]	14:3F:C3: [REDACTED]	14:3F:C3: [REDACTED]
Number of Networks 	3	3	2
Number of Connected Clients	5	7	1
Operation Mode	Access Point	Access Point	Access Point
TX	429.95 MB	130.49 MB	127.99 MB
RX	11.55 MB	20.58 MB	4.85 MB
Guest Network	Off	Off	Off
Number of Connected Guests	0	0	0

LAN Information

Displays the current LAN connection parameters.

Path: Status > System > LAN Information

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.

LAN Information			
LAN1			
Speed	2.5Gbps	IP Address	192.168.1.184
Duplex	Full	Subnet Mask	255.255.255.0
MAC Address	14:3F:C3: [redacted]	Default Gateway	192.168.1.1
TX	1.70 GB	Primary DNS	192.168.1.1
RX	12.83 GB	Secondary DNS	

System Log

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

Path: Status > System > System Log

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.

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	WPA: EAPOL-Key timeout
Fri Apr 29 11:17:55 2022	daemon.debug	hostapd: ath0: STA	WPA: EAPOL-Key timeout
Fri Apr 29 10:17:56 2022	daemon.debug	hostapd: ath0: STA	WPA: EAPOL-Key timeout
Fri Apr 29 10:17:55 2022	daemon.debug	hostapd: ath0: STA	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	WPA: FT: Received PMK-R1 push fr
Fri Apr 29 09:48:47 2022	daemon.debug	hostapd: ath0: STA	WPA: FT: Send PMK-R1 push fr
Fri Apr 29 09:48:47 2022	daemon.debug	hostapd: ath0: STA	WPA: pairwise key handshake c
Fri Apr 29 09:48:47 2022	daemon.debug	hostapd: ath0: STA	IEEE 802.11: association OK (
Fri Apr 29 09:48:39 2022	daemon.debug	hostapd: ath0: STA	WPA: FT: Received PMK-R1 pull

Save LogClear 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. Most of which is configurable under Settings >

[Wi-Fi Setup](#).

Radio Status

Provides a detailed look at the radio settings and performance.

Path: Status > Wi-Fi Status > Radio Status

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.

Radio Status			
	2.4GHz	5GHz	6GHz
Interface Status	Enabled	Enabled	Enabled
Operation Mode	Access Point	Access Point	Access Point
Wireless Mode	802.11 BE	802.11 BE	802.11 BE
Channel Bandwidth	20 MHz	80 MHz	160 MHz
Channel Selection	11	36	97 - 125
Operating Channel	Channel 11	Channel 36	Channel 97
Channel Frequency	2.462 GHz	5.180 GHz	6.435 GHz
TX	5.11 GB	47.62 GB	5.35 GB
RX	380.43 MB	4.41 GB	203.42 MB

Utilization of SSID

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

Path: Status > Wi-Fi Status > Utilization of SSID

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.
- **Guest Network:** Displays if a Guest Network is enabled on the radio.
- **Wireless Bridge:** Displays if the radio is configured as a Wireless Bridge. This is configurable under Settings >

Wireless Bridge Setup.

Utilization of SSID			
	2.4GHz	5GHz	6GHz
SSID's Used	3	3	2
SSID's Available	5	5	6
Guest Network	Off	Off	Off
Wireless Bridge	Off	Off	-

Wireless Network

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

Path: Status > Wi-Fi Status > Wireless Network

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.
- **TX:** The amount of data transmitted in bytes on the SSID broadcast on the specific radio.
- **RX:** The amount of data received in bytes on the SSID broadcast on the specific radio.
- **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.

Wireless Network									
Wireless Network (SSID)	Enabled	Interface	Security	VLAN ID	MAC Address	TX	RX	Broadcast SSID	Client Isolation
araknis_initial	No	2.4GHz	OWE		00:00:00:00:00:00	0.00 B	0.00 B	No	No
araknis_initial	No	5GHz	OWE		00:00:00:00:00:00	0.00 B	0.00 B	No	No
araknis_initial	No	6GHz	OWE		00:00:00:00:00:00	0.00 B	0.00 B	No	No
Main	Yes	2.4GHz	WPA3-SAE		14:3F:C3: [redacted]	1.30 GB	135.75 MB	Yes	No
Main	Yes	5GHz	WPA3-SAE		14:3F:C3: [redacted]	11.14 GB	2.27 GB	Yes	No
Main	Yes	6GHz	WPA3-SAE		8E:E0:1B: [redacted]	5.35 GB	203.52 MB	Yes	No
Secondary	Yes	2.4GHz	WPA2-PSK		1A:3F:C3: [redacted]	3.81 GB	244.68 MB	Yes	No
Secondary	Yes	5GHz	WPA2-PSK		1A:3F:C3: [redacted]	36.47 GB	2.14 GB	Yes	No
Guest	Yes	2.4GHz	WPA3-SAE	2	1E:3F:C3: [redacted]	0.00 B	0.00 B	No	No
Guest	Yes	5GHz	WPA3-SAE	2	1E:3F:C3: [redacted]	0.00 B	0.00 B	No	No

Connected Clients

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

Path: Status > Wi-Fi Status >

Connected Clients

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.
- **Radio:** The radio interface being measured.
- **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.

Connected Clients

Status	Wireless Network (SSID) 	Radio 	Device Name 	MAC Address 	TX 	RX 	RSSI (dbm) 	Release
 Secondary	2.4GHz	Unknown_Host	20:0B:CF: 	14.37 MB	4.18 MB	-56	Deny	
 Main	5GHz	halo-tactile-293	50:26:EF: 	9.61 MB	11.73 MB	-65	Deny	
 Main	5GHz	MacBookAir	76:59:57: 	104.63 MB	55.76 MB	-56	Deny	
 Main	5GHz	iPhone	1A:69:23: 	335.90 KB	551.18 KB	-63	Deny	
 Main	5GHz	EmergencysME	88:66:5A: 	57.07 KB	151.03 KB	-57	Deny	
 Secondary	5GHz	Unknown_Host	E8:51:77: 	28.27 MB	98.19 MB	-52	Deny	



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

System Settings

Configure access to the AP's local UI and adjust the time settings.

System Information

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

Path: Settings > System > System Information

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.



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

Path: Settings > System > Date and Time Settings

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)

The screenshot shows the 'Date and Time Settings' interface. It has two main sections. The first section, 'Manually Set Date and Time', is currently selected with a radio button. It contains input fields for 'Date' (01 / 01 / 2025) and 'Time' (12 : 00 AM). Below these is a green button labeled 'Synchronize with PC'. The second section, 'Automatically Get Date and Time', is unselected. It contains a dropdown menu for 'NTP Server' with 'time.nist.gov' selected.

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 > Time Zone

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.

Time Zone				
Time Zone: (GMT-05-00) Eastern Time (US & Canada) ▼				
☒ Enable Daylight Saving				
Start:	March ▼	2nd ▼	Sun ▼	02:00 AM ▼
End:	November ▼	1st ▼	Sun ▼	02:00 AM ▼

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

LAN Settings

Configure the Local-Area-Network (LAN) configuration of the AP.

IP Settings

Configure the AP's IP address and subnet mask.



Pro Tip: Keep 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

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

IP Settings	
IP Address	192.168.1.184
Subnet Mask	255.255.255.0
DHCP	☒ ON

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: Do not alter the default settings unless you have a specific use case or for troubleshooting.

Path: Settings > LAN > Interface Settings

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

Interface Settings	
LAN1	
Speed	Auto

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

Wi-Fi Setup

Configure the radio settings and SSIDs.

Radio Settings

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

Path: Settings > Wi-Fi Setup> Radio Settings

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 > Wi-Fi Setup > Utilization of SSID

Table Fields

- **SSIDs Used:** The number of SSIDs currently configured for each radio interface.
- **SSIDs Available:** The remaining number of SSIDs that can be configured for each radio interface.
- **Guest Network:** Display the number of Guest Networks configured for each radio interface.
- **Wireless Bridge:** Displays if the radio is configured as a Wireless Bridge.

Utilization of SSID			
	2.4GHz	5GHz	6GHz
SSID's Used	3	3	2
SSID's Available	5	5	6
Guest Network	Off	Off	Off
Wireless Bridge	Off	Off	-

Wireless Networks

Use the Wireless Networks menu to edit, add, and delete wireless networks (SSIDs). Click the **Add** button at the bottom of the table to create a new wireless network.

 **Note:** The default araknis_initial SSID cannot be deleted, but can be modified or disabled.

Path: Settings > Wi-Fi Setup > Wireless Networks

Configurable Settings

- Enable:** Select Yes to make the SSID available.
Default: On.
- Name (SSID):** Enter a name for the network.
Default: araknis_initial (Blank when adding a new network).
- Interface:** Select which channel frequencies to broadcast.
2.4GHz, 5GHz, 6GHz, or all three.
- Security Mode:** Select a security mode from the drop-down to open the Wireless Security window. Options include OWE, WPA2/WPA3-PSK Mixed, WPA3-SAE, and WPA3.
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 "Fast Roaming" on page 45 section for more information.

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

**Note:** Client Isolation and Band Steering are under 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](#).

Wireless Networks						
Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Fast Roaming	Delete
☐	araknis_initial	2.4GHz, 5GHz, 6GHz	OWE	☐	☐	
☒	Main	2.4GHz, 5GHz, 6GHz	WPA3-SAE	☒	☐	
☒	Secondary	2.4GHz, 5GHz	WPA2-PSK	☒	☐	
☒	Security VLAN	2.4GHz, 5GHz, 6GHz	WPA3-SAE	☐	☐	

1. From the Wireless Settings page, scroll to the Wireless Networks menu. 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
☒	Home	Both	WPA3-SAE Mixed	☒	☒	
Add						

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 can connect to the network.
- **WPA2-PSK, WPA-PSK Mixed, WPA3, WPA3-SAE Mixed Configuration, and OWE**

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

- **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**.

- WPA2 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:** AES. This cannot be modified.

- **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**, at 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 > Wi-Fi Setup > Guest Network

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

Configure users for the local user interface and security protocol settings.

User Accounts

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

Path: Settings > Security > User Accounts

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)

User Accounts					
Select	Username	Privilege Level	Password	Confirm Password	Delete
☐	araknis	admin	*****	*****	
☐		Status+Settings ▾			

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

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

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

Default: Off

- **LLDP (Link Layer Discovery Protocol):** Allows the access point to exchange information between network devices. This allows the network infrastructure to automatically recognize and map the access point.

Default: On

Device Discovery	
Bonjour	 ☐ OFF
UPnP	 ☐ OFF
LLDP	 ☒ ON

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

Schedule

Configure schedules for Auto Reboot, the Gateway Connection Monitor, and SSID availability.

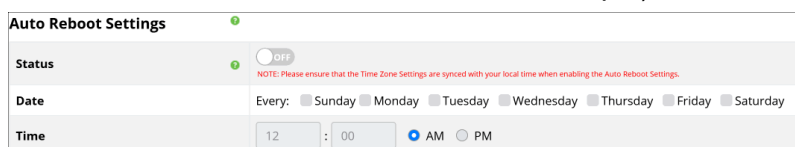
Auto Reboot Settings

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

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)



The screenshot shows the 'Auto Reboot Settings' interface. At the top, there's a green status indicator and a toggle switch labeled 'OFF'. Below this, a note states: 'NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Auto Reboot Settings.' The 'Date' section features a row of checkboxes for 'Every: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday', all of which are currently unchecked. The 'Time' section displays a digital clock set to '12 : 00' with 'AM' selected over 'PM'.

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

Configurable Settings

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

- **Status:** Toggle Auto Reboot on or off.
Default: Off
- **Gateway IP Address:** Enter the gateway IP address to be pinged, usually the router. Click **Get Current Gateway IP** to automatically enter the gateway address assigned to the access point.
- **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 rebooting 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

Gateway Connection Monitor	
Status	☐ OFF
Gateway IP Address	<button>Get Current Gateway IP</button>
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)

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.

Configurable Settings

- **Status:** Toggle the Wi-Fi Scheduler on or off.
Default: Off
- **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 8AM-5PM Daily:** The wireless network is on at 8:00AM and off at 5:00PM (08:00-17:00).
 - **Available 8AM-5PM Daily Except Weekends:** The wireless network is on at 8:00AM and off at 5:00PM (08:00-17:00) 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

Status ☒

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

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

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 ☒

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.

Wireless Bridge Setup

Wireless Bridge Mode creates a point-to-point connection between two Araknis x30 series access points. This expands the network coverage in an area you can't get a wire to. You cannot build a wireless bridge across more than two access points.

The remote access point requires power and a LAN connection for configuration. You must remove the LAN connection afterward to avoid a network loop.

Wireless Bridge must be configured in a local and remote access point to work. To do so:

1. Log in to the local UI of the access point that is going to keep a LAN connection.
2. In the local UI, go to **Wireless Bridge** and enable the feature.
3. Select the radio to connect with. 2.4 or 5GHz.

Bridge Mode Configuration	
Enable Wireless Bridge	☒
Role	--
Backhaul Radio	2.4GHz

4. Enter a unique name for the **Backhaul SSID**. This SSID is unique to the wireless bridge and should not match other SSIDs on the network. This must match on the two x30 access points you're configuring.

Backhaul Configuration	
Backhaul SSID	Repeater SSID
Local BSSID	36:3F:C3: (This BSSID will be used by the remote device)
Remote BSSID	14:3F:C3:
Passkey	
Security Type	WPA3-SAE (Fixed)

5. The **Remote BSSID** is the **Local BSSID** of the access point you're building the bridge with.

Local Access Point	Remote Access Point																								
<table border="1"> <thead> <tr> <th colspan="2">Backhaul Configuration</th> </tr> </thead> <tbody> <tr> <td>Backhaul SSID</td> <td>Repeater SSID</td> </tr> <tr> <td>Local BSSID</td> <td>36:3F:C3:E3:E1:2D (This BSSID will be used by the remote device)</td> </tr> <tr> <td>Remote BSSID</td> <td>XX:XX:XX:XX:XX:XX</td> </tr> <tr> <td>Passkey</td> <td>Enter WPA3-SAE passkey</td> </tr> <tr> <td>Security Type</td> <td>WPA3-SAE (Fixed)</td> </tr> </tbody> </table>	Backhaul Configuration		Backhaul SSID	Repeater SSID	Local BSSID	36:3F:C3:E3:E1:2D (This BSSID will be used by the remote device)	Remote BSSID	XX:XX:XX:XX:XX:XX	Passkey	Enter WPA3-SAE passkey	Security Type	WPA3-SAE (Fixed)	<table border="1"> <thead> <tr> <th colspan="2">Backhaul Configuration</th> </tr> </thead> <tbody> <tr> <td>Backhaul SSID</td> <td>Repeater SSID</td> </tr> <tr> <td>Local BSSID</td> <td>36:3F:C3:E3:E1:2D (This BSSID will be used by the remote device)</td> </tr> <tr> <td>Remote BSSID</td> <td>XX:XX:XX:XX:XX:XX</td> </tr> <tr> <td>Passkey</td> <td>Enter WPA3-SAE passkey</td> </tr> <tr> <td>Security Type</td> <td>WPA3-SAE (Fixed)</td> </tr> </tbody> </table>	Backhaul Configuration		Backhaul SSID	Repeater SSID	Local BSSID	36:3F:C3:E3:E1:2D (This BSSID will be used by the remote device)	Remote BSSID	XX:XX:XX:XX:XX:XX	Passkey	Enter WPA3-SAE passkey	Security Type	WPA3-SAE (Fixed)
Backhaul Configuration																									
Backhaul SSID	Repeater SSID																								
Local BSSID	36:3F:C3:E3:E1:2D (This BSSID will be used by the remote device)																								
Remote BSSID	XX:XX:XX:XX:XX:XX																								
Passkey	Enter WPA3-SAE passkey																								
Security Type	WPA3-SAE (Fixed)																								
Backhaul Configuration																									
Backhaul SSID	Repeater SSID																								
Local BSSID	36:3F:C3:E3:E1:2D (This BSSID will be used by the remote device)																								
Remote BSSID	XX:XX:XX:XX:XX:XX																								
Passkey	Enter WPA3-SAE passkey																								
Security Type	WPA3-SAE (Fixed)																								

6. Enter a unique **passkey**. This must match on the two x30 access points you're configuring.

Backhaul Configuration	
Backhaul SSID	Repeater SSID
Local BSSID	36:3F:C3: (This BSSID will be used by the remote device)
Remote BSSID	14:3F:C3:
Passkey	
Security Type	WPA3-SAE (Fixed)

7. Click **Save**, then **Apply** the changes. Wait for the progress bar to complete and the access points to restart. Typically about three minutes.
8. Repeat steps 2 through 7 for the access point you're installing at the remote location.
9. Give the remote access point about 2 minutes for the wireless bridge to start.
10. Remove the Ethernet cable from the remote access point. Failure to do so creates a network loop.
11. Place the remote access point in the desired location and apply power.
12. Once it's connected, log in to remote access point's local UI and go back to the Wireless Bridge Setup page.
13. Verify the integrity of **Connection Status** by clicking **Run Test**.

Connection Status

Remote Device Status

● Online

Link Uptime

0 d 0 h 12 m 19 s

Connection Health

77% - Good

Run Test

Detailed Connection Information

Parameter	Value	Status
Throughput	183.96 Mbps	⬇ - Fair
Latency	1.67 ms	✓ - Excellent
Jitter	0.30 ms	✓ - Excellent
Signal Strength	-67.00 dBm	X - Poor
Packet Loss	0	✓ - Perfect

The **Detailed Connection Information** provides a Poor, Fair, or Excellent status.

Ping

Ping tests determine if an 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

Start**Stop**

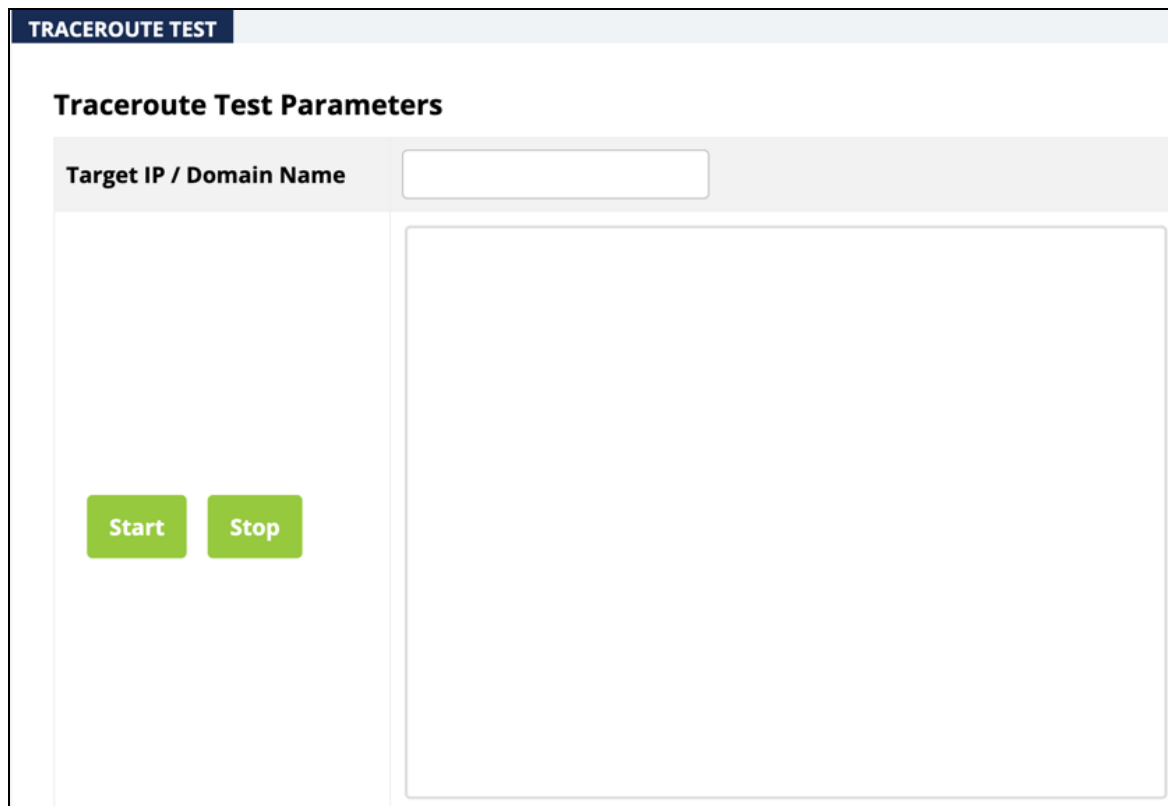
How to Run a Ping Test

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

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

Path: Maintenance > Traceroute



The screenshot shows a web interface titled "TRACEROUTE TEST" in a dark blue header. Below the header, the main section is titled "Traceroute Test Parameters". It features a light gray header bar with the label "Target IP / Domain Name" and an adjacent text input field. The main content area is split into two columns. The left column contains two green buttons labeled "Start" and "Stop". The right column is a large, empty rectangular box intended for displaying test results.

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.

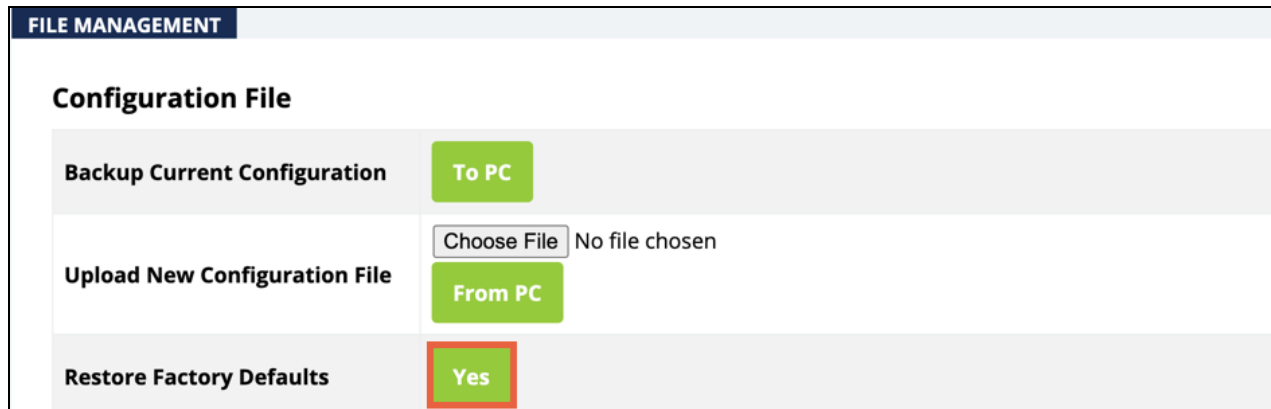
How to Upload a Configuration File

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.



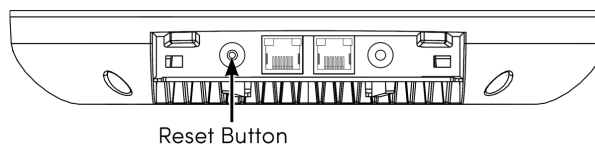
2. Click **Confirm** to restore factory defaults. A loading page pops up while the AP restores the factory defaults. When complete, the login window appears.
3. Enter the default username and password. (araknis; araknis) and configure the AP like new, or upload a configuration file.

How to manually factory default the access point

Press and hold the Reset button for more

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

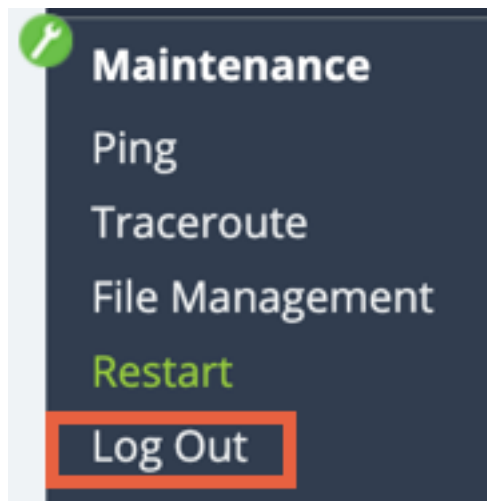


Click the **Reboot the Device** button. You'll get a confirmation message and be presented with the login screen when the AP restarts.

Logging Out of the AP

Path: Maintenance > Logout

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



Advanced Wireless Settings

Use this page to fine tune the performance of the AP.

Radio Settings

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

Path: Advanced > Wireless Settings > Radio Settings

Radio Settings			
Transmit Power Unit	☒ dBm ☐ mW		
	2.4GHz	5GHz	6GHz
Transmit Power ?	Custom ▾	Custom ▾	
	12 dBm (Range:5dBm ~ 25dBm)	12 dBm (Range:6dBm ~ 26dBm)	Full 100%-26 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 for 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	6GHz
Enable		☐ OFF	☐ OFF	☐ OFF
Max Client No.		127	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

SSID	Client Isolation ?	Band Steering ?	OFDM Only ?	WiFi 6 / 7 ?	Wi-Fi Power Save ?	DTIM ?	MC/BC Threshold ?	mDNS Forwarding ?
araknis_initial	☐ OFF	☐ OFF	☐ OFF	☒ ON	☐ OFF	1	20	☐ ON
araknis_test	☐ OFF	☐ OFF	☐ OFF	☒ ON	☐ OFF	1	20	☒ 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, 5GHz, and 6GHz 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 allow legacy 802.11b/g devices to connect on the SSID.

When OFDM (Orthogonal Frequency Division Multiplexing) only is enabled, it blocks legacy 2.4 GHz 802.11b and early 802.11g clients from connecting by disabling CCK (Complementary Code Keying) data rates of 1, 2, 5.5, and 11 Mbps. This ensures maximum throughput for modern 802.11g and newer 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.

- **WiFi 6/7:** Turn this feature off to allow incompatible devices to connect to the SSID. When enabled, WiFi 6/7 clients on this SSID can use advanced features such as OFDMA and Target Wake Time (TWT) to improve efficiency and performance.
- **Wi-Fi Power Save:** Allows compatible client devices to "sleep smarter" by scheduling they wake to send and receive data. This reduces network congestion and extends the client device's battery life, but it may also expose issues with some clients.
- **DTIM (Deliver Traffic Indication Message):** A message interval that can wake a device in a sleeping state. The higher the value the less often the device will be woken up, which can increase battery life but also increase the response time/latency.
- **MC/BC Threshold (Multicast/Broadcast-to-Unicast Conversion Threshold):** Enter a value to dynamically adjust when multicast-to-unicast conversion is turned on.
 - 0 = Always disabled
 - 64 = Always enabled
 - 20 = Default. Multicast-to-unicast conversion is disabled once the client count reaches this value.

Click here for more details

Broadcast and multicast traffic are always sent at the lowest basic rate. Heavy broadcast/multicast traffic can negatively impact high-bandwidth applications.

Multicast traffic is not acknowledged by Wi-Fi receivers, so the access point cannot guarantee a receipt of broadcast/multicast traffic.

Unicast is sent at higher data rates so it can guarantee a receipt of each packet. Since unicast is a direct relationship between each client and the access point, additional clients added to the network add additional traffic overhead.

- **mDNS Forwarding:** mDNS Forwarding allows devices on this SSID to discover and access network services—such as printers or media servers—across different VLANs or subnets. When disabled, mDNS packets from this SSID are blocked from reaching other networks, enhancing isolation and security.

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

MAC Filter

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
-----	-------------	--------

Add

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

ON

NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the MAC Filter Scheduler.

Schedule Templates

Choose a template ▾

Schedule Table

Day	Availability	Start / End Time
Sunday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM
Monday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM
Tuesday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM
Wednesday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM
Thursday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM
Friday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM
Saturday	Available ▾	from 12 : 00 ☒ AM ☐ PM ~ 11 : 59 ☐ AM ☒ PM

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 (00:00-24:00):** The MAC Filter is always on.
 - **Available 8AM-5PM Daily (08:00-17:00):** The MAC Filter is on at 8:00AM and off at 5:00PM.

- **Available 8AM-5PM 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 12 hour format. 12:00AM = midnight. 12:00PM = noon. The numbers restart after 12:00PM, noon. For example, 17:00 = 5PM. Subtract 12 from the total.
 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, 5GHz, and 6GHz 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 ☐ 6GHz

Scan Nearby Networks

?

Scan

Result

BSSID ↕	SSID ↕	Mode ↕	Channel ↕	Channel Utilization ↕	Signal ↕	Encryption ↕	Type ↕
1E:D7:5B: [REDACTED]		AP	44	1 %	-87	WPA2-PSK	11AC
3E:D7:5B: [REDACTED]		AP	44	1 %	-86	WPA2-PSK	11AC
2E:D7:5B: [REDACTED]	SpectrumSetup-C3	AP	44	1 %	-87	WPA2-PSK	11AC
1E:55:1F: [REDACTED]	Spectrum Mobile	AP	157	3 %	-85	WPA2	11AXA
1E:D7:5B: [REDACTED]		AP	157	3 %	-85	WPA2-PSK	11AC

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, 5GHz, or 6GHz 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 access point is measuring in the surrounding area. The higher the percentage, the busier the channel is.

Path: Advanced > Channel Utilization

CHANNEL UTILIZATION	
Select Interface	☐ 2.4GHz ☐ 5GHz ☒ 6GHz
Current Bandwidth	160 MHz
Current Channel	6.115 GHz (Channel 33)
Channel Usage	1%
Start	

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.

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					
Enable ?	SSID	Interface	Download Limit		Upload Limit
☐ OFF	araknis test	2.4GHz	325	Mbps(1 - 325)	325 Mbps(1 - 325)
☐ OFF	araknis test	5GHz	1361	Mbps(1 - 1361)	1361 Mbps(1 - 1361)
☐ OFF	araknis test	6GHz	2722	Mbps(1 - 2722)	2722 Mbps(1 - 2722)

How to configure Wireless Traffic Shaping

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.



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

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

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

SNMPv3 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.

Unnecessary STP implementation usually leads to a call to support, who will ask you to turn it off unless you have documentation for a specific use case.

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 seconds. 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.

 **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 ↕	VLAN ID
☒	Primary	1
☒	Secondary	2

How to Tag an SSID with a VLAN ID

1. Click the **Enable** toggle next the SSID 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.
3. Click **Save**, then **Apply Changes** when you're finished with the configuration.

Firmware Release Notes

Araknis 530 Series Access Point Firmware Release Notes

v2.0.02

Release date	2025-19-03
Firmware version	2.0.02
Product SKUs affected	AN-530-AP-I

This is the initial release.

Araknis 830 Series Access Point Firmware Release Notes

v2.0.05

Release date	2026-06-18
Firmware version	2.0.05
Product SKUs affected	AN-830-AP-I

This is the initial release.