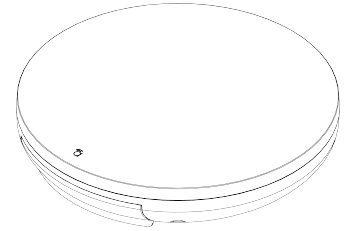

AN-x20-AP-I Wi-Fi 6 Wireless Access Point

Welcome to Araknis Networks™

Thank you for choosing an Araknis™ Wi-Fi 6 Wireless Access Point (AP). With a circular housing, an easy mounting system, convenient PoE power, and the latest Wi-Fi 6 wireless technologies, these products are ideal as staples in both residential and commercial applications.



Features

- 802.11AX Wi-Fi 6 Certified
- Sleek circular design

AN-820-AP-I: High-performance 4x4 dual-band 802.11AX 3600Mbps (80MHz support)

- 1x 2.5 Gigabit LAN port w/PoE-IN
- 1x Gigabit LAN port (data only)

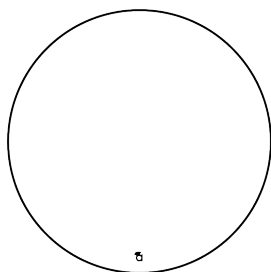
AN-520-AP-I: 2x2 Mid-range dual-band 802.11AX 3000Mbps (160MHz support)

- 1x 2.5 Gigabit LAN port w/PoE-IN
- 1x Gigabit LAN port (data only)

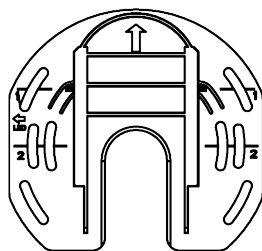
AN-320-AP-I: 2x2 Entry-level dual-band 802.11AX 1800Mbps (80MHz support)

- 1x Gigabit LAN port w/PoE-IN
- OvrC-enabled

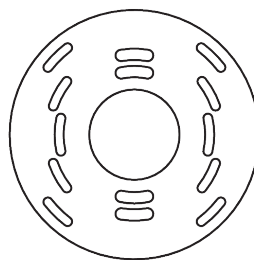
Box contents



Access point (AP)



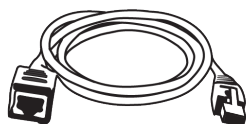
Mounting bracket



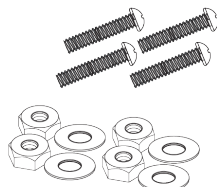
Tile ceiling backing
plate



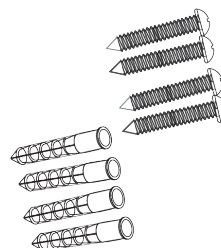
Quick Start Guide QR
card



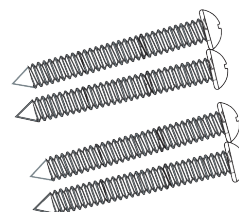
Male-to-female
category jumper
cable



Tile ceiling mounting
hardware



Drywall mounting
hardware

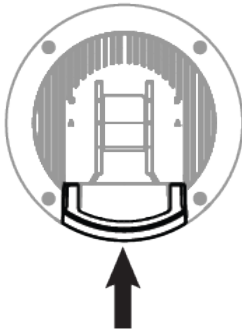


Wood surface
mounting hardware

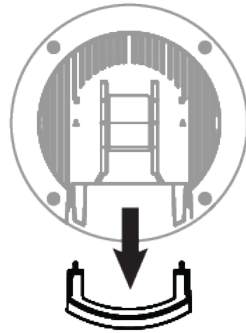
 **Note:** This guide uses the 820 AP for illustrative purposes.

Installing the AP

How to Remove the Cable Bay Cover

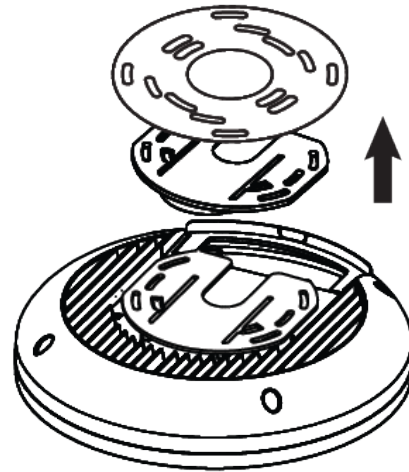


Press in Center



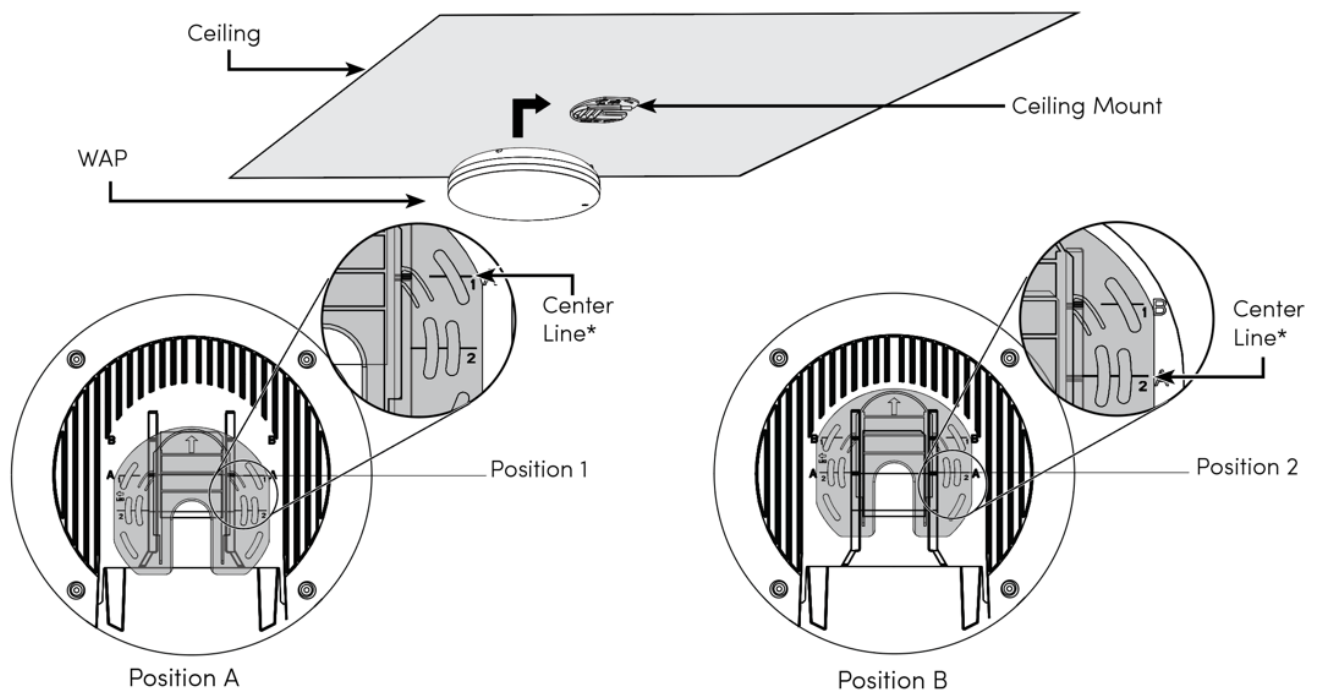
Remove

Ceiling Mount



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

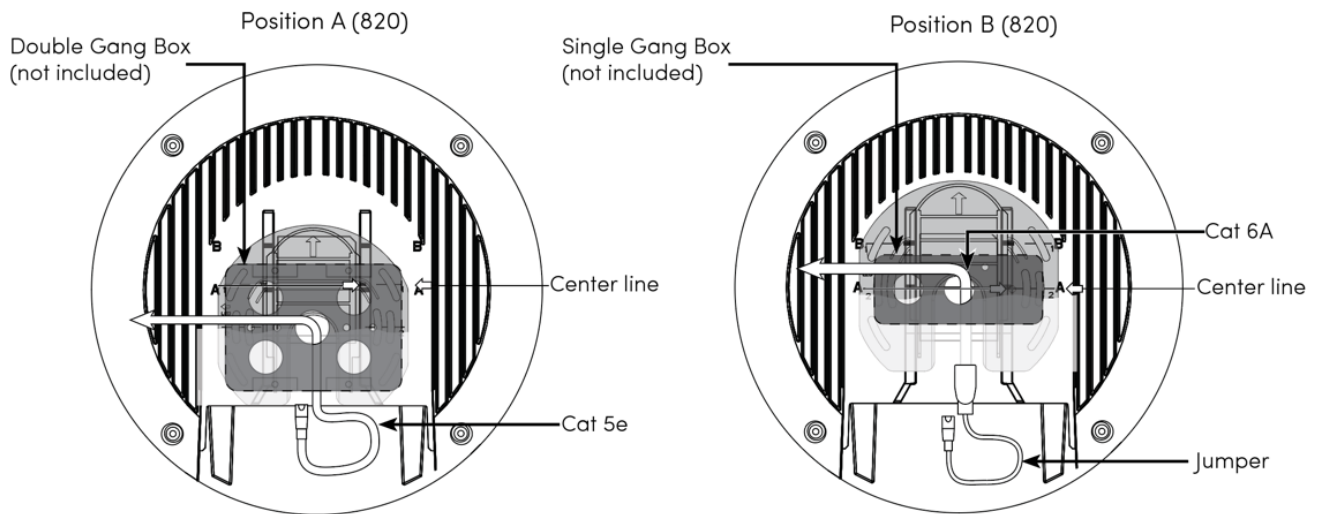
Positioning the Ceiling Mount



* 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.

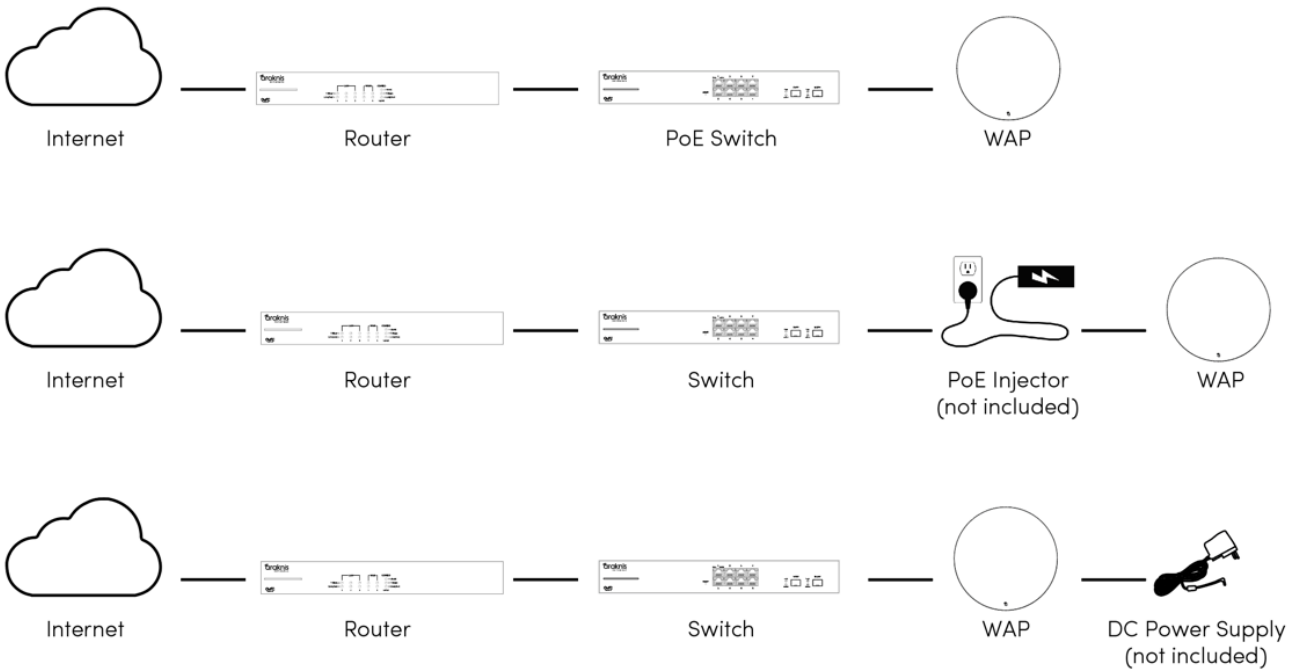
Using the Jumper Cable

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.**



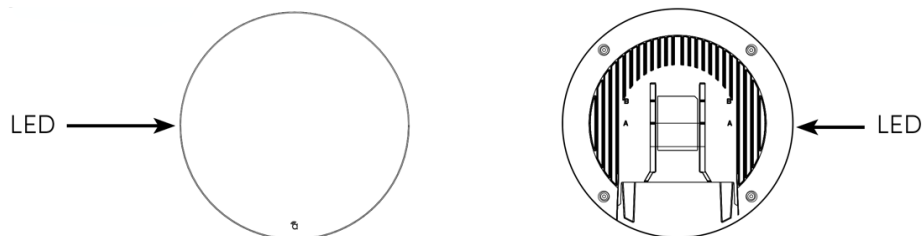
Note: Use the jumper cable when using Cat 6A in Position B.

Connections



 **Note:** 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.

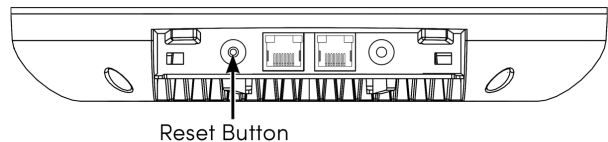
LED behaviors



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

Reset Button Action	LED State	Description
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.

Araknis 520 Series Outdoor Access Points

Documentation

AN-520-AP-O

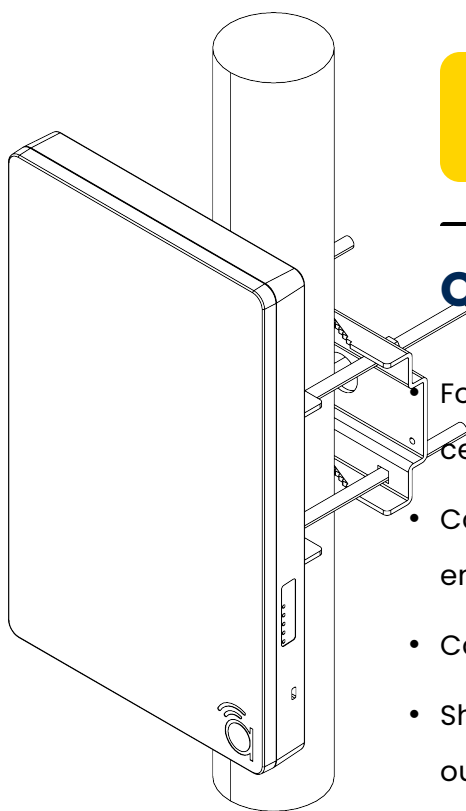
Outdoor Wi-Fi 6 Access Points Installation Guide

Welcome to Araknis Networks™

Thank you for choosing an Araknis Outdoor Wireless Access Point (AP). With sleek, unobtrusive housings, extensive features, unique easy setup, and convenient PoE power, these products are ideal for use in both residential and commercial applications.

Features

- IP55 weather resistant
- Versatile mounting
- Bottom or rear cable entrance
- Kensington lock hole for added security
- 2×2 dual-band 802.11AX 3000Mbps
- 1× 2.5 Gigabit PoE-in (no DC input)
 - IEEE 802.3at PoE+ (30W) required for power
- 1× 1 Gigabit LAN port out for data and PoE (15W)
 - IEEE 802.3bt PoE++ is required to pass PoE out
- OvrC enabled



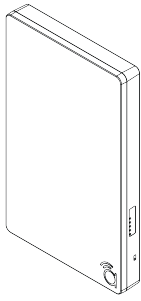
Caution: Install with the ports facing downward to avoid water collecting in the ports.

Outdoor Installation Guidelines

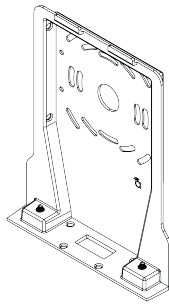
- For wall mount, position at least 24" (60cm) from eave or ceiling edges.
- Cable feed opening must be directed away from the open environment.
- Cable feed must be pointed down when wall-mounted.
- Shielded Cat 5 cable or above is recommended for outdoor installation and should be grounded through the AC ground of the PoE.
- Operating Temperature Range: -20-55° C
- Storage Temperature Range: -30-80° C

Caution: Install with the ports facing downward to avoid water collecting in the ports.

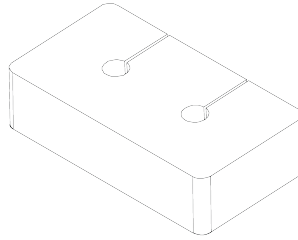
Box contents



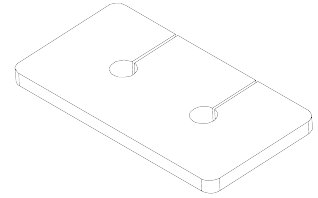
Access Point (AP)



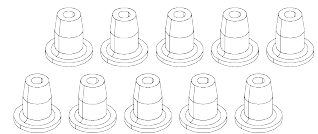
Mounting bracket



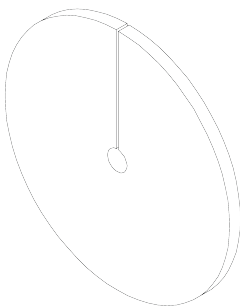
Inner foam cable
inserts (2*)



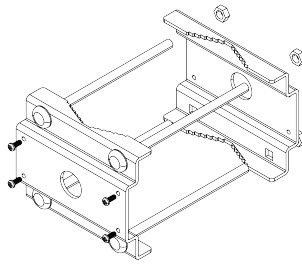
Bracket cable inserts



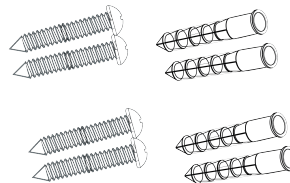
Rubber weep hole
plugs (10)



Rear bracket foam
inserts (2*)



AN-ACC-AP-O-POLE
Access pole mount
sold separately

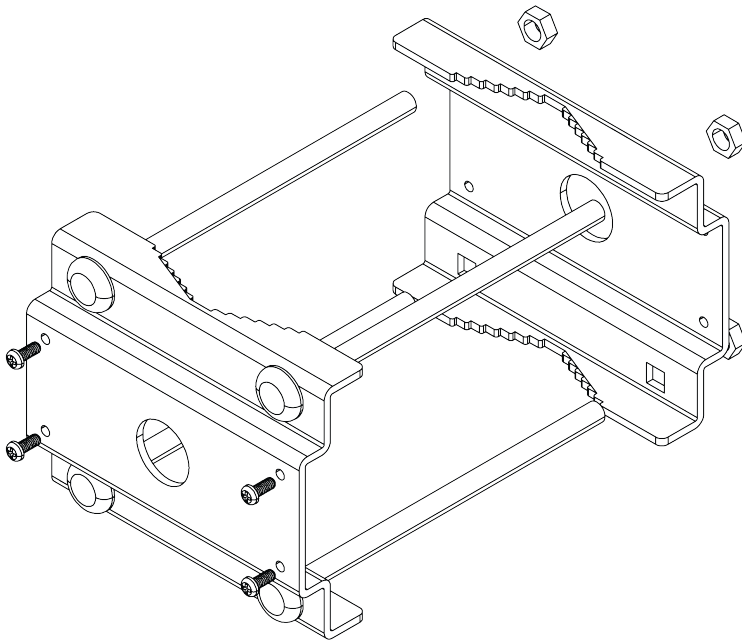


Wall mount
hardware (4 each of
screws & anchors)

*Includes one gasket each for small or large diameter cables. Use the size that best fits your cable.

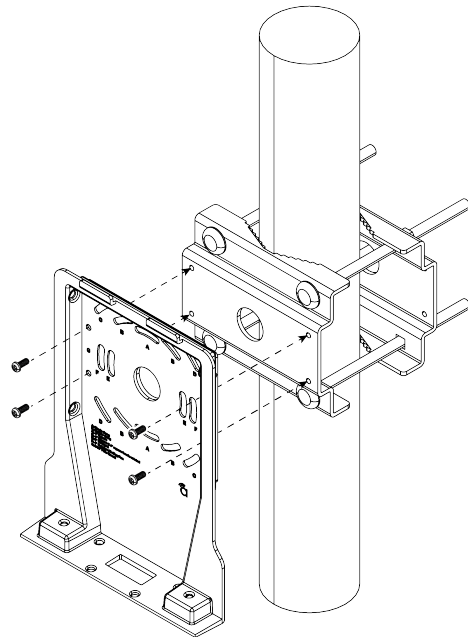
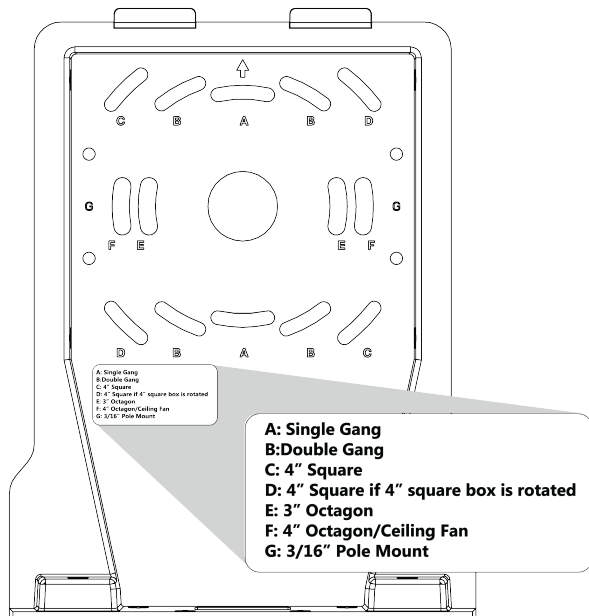
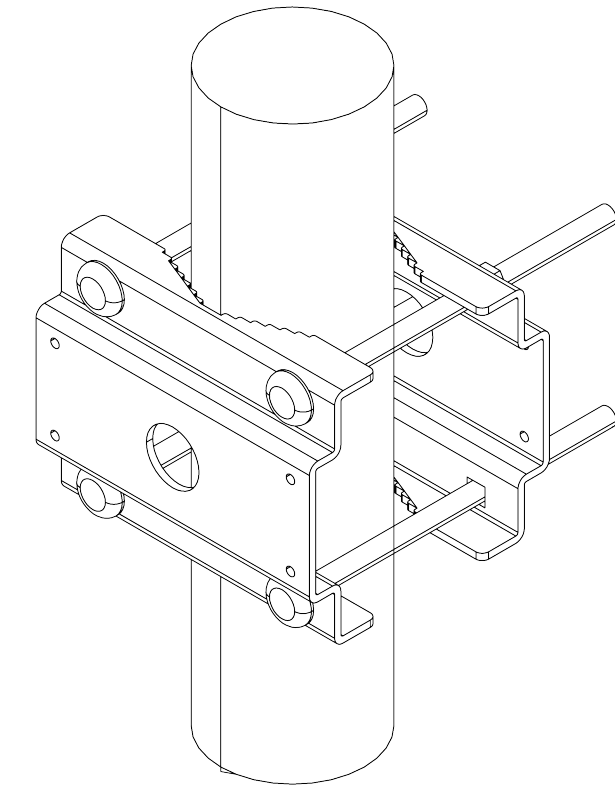
Optional installation of the pole mount accessory

The AN-ACC-AP-O-POLE accessory mount can be purchased separately and used to securely attach the access point to a pole 1.5-3.1" in diameter.



Tighten the clamp nuts enough to prevent unwanted side-to-side movement without damaging the pole or clamps.

Bracket Mounting

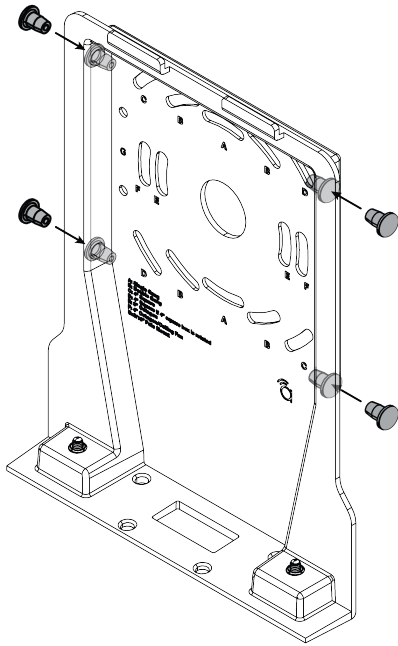


Pole mounting shown for reference. For surface mounting, fasten to the surface using the included screws and anchors.

 **Caution:** Install with the ports facing downward to avoid water collecting in the ports.

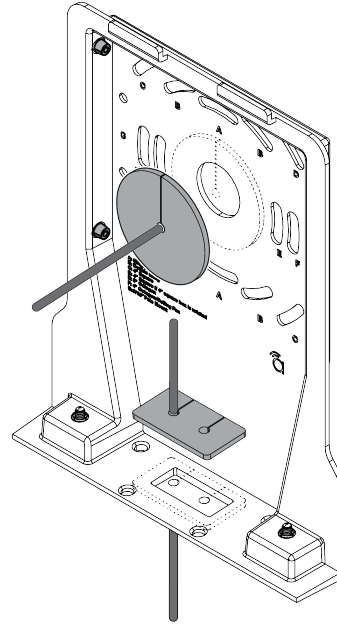
Weatherproofing

The weep hole plugs must be installed correctly.



Leave the bottom weep holes open for drainage.

Pull the cables through before installing the foam pieces to avoid tearing the foam.



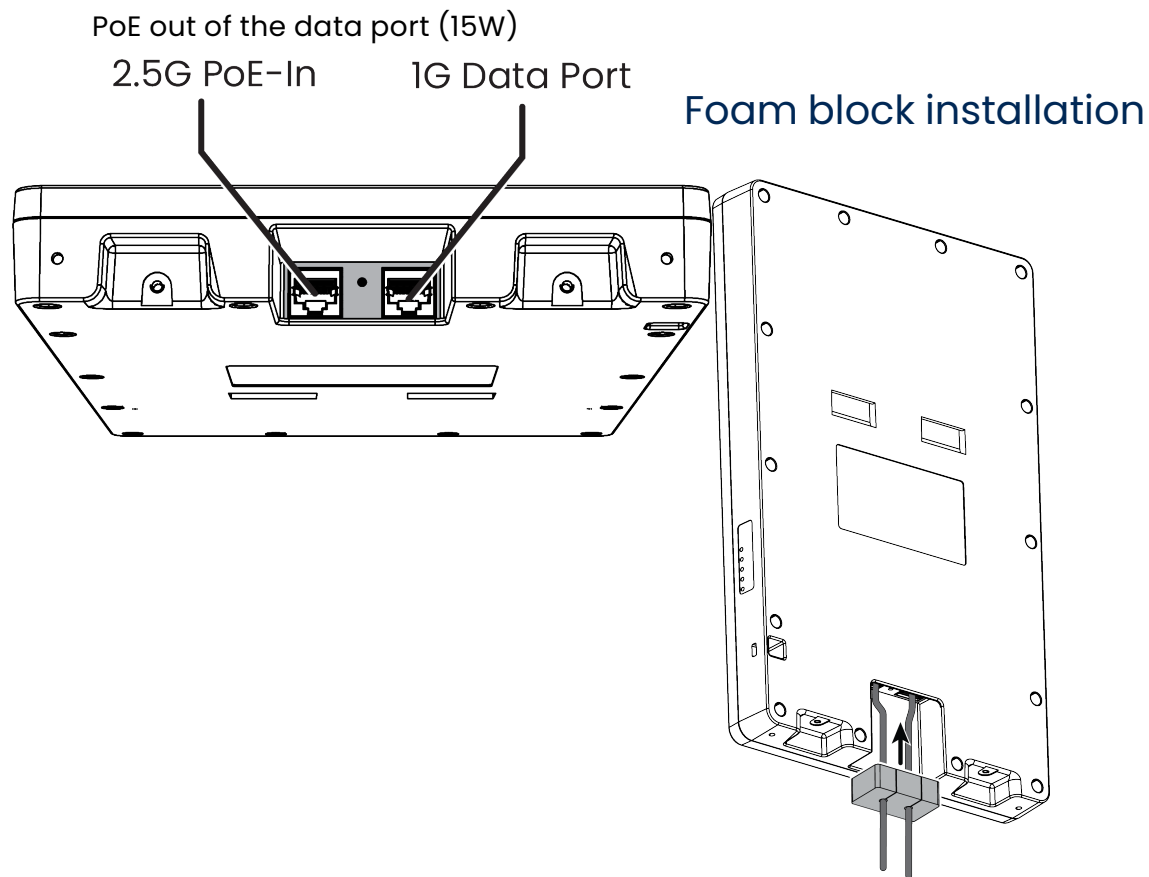
Caution: Use gaskets that best fit the cable diameter.

To ensure weatherproofing, insert the gasket even if the cable entrance is not used.

Connections

PoE specifications

- IEEE 802.3af PoE+ (30W) required for power.
- IEEE 802.3bt PoE++ is required to pass



The foam block must be pushed to the back of the cable entrance with large holes facing connectors.

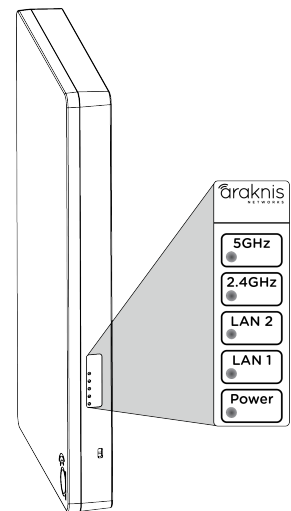
Remove the adhesive backing before installation.

 **Note:** Leave the white dust cover in the Data Port if it is not being used. Use pliers to remove the dust cover.

LED operation

Verify the AP's operation with the Power LED.

AP state	Power LED color	Description
Operational	No LED	The AP is not powered on
	Solid white	The AP is in a startup process at the uboot stage
	Blinking white	The AP is in a startup process at the kernel stage
	Solid blue	The AP started correctly and is running in an operational state
	Blinking blue	The AP is operating but is underpowered
Environmental	Solid white	The heater is operating
Error	Blinking orange	The AP is not connected to the internet
	Blinking green	The AP is performing a firmware update
	Solid orange	The AP failed a firmware update and needs to be recovered
	Solid red	The AP is non-functional

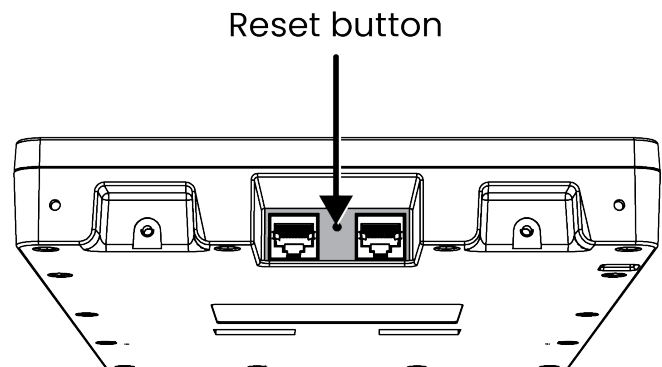


LEDs	LED state	Description
2.4 and 5GHz	Off	The radio is disabled
	Solid blue	The radio is enabled
	Blinking blue	The radio is passing network packets
LAN1 and LAN2	Off	The AP is not connected to the internet

LEDs	LED state	Description
	Solid blue	The AP is performing a firmware update
	Blinking blue	The AP failed a firmware update and needs to be recovered

Reset procedures

The reset button is in the AP's cable bay.



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	Resets the username and password only
Hold the reset button for more than 20 seconds	Blinking red	Resets the AP to factory defaults

Connecting to the AP

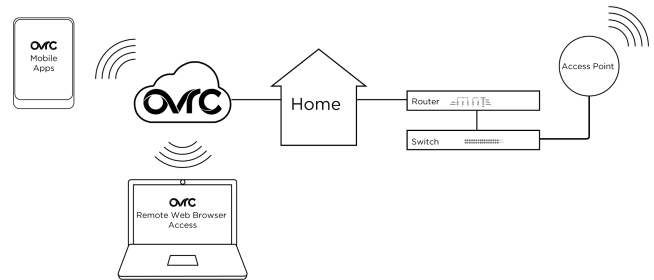
Araknis APs can be configured through OvrC or the local interface. The local interface is accessible using OvrC's webconnect feature, typing the AP's DHCP address into your browser's address bar, or using the AP's default IP address.

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*.

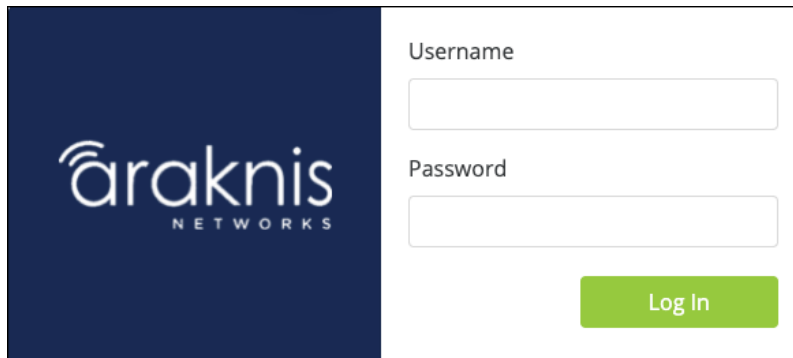


Logging into the Web Interface

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

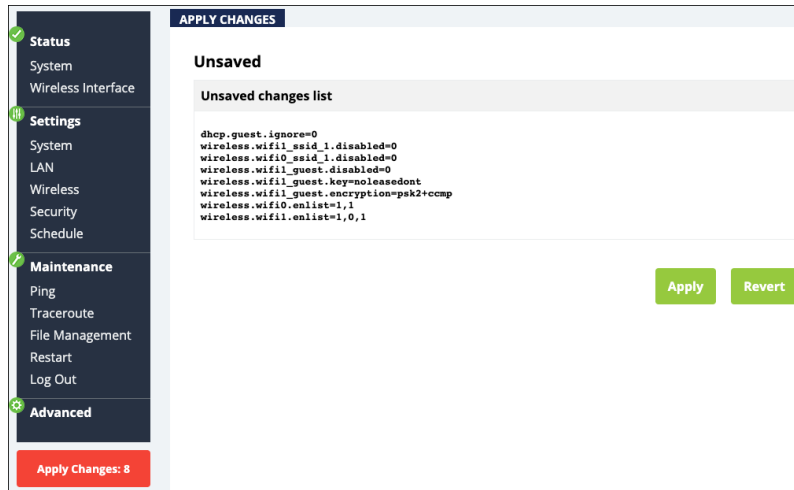
Log In



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.



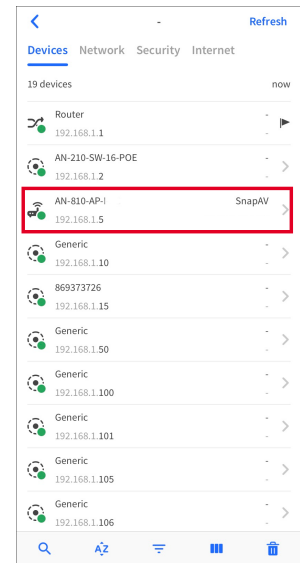
 **Note:** Settings take effect after the progress bar reaches 100%.

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:

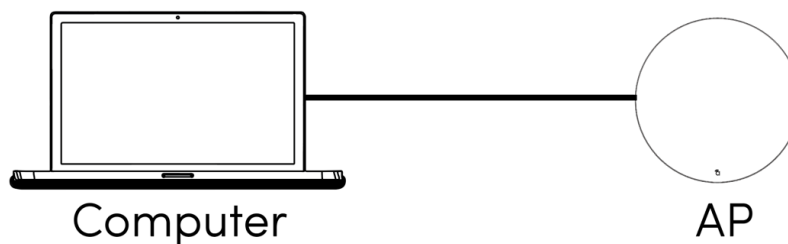
- Check the device list in OvrC.
- Check the client table on your router.
- Use a network scanner (e.g. Fing) to scan the network. The Araknis WAP manufacturer field displays SnapAV.
- See the highlighted field in the Fing screenshot to the right for an example of an Araknis device being identified.



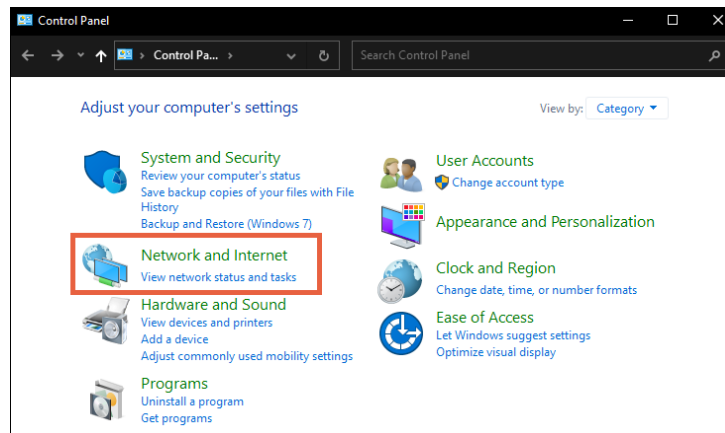
Accessing the AP Using the Default IP Address

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**.

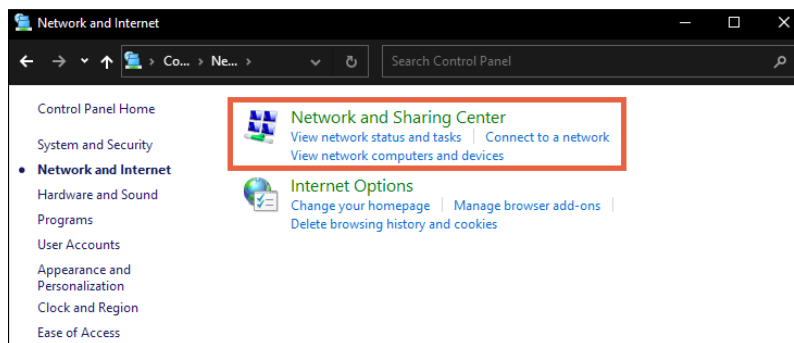
Step 1: Connect your PC to the AP using an Ethernet cable.



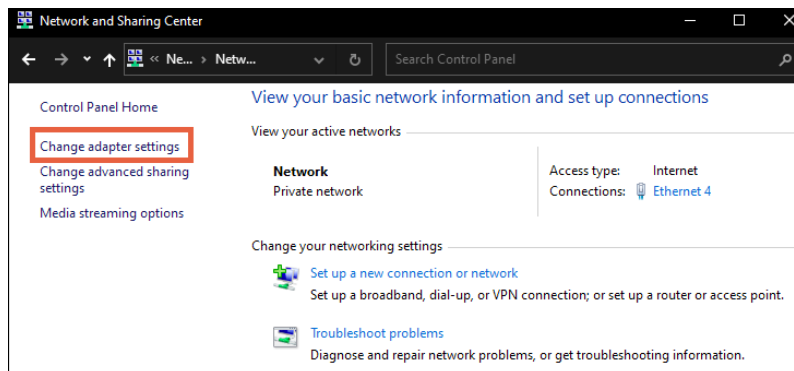
Step 2: Open the Control Panel and click Network and Internet.



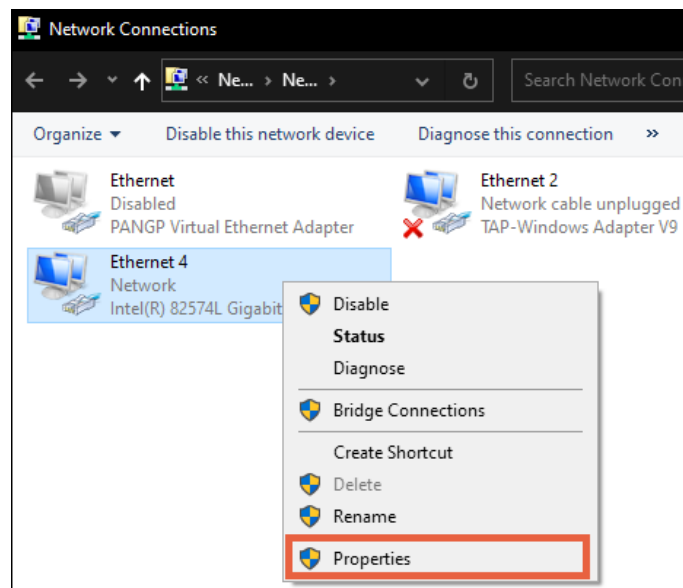
Step 3: Click Network and Sharing Center.



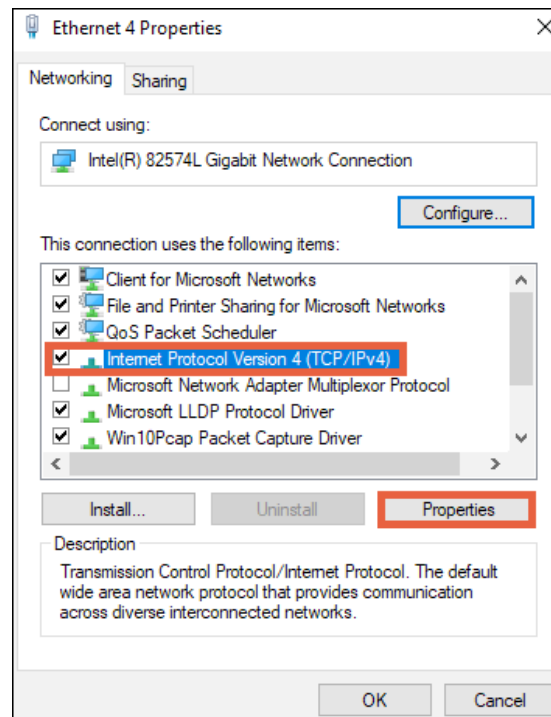
Step 4: Click Change adapter settings.



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

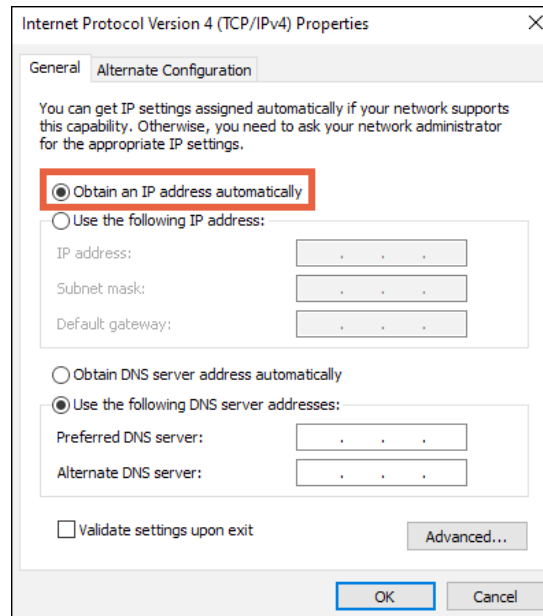
araknis NETWORKS

Username

Password

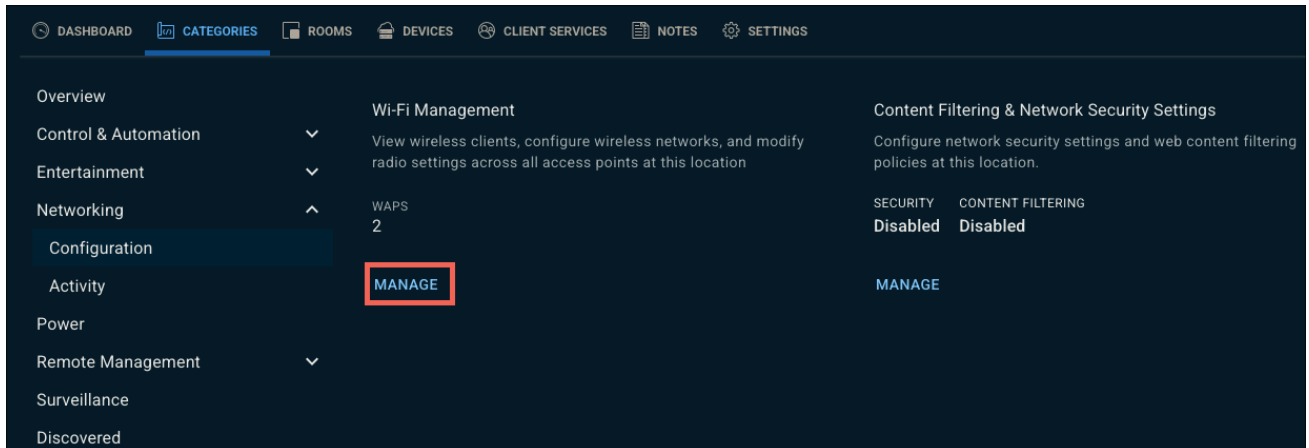
Log In

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

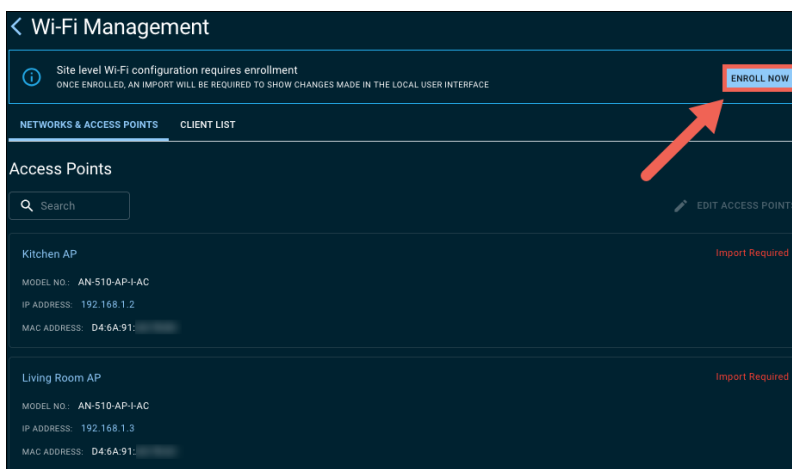


Getting started with Araknis APs

1. Verify the APs are claimed on the customer's site. Read [Claiming devices \(manually and using OvrC Pro\)](#) if you need help with this process.
2. Select a **Customer** and go to **CATEGORIES > Networking > Configuration**.
3. Under Wi-Fi Management, click **MANAGE**.

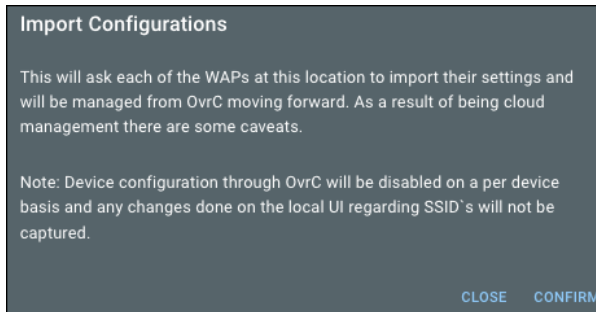


4. The Wi-Fi Management page displays the Access Points claimed on the site. At the top of the page there's a banner informing you that you must enroll the APs in Wi-Fi Management to import the APs displayed at the bottom of the page. Click **ENROLL NOW**.



5. Review the Import Configurations notice before clicking **CONFIRM**.

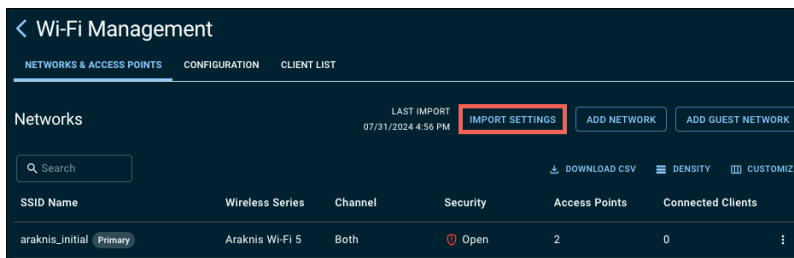
 **Note:** APs enrolled in Wi-Fi Management cannot be configured on a per device basis and any changes made in the AP's local UI are not captured.



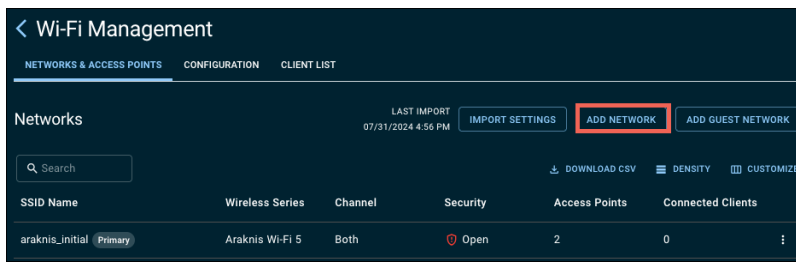
6. Allow OvrC to import the AP configurations. When it's done, the page presents a Networks table with information about each configured SSID and lists more information about the wireless radio settings for each AP.
7. Perform any available firmware updates. If you're using Araknis x20 or x30 series APs, you can use the [Bulk Firmware Update feature](#).

Adding a new network

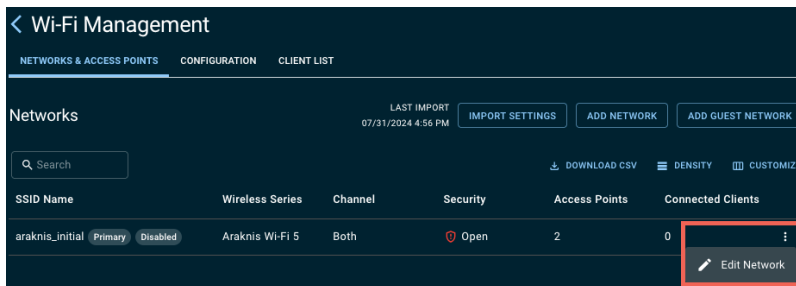
1. For Araknis and Pakedge networks, click the **Import Settings** button to ensure that OvrC does not overwrite changes made in the AP's local UI.



2. Click the **Add Network** button or the **Configuration** tab.



If using Araknis APs you can edit the existing araknis_initial SSID by clicking the three-dot icon and selecting **Edit Network**.



 **Caution:** Any pending changes in the AP's local interface are also applied when you click the **Apply** button.

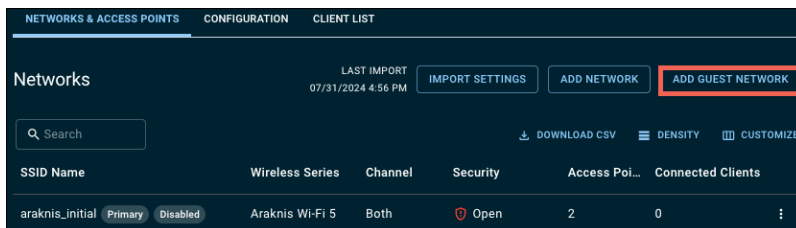
How to add a Guest Network

The Guest Network feature provides limited wireless network access by using a different DHCP pool, security credentials, and SSID.

 **Note:** This feature is not currently supported on Access Networks devices.

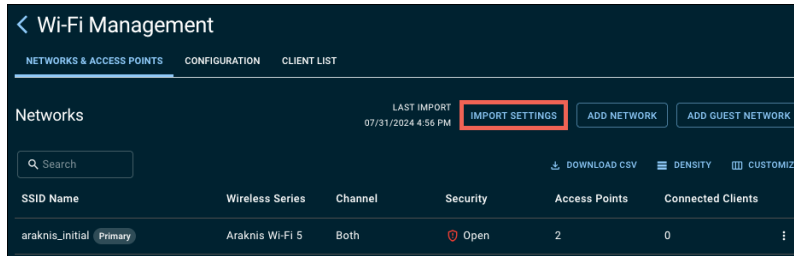
To add a Guest Network:

1. From the **Networks & Access Points** tab, click **Add Guest Network**.

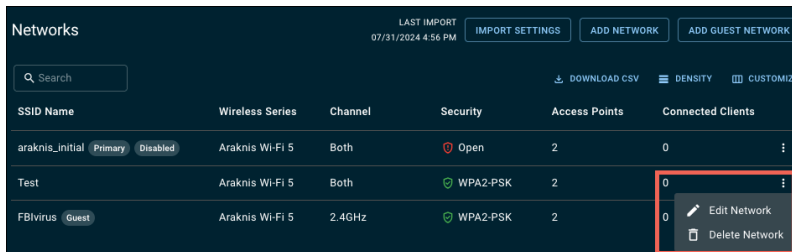


Editing SSIDs

 **Caution:** For Araknis and Pakedge networks, click the **Import Settings** button before making any changes. Failing to do so can result in OvrC overwriting changes made in the AP's user interface.



1. In the row of the SSID you want to edit, click the three-dot icon and selecting **Edit Network**. You can also Delete the network from here.



 **Note:** araknis_initial can be edited or disabled but cannot be deleted.

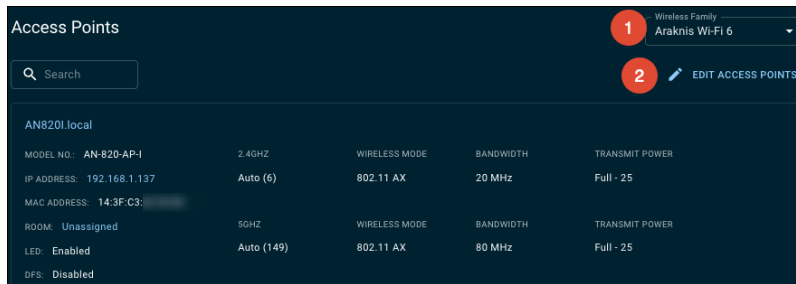
Fine-tuning the wireless radios

Optimize the network by adjusting the wireless radios in each access point. Settings include the Wireless Channel, Wireless Mode, Bandwidth, and Transmit Power. Read about [Wi-Fi Channel Optimization in our Wi-Fi Best Practices](#).

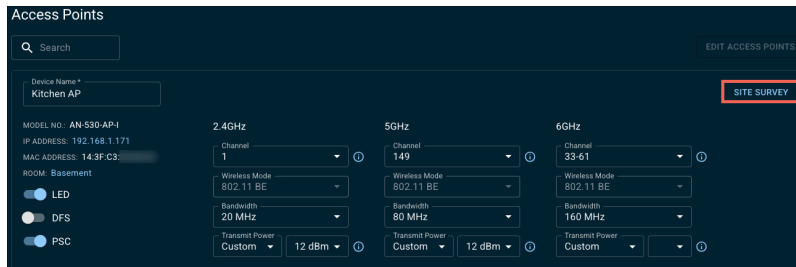
If you're using Araknis x20 or x30 access points, use the [Channel Optimization](#) and [Proximity Check](#) features on the Admin tab. These features make it much easier to determine the best channel to avoid interference and their optimal power settings.

To adjust the radios, click **Edit Access Points**.

 **Note:** If you have multiple AP series on-site, you have to select the **Wireless Family** you want to adjust.



You can also run a **Site Survey** from each access point to see interference from other devices on each radio.



 **Note:** This feature is not supported on Wi-Fi 5 APs. Use the site survey tool in their local UI.

Allow the new site survey window to finish the scan. The **BSSID** field typically displays the MAC address of the radio being scanned. Click the table headers to sort the information.

The 'Run Site Survey' window displays configuration options for two radios. The 2.4GHz radio is set to 'Auto' frequency, '802.11 AX' mode, '20 MHz' bandwidth, and 'Full - 25' power. The 5GHz radio is also set to 'Auto' frequency, '802.11 AX' mode, '80 MHz' bandwidth, and 'Full - 25' power. Below these settings, radio buttons allow selecting between '2.4 Ghz' and '5 Ghz', with '5 Ghz' currently selected. A 'REFRESH SURVEY' button is located to the right. A table lists detected networks with columns for BSSID, SSID, Channel, Utilization, Signal, Encryption, and Type. The table contains four entries. At the bottom are 'CANCEL' and 'SAVE' buttons.

BSSID	SSID	Channel	Utilization	Signal	Encryption	Type
76:9B:E8:...	CODA-B150-5G	161	7%	-89	WPA2-PSK	11AC
40:E1:E4:...	TMOBILE-3B88	161	7%	-87	WPA3-SAE...	11AXA
52:E1:E4:...		161	7%	-87	WPA2-PSK	11AXA
DE:72:23:...		40	2%	-45	WPA2-PSK	11NA

Use the **2.4**, **5**, and **6 GHz** selections to view the survey for each radio. Use the dropdowns to adjust the settings for each.

After making all the adjustments for the AP, click **Save** to close the site survey window.

You can continue adjusting the rest of the APs from the Networks & Access Points tab using the dropdowns. If you're configuring a Wi-Fi 6 AP, you can also enable or disable the **DFS** channels and the AP's **LED**.

The configuration window for device 'AN820I.local' shows details like Model No. (AN-820-AP-1), IP Address (192.168.1.137), MAC Address (14:3F:C3:...), and Room (Unassigned). It features radio settings for 2.4GHz and 5GHz, including frequency, mode, bandwidth, power, and a 'DFS' toggle. At the bottom, there are 'LED' and 'DFS' status indicators.

Click **Apply Changes** to push the changes to the APs.

The Admin tab

The admin tab has a few use cases that differ based on the series of access points you're using. Click the series name to see what's available.

Access Networks

Access Networks allows you to change the system password and select your primary and secondary access points.

The image displays two screenshots of the 'Wi-Fi Management' Admin tab interface. The left screenshot shows the 'Device Credentials' section with a 'CHANGE USERNAME OR PASSWORD' link and 'Preferred Controllers' dropdowns. The right screenshot shows the 'Change Username or Password' modal with fields for current and new passwords, and a password requirements list.

Left Screenshot: Wi-Fi Management - ADMIN

- Section: Device Credentials
- Link: CHANGE USERNAME OR PASSWORD
- Section: Preferred Controllers
- Text: Upon applying this change, the Primary Preferred Controller will become the Main Controller AP and the previous Controller will be rebooted to become a Member AP; the selected Secondary Controller will become Primary Controller once Preferred Primary Controller is down. Please note there may be a brief network disruption when changing the Controller.
- Primary Preferred Controller: A350
- Secondary Preferred Controller: A350 Member

Right Screenshot: Wi-Fi Management - ADMIN (Modal)

- Section: Change Username or Password
- Current Admin Username: admin
- Current Password: (Redacted)
- New Admin Username: (Empty)
- OR
- Enter New Password: (Empty)
- Text: Your password must meet the minimum password requirements outlined below:
- Requirements:
 - Password length: 8 - 64 characters
 - Uppercase: 1 character
 - Lowercase: 1 character
 - Numbers: 1 character
 - Special characters: 1 character
- Confirm New Password: (Empty)
- Buttons: CANCEL, SAVE CREDENTIALS

Araknis international models

Use the admin tab to select the country they're installed in.

Araknis x20 and x30 series access points

Proximity Check

The AP Proximity Check is similar to a Site Survey, except it only shows you how much the claimed access points overlap and how close they are to each other. It's not only helpful for new installs. If it's a takeover job, you can get this information without a floor plan or previous documentation.

To run a Proximity Check, go to the Admin tab and click **Go to AP Proximity Check**.

AP Proximity Check

Detects and warns administrators about strong radio interference between managed access points caused by physical proximity or excessive TX power levels.

This helps prevent poor roaming, reduced throughput, and unstable connections caused by overly strong overlapping coverage.

 [GO TO AP PROXIMITY CHECK](#)

Report [DOWNLOAD RESULTS](#)

Use the RSSI values below to understand how close your access points are to each other. For the best performance and roaming:

- Neighboring APs should ideally see each other between -60 and -65dBm.
- Values stronger than -60 dBm may indicate APs are too close and could create unnecessary overlap.
- Values weaker than -65 dBm are mainly a concern for neighboring APs that clients are expected to roam between; they can indicate limited overlap, which may slow roaming or create coverage gaps.

SIGNAL OVERLAP INDICATOR

Strong Overlap

 0 to -59 dBm Strong neighboring signal; may impact roaming.

AN-530-AP-I-143fc3e3e00c (14:3F:C3:E3:E0:0C) ^

AN-530-AP-I-143fc3e3e018 (14:3F:C3:E3:E0:18)

2.4 GHZ  -69 dBm	5 GHZ  -66 dBm	6 GHZ  -71 dBm
--	--	--

AN-530-AP-I-143fc3e3e018 (14:3F:C3:E3:E0:18) ^

AN-530-AP-I-143fc3e3e00c (14:3F:C3:E3:E0:0C)

2.4 GHZ  -63 dBm	5 GHZ  -67 dBm	6 GHZ  -79 dBm
--	--	--

This helps you determine the power-level settings for each radio on the access points so they do not interfere with each other. This improves device roaming, reduces throughput, and provides more stable connections for clients connecting to each access point.

 **Note:** If an access point is too far away from the others, you won't see an overlapping signal.

Adjust the radio's power levels on the Networks & Access Points tab by clicking **Edit Access Points**.

Access Points			
Search EDIT ACCESS POINTS			
Kitchen AP MODEL NO. AN-530-AP-1 IP ADDRESS: 192.168.1.171 MAC ADDRESS: 14:3F:C3:E3:E3:0C ROOM: Unassigned LED: Enabled DFS: Disabled PSC: Enabled	2.4GHz CHANNEL: 1 WIRELESS MODE: 802.11 BE BANDWIDTH: 20 MHz TRANSMIT POWER: Custom - 12 dBm	5GHz CHANNEL: 149 WIRELESS MODE: 802.11 BE BANDWIDTH: 80 MHz TRANSMIT POWER: Custom - 12 dBm	6GHz CHANNEL: 33 WIRELESS MODE: 802.11 BE BANDWIDTH: 160 MHz TRANSMIT POWER: Custom - 26 dBm

Manually adjust the transmit power for each radio on each access point.

Access Points

EDIT ACCESS POINTS

Device Name *

Kitchen AP

MODEL NO. AN-530-AP-1

IP ADDRESS: 192.168.1.171

MAC ADDRESS: 14:3F:C3:E3:E3:0C

ROOM: Unassigned

LED: ☒

DFS: ☐

PSC: ☐

2.4GHz

Channel: 1

Wireless Mode: 802.11 BE

Bandwidth: 20 MHz

Transmit Power: Custom - 12 dBm

5GHz

Channel: 149

Wireless Mode: 802.11 BE

Bandwidth: 80 MHz

Transmit Power: Custom - 12 dBm

6GHz

Channel: 33-61

Wireless Mode: 802.11 BE

Bandwidth: 160 MHz

Transmit Power: Custom - 26 dBm

Channel Optimization

Channel Optimization creates a schedule for your access points to scan for network interference and move to the best channel for each access point. This reduces service calls for Wi-Fi issues caused by newly added wireless devices from the customer or the neighbor's location.

Under the Admin tab, Click **On-Demand Channel Optimization** to immediately perform a scan and radio assignment to the least busy channel.

 **Pro Tip:** Use the On-Demand feature during the initial configuration.

< Wi-Fi Management

NETWORKS & ACCESS POINTS

CONFIGURATION

CLIENT LIST

ADMIN

Channel Optimization

Auto-scan and Reassign Wi-Fi Channels

☐

Automatically optimize your Wi-Fi performance by scanning for interference and reassigning channels to reduce congestion. Scheduling ensures your network always runs on the best available channel without disrupting your devices.

On-Demand Channel Optimization

Run a manual scan at any time to immediately reassign your Wi-Fi channels for improved connectivity

 FORCE OPTIMIZATION

Channel Optimization

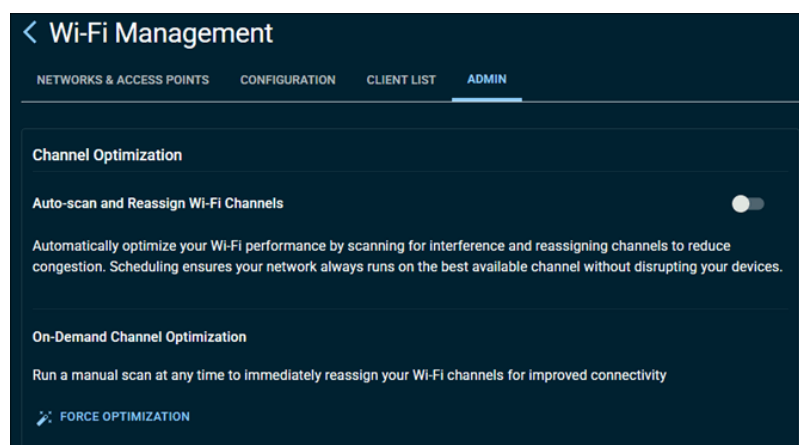
This feature is only available for Araknis x20 and x30 series access points.

Channel Optimization creates a schedule for your access points to scan for network interference and move to the best channel for each access point. This reduces service calls for Wi-Fi issues caused by newly added wireless devices from the customer or the neighbor's location.

Under the Admin tab, Click **On-Demand Channel Optimization** to immediately perform a scan and radio assignment to the least busy channel.



Pro Tip: Use the On-Demand feature during the initial configuration.



Proximity Check

This feature is only available for Araknis x20 and x30 series access points.

The AP Proximity Check is similar to a Site Survey, except it only shows you how much the claimed access points overlap and how close they are to each other. It's not only helpful for new installs. If it's a takeover job, you can get this information without a floor plan or previous documentation.

To run a Proximity Check, go to the Admin tab and click **Go to AP Proximity Check**.

AP Proximity Check

Detects and warns administrators about strong radio interference between managed access points caused by physical proximity or excessive TX power levels.

This helps prevent poor roaming, reduced throughput, and unstable connections caused by overly strong overlapping coverage.

 [GO TO AP PROXIMITY CHECK](#)

Report [DOWNLOAD RESULTS](#)

Use the RSSI values below to understand how close your access points are to each other. For the best performance and roaming:

- Neighboring APs should ideally see each other between -60 and -65dBm.
- Values stronger than -60 dBm may indicate APs are too close and could create unnecessary overlap.
- Values weaker than -65 dBm are mainly a concern for neighboring APs that clients are expected to roam between; they can indicate limited overlap, which may slow roaming or create coverage gaps.

SIGNAL OVERLAP INDICATOR

Strong Overlap

 0 to -59 dBm Strong neighboring signal; may impact roaming.

AN-530-AP-I-143fc3e3e00c (14:3F:C3:E3:E0:0C) ^

2.4 GHZ	5 GHZ	6 GHZ
 -69 dBm	 -66 dBm	 -71 dBm

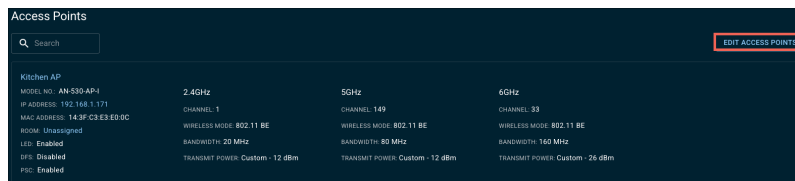
AN-530-AP-I-143fc3e3e018 (14:3F:C3:E3:E0:18) ^

2.4 GHZ	5 GHZ	6 GHZ
 -63 dBm	 -67 dBm	 -79 dBm

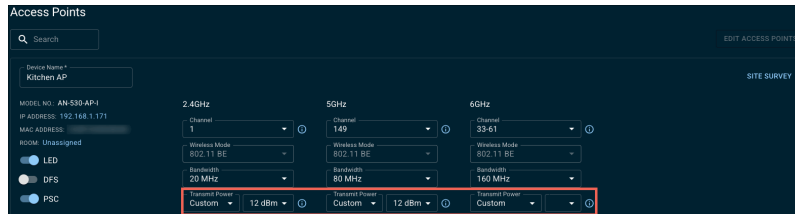
This helps you determine the power-level settings for each radio on the access points so they do not interfere with each other. This improves device roaming, reduces throughput, and provides more stable connections for clients connecting to each access point.

 **Note:** If an access point is too far away from the others, you won't see an overlapping signal.

Adjust the radio's power levels on the Networks & Access Points tab by clicking **Edit Access Points**.



Manually adjust the transmit power for each radio on each access point.



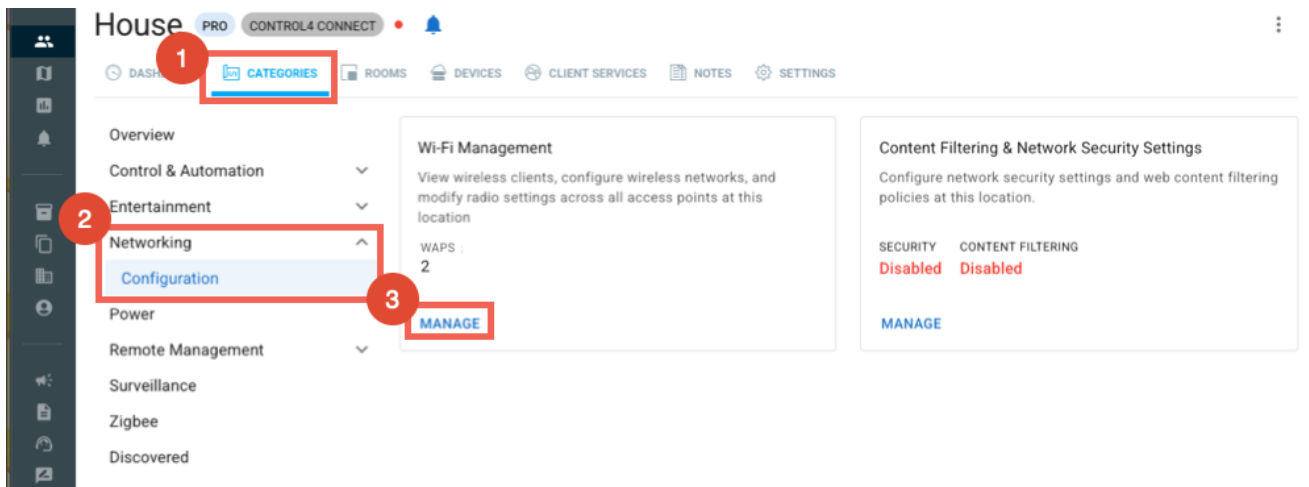
Bulk Firmware Updates in Wi-Fi Management

Use OvrC Wi-Fi Management to simultaneously upgrade the firmware on all the Araknis x20 or x30 series access points (APs) on location.

 **Note:** The Bulk Firmware Update button only appears if a firmware update is available.

To bulk firmware update:

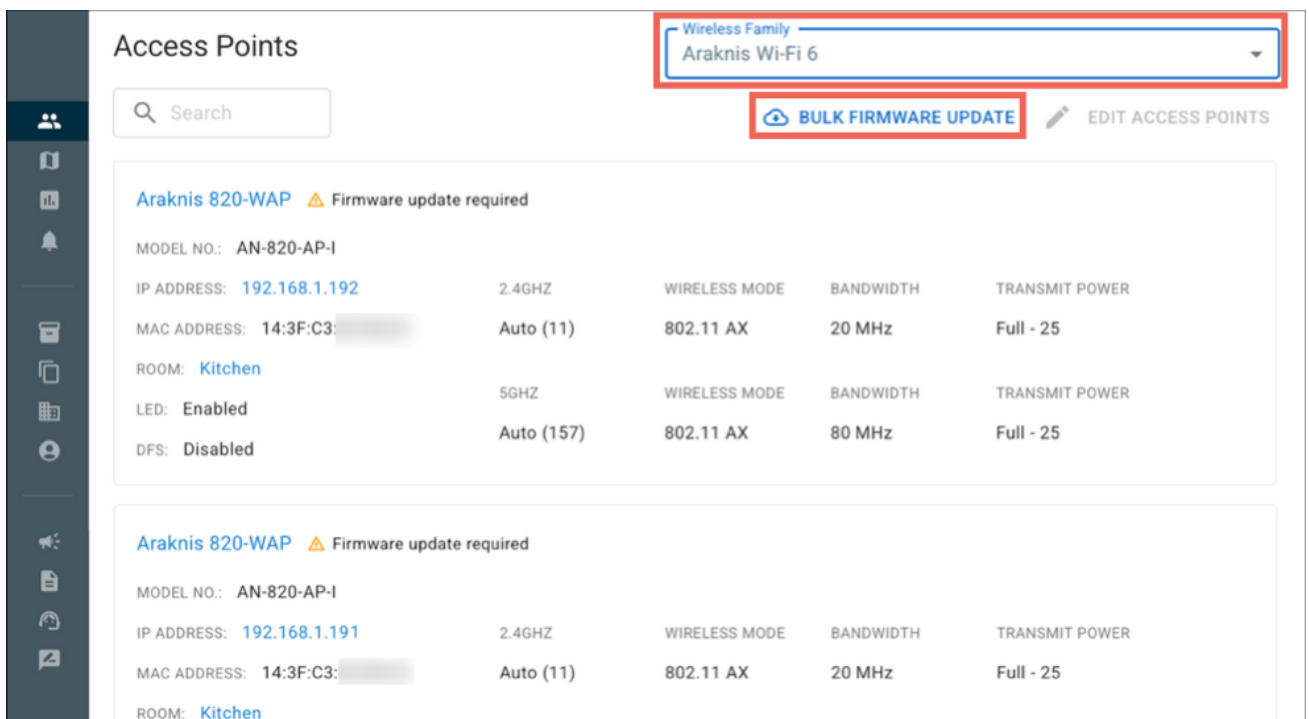
1. Go to the **CATEGORIES** tab > **Networking** > **Configuration**.
2. In the **Wi-Fi Management** tile, click **MANAGE**.



3. If you're using a mix of APs, make sure the **Wireless Family** is set to **Araknis Wi-Fi**

6.

4. Click **BULK FIRMWARE UPDATE**.



OvrC Wi-Fi Management: Wireless Bridge Mode

Wireless Bridge Mode creates a point-to-point connection between two 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.

If you're new to OvrC Wi-Fi Management, [click here](#).

 **Note:** OvrC does not import Wireless Bridge configurations made in the local UI. We recommend creating the bridge in OvrC.

Supported access points:

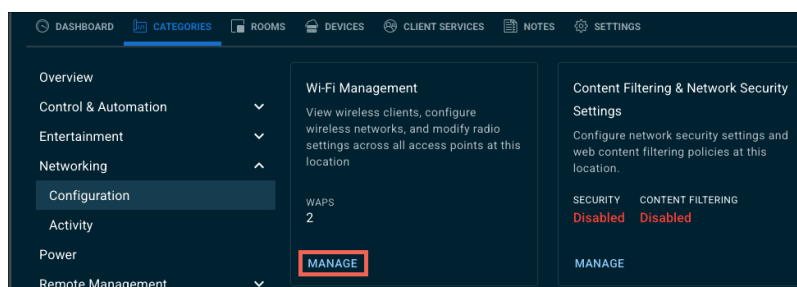
- Araknis 530 series access points on firmware 2.0.02+
- Araknis 830 series access points on firmware 2.0.05+
- Coming soon: Araknis x20 series access points on firmware 2.0.05+

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

You can only have one bridge per access point. If you want to create another wireless bridge, select two different access points.

To create a wireless bridge:

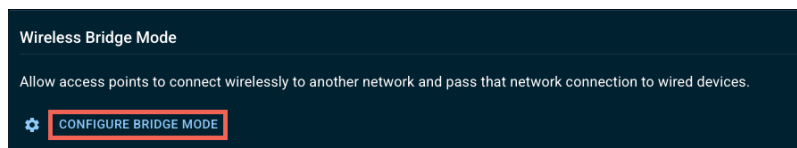
1. Claim your access points in OvrC.
2. Give each access point a meaningful name.
3. Go to **CATEGORIES > Networking > Configuration**.
4. In the Wi-Fi Management tile, click **MANAGE**.



5. If you haven't already, import the access point(s) into Wi-Fi Management. OvrC provides a banner if it detects an access point that hasn't been imported.
6. Perform available firmware updates.
7. Apply any SSID changes to the access point.

 **Note:** You can edit the SSIDs after the bridge has been configured

8. Go to the **ADMIN** tab.
9. Scroll down to the bottom of the page and click **CONFIGURE BRIDGE MODE**.



10. Use the **Access Point 1** dropdown to select one of the access points you want to include in the bridge.

Add Wireless Bridge

Set up a wireless bridge by connecting a bridged access point to a wired access point, enabling network access for wired devices.

Access Point 1 *
Bridge AP

Access Point 2 *
Kitchen AP

Backhaul Radio *
2.4 GHz

SSID Name
an_backhaul-CbzusrtmeQdM

Security Mode *
WPA3-SAE

When setup completes:
Unplug the Ethernet cable from the Bridge device to prevent a network loop.

APPLY

- Click the **Access Point 2** dropdown to select the other access point in the bridge. It does not matter which access point is going to be the wireless bridge.

Add Wireless Bridge

Set up a wireless bridge by connecting a bridged access point to a wired access point, enabling network access for wired devices.

Access Point 1 *
Bridge AP

Access Point 2 *
Kitchen AP

Backhaul Radio *
2.4 GHz

SSID Name
an_backhaul-CbzusrtmeQdM

Security Mode *
WPA3-SAE

When setup completes:
Unplug the Ethernet cable from the Bridge device to prevent a network loop.

APPLY

12. Select which **Backhaul Radio** to use:

- 5 GHz provides faster throughput
- 2.4 GHz has more broadcast range

13. Click **APPLY**.

 **Note:** The SSID Name and Security Mode are read-only. These fields are for informational use.

Add Wireless Bridge

Set up a wireless bridge by connecting a bridged access point to a wired access point, enabling network access for wired devices.

Access Point 1 *
Bridge AP

Access Point 2 *
Kitchen AP

Backhaul Radio *
2.4 GHz

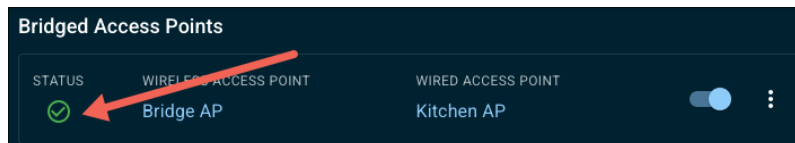
SSID Name
an_backhaul-CbzusrtmeQdM

Security Mode *
WPA3-SAE

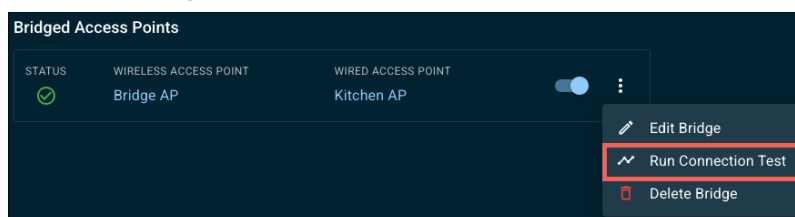
When setup completes:
Unplug the Ethernet cable from the Bridge device to prevent a network loop.

APPLY

14. When you see the bridge appear and the toggle is no longer greyed out, unplug the Ethernet cable from one of the access points to avoid a network loop.
15. Move the access point you unplugged to the remote location and apply power using a DC power supply or PoE injector that meets the access point's power requirements.
16. Allow the remote access point to come online and verify the bridge status is good.



17. Click the **kebab menu**, then select **Run Connection Test** to verify the wireless bridge's throughput and stability.



Here's a test result example:

Connection Test

Verify that your Access Points are properly linked by running a health test.

Bridged Devices

WIRELESS ACCESS POINT	WIRED ACCESS POINT
Bridge AP	Kitchen AP

Connection

RUN TEST

STATUS	LINK UPTIME	HEALTH
Online	0d 0h 1m 52s	62.28% Fair

Test Results

Signal Strength	-26.00 dBm	Excellent
Throughput	41.33 Mbps	Fair
Latency	4.71 ms	Good
Jitter	4.28 ms	Poor
Packet Loss	0	Perfect

CLOSE

Disabling a bridge

Click the toggle to enable or disable the bridge. Disabling a bridge only disables it on the wired access point, so it can be enabled again.

Bridged Access Points

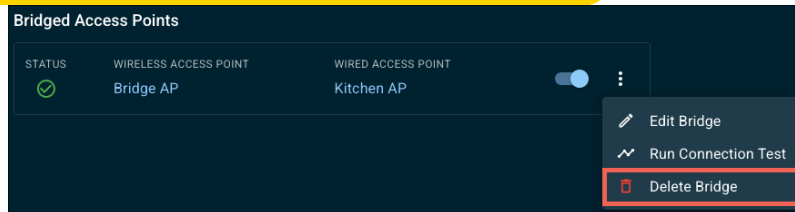
STATUS	WIRELESS ACCESS POINT	WIRED ACCESS POINT	
	Bridge AP	Kitchen AP	

Deleting a bridge

To delete a bridge, click the **kebab menu**, then click **Delete Bridge**.

Deleting the bridge removes the wireless bridge configuration from both access points.

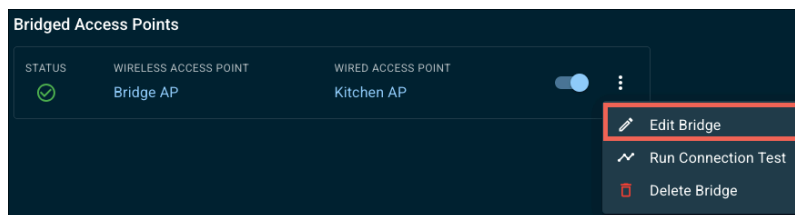
Caution: The bridge access point will not be accessible if you delete the bridge. You must connect it to the LAN again to reach it.



Editing a bridge

You can only change the Backhaul Radio.

To do so, click the **kebab menu**, then click **Edit Bridge**.



Use the **Backhaul Radio** dropdown to change the radio from 2.4 to 5, or vice versa.

Edit Bridge

Access Point 1 *
Kitchen AP

Access Point 2 *

Backhaul Radio *
2.4 GHz

SSID Name
an_backhaul-KvheGiaeYfqk

Security Mode *
WPA3-SAE

DELETE BRIDGE

CANCEL

SAVE

Access Wi-Fi Instantly with Control4

Connecting to Wi-Fi has required balancing ease of use versus network security. The more complex the password, the more annoying it is to connect new devices to Wi-Fi. The easier the password, the less secure your network.

The OvrC Wi-Fi QR Code Agent provides both security and ease of use. With the tap of a button, the user can share Wi-Fi details as well as a QR code that automatically logs the device in to the network.



Requirements and Restrictions

- Only one SSID can be shared via OvrC at a time.
- If SSID sharing is disabled, this agent is likewise disabled.

The agent requires

- Control4 controller and T4 touchscreens on OS 4.0 (X4 platform) or later. This is not supported on T3 touchscreens or HALO remotes.

Automatic installation requires

- an OvrC-enabled access point (Araknis x10 or later, Access Networks Unleashed or later).
- an OvrC customer location mapped to the Control4 customer account.

Automatic Configuration

Automatic configuration is available on sites claimed by OvrC that use supported hardware.

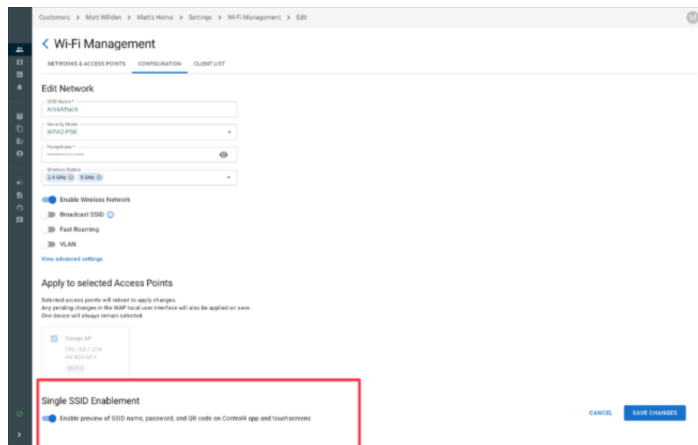
Configuration

1. In OvrC, navigate to Network Site Settings for the location.
2. Select an existing SSID (or create a new one).
3. Activate Single SSID Enablement for that network.

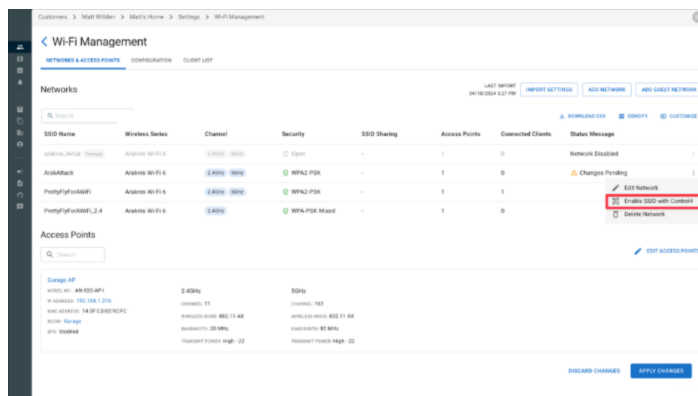
OvrC automatically installs the OvrC Wi-Fi QR Code Agent in the Control4 project and syncs the SSID and password (it resyncs after any changes to the credentials). The agent creates a new Wi-Fi option in the Settings menu of the Control4 app and

If there is no stored Wi-Fi information in the agent, or if SSID sharing is disabled, the Wi-Fi option does not appear in Settings.

If there is no stored Wi-Fi information in the agent, or if SSID sharing is disabled, the Wi-Fi option does not appear in Settings.



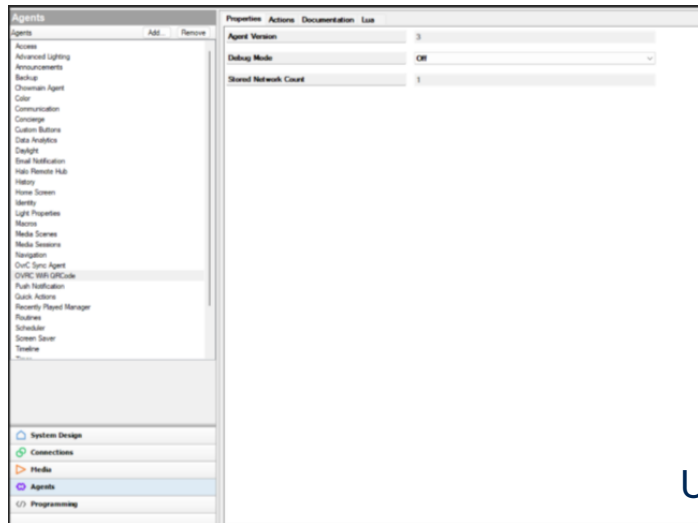
Alternatively, if you are in the SSID window, click Enable SSID with Control4.



Manual Configuration

To use this with unsupported wireless hardware, open Composer, download the OvrC Wi-Fi QR Code Agent, and manually

enter SSID and password information into the agent. If OvrC SSID Sharing is later enabled, this manual entry will be overridden.

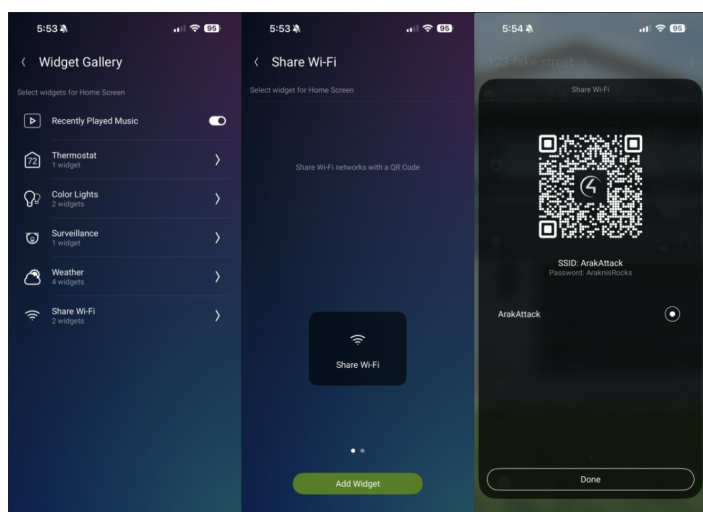


User Experience

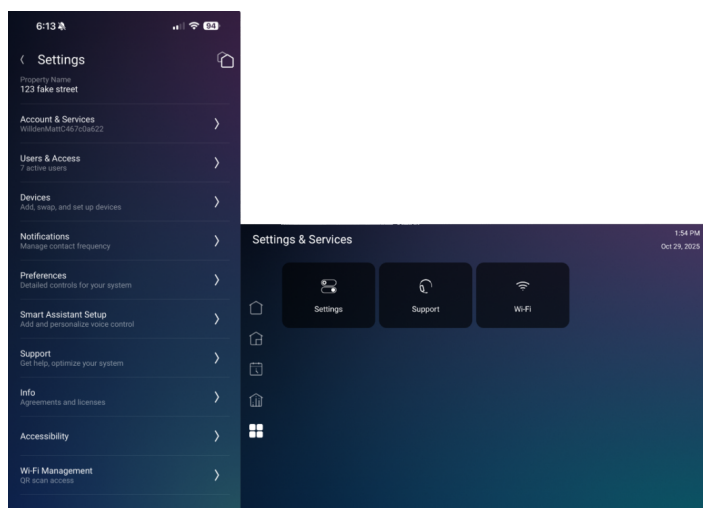
For the best user experience, install the Wi-Fi widget.

1. Go to the Home Screen or any Room Screen.
2. Tap the kebab ☰ menu in the upper right.
3. Tap Add Widgets to open the widget gallery.
4. Locate the new Wi-Fi widget and select it.

Once added to the Home Screen or Room, users can tap the widget and it displays the QR code for easy Wi-Fi sharing. It also displays the SSID and password for devices that can't scan the QR code.



If the user doesn't want their screens to display the Wi-Fi widget, the user can access the QR code by navigating to the Settings menu on a touch panel or mobile device, then viewing the Wi-Fi Management information there.



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.

User Interface Overview

The screenshot displays the Araknis Networks user interface. At the top, a status bar (labeled C) shows 'CLOUD SERVER: Connected', 'System Time: 2022-04-28 10:44:47', and 'System Uptime: 10:34:30'. On the left, a main navigation menu (labeled A) includes sections for Status (System, Wi-Fi Status), Settings (System, LAN, Wi-Fi Setup, Security, Schedule), Maintenance (Ping, Traceroute, File Management, Restart, Log Out), and Advanced. An 'Apply Changes: 0' button is at the bottom of the menu. The main window (labeled B) shows the 'SYSTEM STATUS' page with 'System Information' and 'Wireless Information' sections.

System Information

System Name	AN-820-AP-I
Firmware Version	1.0.04
Service Tag	5721300015186421
Management VLAN ID	Untagged
Power	DC

Wireless Information

	2.4GHz	5GHz
MAC Address	08:00:07:63:00:0A	08:00:07:63:00:0B
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 Changes** 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.

The image displays two side-by-side screenshots of the Araknis Networks web interface, illustrating the process of applying configuration changes.

Left Screenshot (LAN SETTINGS):

- Header:** Araknis Networks logo, Cloud Server: Connected, System Time: 2022-04-28 15:41:01, System Uptime: 15:30:4.
- Left Sidebar:** Status, System, Wi-Fi Status, Settings (selected), LAN, Wi-Fi Setup, Security, Schedule, Maintenance (Ping, Traceroute, File Management, Restart, Log Out), and a red 'Apply Changes: 1' button at the bottom.
- Main Content Area:**
 - IP Settings:** IP Address (192.168.1.109), Subnet Mask (255.255.255.0), DHCP (ON).
 - Interface Settings:** A table with columns LAN1 and LAN2.

	LAN1	LAN2
Speed	1Gbps	Auto
Duplex	Full	Full
- Bottom:** 'Save' and 'Cancel' buttons. A red circle with the number '1' is placed over the 'Save' button.

Right Screenshot (APPLY CHANGES):

- Header:** Araknis Networks logo, Cloud Server: Connected, System Time: 2022-04-28 15:41:56, System Uptime: 15:31:39.
- Left Sidebar:** Same as the left screenshot, with a red 'Apply Changes: 1' button at the bottom.
- Main Content Area:**
 - Unsaved:** A section titled 'Unsaved changes list' showing 'network.phy.speed=1000'. A red circle with the number '3' is placed over this list.
 - Buttons:** 'Apply' and 'Revert' buttons.

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 STATUS	
System Information	
System Name	AN-820-AP-I
Firmware Version	1.0.04
Service Tag	
Management VLAN ID	Untagged
Power	DC

Table Fields

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

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		
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 (SSIDs) configured on the radio interface.
- **Number of Connected Clients:** The amount of wireless clients currently connected on all the configured SSIDs.
- **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.
- **Guest Network:** Indicates if a Guest Network is configured for the radio.

- **Number of Connected Guests:** The amount of wireless clients currently connected to Guest Networks.

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	XXXXXXXXXX	XXXXXXXXXX	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 the 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 IP address issued to the access point 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's 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

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 push
Fri Apr 29 09:48:47 2022 daemon.debug hostapd: ath0: STA [redacted] WPA: FT: Send PMK-R1 push from
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

```

Save Log
Clear 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.

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			Yes	No
Home	Yes	5GHz	WPA3-SAE Mixed			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, including Guest SSIDs.

Path: Status > Wireless interface > Connected Clients

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

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

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

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. Periods (.) or hyphens (-) cannot be the first or last character.
- **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 you to lose 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: / /

Time: : (24-Hour)

☒ **Automatically Get Date and Time**

NTP Server:

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)

☒ **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

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

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

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 > Wireless > Radio Settings

WI-FI SETUP		
Radio Settings		
	2.4GHz	5GHz
Enable Interface	☒	☒
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		☒

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
☒	Home	Both	WPA3-SAE Mixed*	☒	☒	
☒	Home 2.4 Devices	2.4GHz	WPA3-SAE Mixed*	☒	☐	
						Add

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. Options include WPA2-PSK, WPA-PSK Mixed, WPA3, WPA3-SAE Mixed Configuration, and OWE.
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 84 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
☒	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 that can find or see the SSID can connect.
 - **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**.

- **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

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:** 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**, 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

- **Does Fast Roaming work on sites with a mix of x20 APs, 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
☒	Araknis-2.4_GuestNetwork	2.4GHz	Open	☐	☐
☐	Araknis-5.0_GuestNetwork	5GHz	Open	☐	☐
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

Configure users for the local UI 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

SECURITY SETTINGS

User Accounts

Select	Username	Privilege Level	Password	Confirm Password	Delete
☐	araknis	admin	*****	*****	
☐	homeowner	Status	*****	*****	

Add

Edit

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



Pro Tip: 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 access port to connect to the AP. 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

Default: 443



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	 ☐
UPnP	 ☐

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

Configure schedules for Auto Reboot, gateway connection, and SSIDs.

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 : (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 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

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

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 ▾

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

SSID Selection

Market 2 ▾

- 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 ▾

- 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

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

Maintenance

Use this page to test and troubleshoot potential network issues.

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

Start

Stop

98



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

TRACEROUTE TEST

Traceroute Test Parameters

Target IP / Domain Name

Start

Stop

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

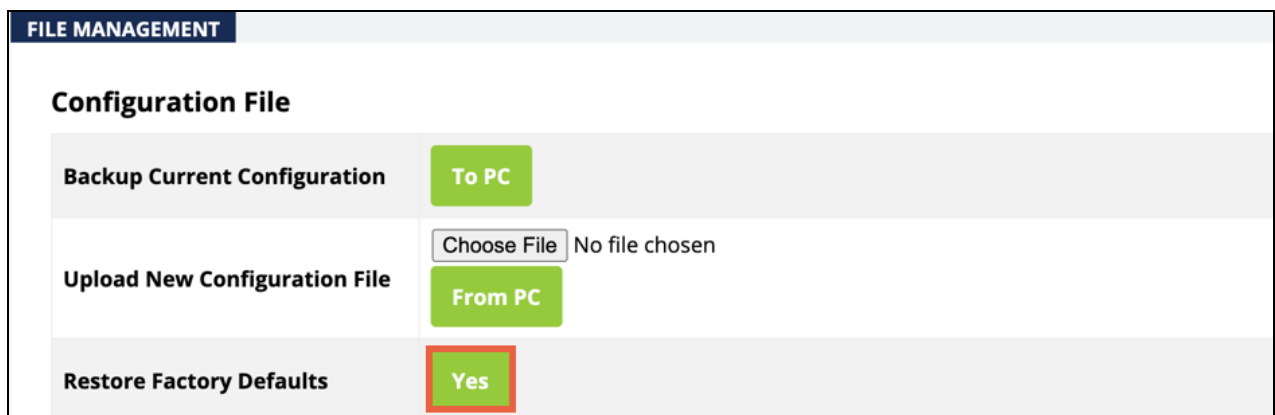
1. Click the **Choose File** button and select a configuration file (.tar file) saved to your computer. The file name appears to the right of the Choose File button.

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.

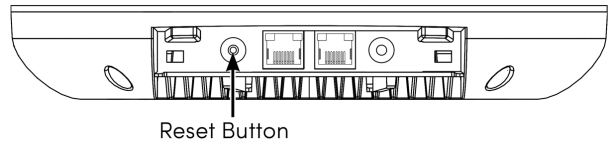
1. Click the **Yes** button to restore the access point to factory default settings, which opens a red alert message.



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.

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

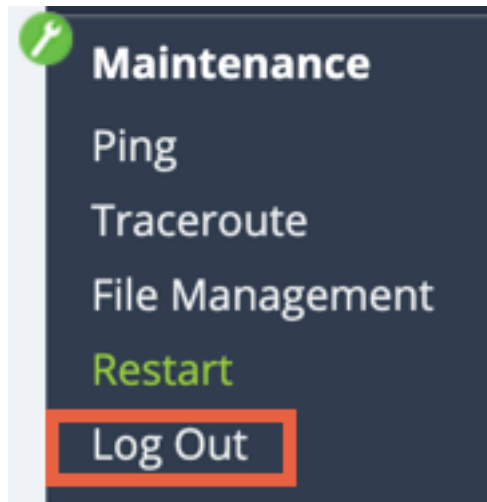
Path: Maintenance > Restart



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

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 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
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	DTIM	MC/BC Threshold
default	☐	☒	☐	☒	1	20
IoT Network	☐	☐	☐	☐	1	64

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.

- **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.

 **Note:** 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.

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

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

☐ 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
		AP	11	53%	-81	WPA2-PSK	11NG
	Honeycutt Orbi	AP	11	53%	-82	WPA2-PSK	11NG
	kiwi	AP	11	53%	-88	WPA2-PSK	11NG
	DIRECT-01-HP OfficeJet 6960	AP	8	34%	-77	WPA2-PSK	11NG
	lx_10_super	AP	11	53%	-85	WPA2-PSK	11NG
	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 %
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.

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
☐	Home	2.4GHz	573 Mbps(1-573)	573 Mbps(1-573)
☐	Home	5GHz	2400 Mbps(1-2400)	2400 Mbps(1-2400)

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.

SNMPv2 Settings

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

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. 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 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			
VLAN Settings			
Enable	SSID ▲	Interface ♦	VLAN ID
☐	Guest	5GHz	
☐	Guest	2.4GHz	
☒	Home	2.4GHz	2
☒	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.

Araknis x20 Series Access Point Firmware

Release Notes

Latest release: v2.0.05

Release date	2026-08-27	
Firmware version	2.0.05	
Product SKUs affected	AN-320-AP-I	AN-520-AP-O
	AN-320-AP-I-1	AN-520-AP-O-1
	AN-520-AP-I	AN-820-AP-I
	AN-520-AP-I-1	AN-820-AP-I-1

Feature Adds

Added Wireless Bridge Mode, enabling point-to-point wireless connectivity between two x20 access points. Also compatible with x30 access points.

[Click here](#) to learn more about Wireless Bridge Mode configuration in OvrC.

Fixes

- Improved macOS client connectivity by addressing Wi-Fi power-save related gateway packet loss.
- Improved MAC Filter reliability when denying clients from the Connected Clients list.
- Fixed Web UI accessibility when using a management VLAN.
- Fixed SSID schedule enforcement for combined SSIDs.

- Resolved an issue where the AP's LED may continue flashing yellow after a firmware update.
- Resolved an issue that could prevent access to the default IP address (192.168.20.253).
- Additional stability and compatibility improvements.
- Cybersecurity vulnerability fixes and improvements.

The full release note history for each access point model is continued on the following pages.

AN-320 Series Access Point Firmware

Release Notes

[Click here to download the latest firmware version.](#)

Firmware v2.0.05 Release Notes

Release date	2026-08-27
Firmware version	2.0.05
Product SKUs affected	AN-320-AP-I AN-320-AP-I-1

Feature Adds

Added Wireless Bridge Mode, enabling point-to-point wireless connectivity between two x20 access points. Also compatible with x30 access points.

[Click here](#) to learn more about Wireless Bridge Mode configuration in OvrC.

Fixes

- Improved macOS client connectivity by addressing Wi-Fi power-save related gateway packet loss.
- Improved MAC Filter reliability when denying clients from the Connected Clients list.
- Fixed Web UI accessibility when using a management VLAN.
- Fixed SSID schedule enforcement for combined SSIDs.
- Resolved an issue where the AP's LED may continue flashing yellow after a firmware update.

- Resolved an issue that could prevent access to the default IP address (192.168.20.253).
- Additional stability and compatibility improvements.
- Cybersecurity vulnerability fixes and improvements.

Firmware v1.4.00 Release Notes

Release date	2025-05-29
Firmware version	1.4.00
Product SKUs affected	AN-320-AP-I AN-320-AP-I-1

Fixes

- Resolved various cybersecurity issues.
- Fixed Web Sessions not timing out/expiring.
- Fixed the Site Survey to display SSIDs with commas.

Improvements

- Updated OvrC agent to improve internet outage reconnection reliability.
- Updated the API for DHCP lease time for the built-in guest network feature.
- Updated error messages for various fields throughout the local UI.
- Updated the System Name requirements to no longer allow a period (.) or hyphen (-) as the first or last character.
- Updated the connected client list to show clients connected to the built-in guest network.
- Updated MC/BC default value logic and threshold.

- Added support for OWE as a security mode for SSIDs.
- Improved logic around the display of an unknown hostname in the client list.

Firmware v1.3.00 Release Notes

Release date	2024-11-07
Firmware version	1.3.00
Product SKUs affected	AN-320-AP-I AN-320-AP-I-1

Fixes

- Fixes the OvrC Wi-Fi Management Site Survey Tool.

Firmware v1.2.00 Release Notes

Release date	2024-06-27
Firmware version	1.2.00
Product SKUs affected	AN-320-AP-I AN-320-AP-I-1

Improvements

- Updated the NTP server options.
- Updated form field validation for ACL blacklist/whitelist accepted characters.
- Added more advanced settings to support IoT heavy installations (DTIM + Directed MC/BC threshold).
- Added the ability to select radios for the primary SSID.

- Various security updates.
- International models: Updated the country code.

Fixes

- Fixed a caching issue where a default UI screen would show up when refreshing the browser window.
- Fixed an issue where Site Surveys took longer to complete than expected when DFS was enabled.

Firmware v1.0.12.09 Release Notes

Release date	2024-06-27
Firmware version	1.0.12.09
Product SKUs affected	AN-320-AP-I AN-320-AP-I-1

- This is the initial release

AN-520 Series Access Point Firmware

Release Notes

[Click here to download the latest firmware version.](#)

Firmware v2.0.05 Release Notes

Release date	2026-08-27
Firmware version	2.0.05
Product SKUs affected	AN-520-AP-I AN-520-AP-I-1

Feature Adds

Added Wireless Bridge Mode, enabling point-to-point wireless connectivity between two x20 access points. Also compatible with x30 access points.

[Click here](#) to learn more about Wireless Bridge Mode configuration in OvrC.

Fixes

- Improved macOS client connectivity by addressing Wi-Fi power-save related gateway packet loss.
- Improved MAC Filter reliability when denying clients from the Connected Clients list.
- Fixed Web UI accessibility when using a management VLAN.
- Fixed SSID schedule enforcement for combined SSIDs.
- Resolved an issue where the AP's LED may continue flashing yellow after a firmware update.

- Resolved an issue that could prevent access to the default IP address (192.168.20.253).
- Additional stability and compatibility improvements.
- Cybersecurity vulnerability fixes and improvements.

Firmware v1.4.00 Release Notes

Release date	2025-05-29
Firmware version	1.4.00
Product SKUs affected	AN-520-AP-I AN-520-AP-I-1

Fixes

- Resolved various cybersecurity issues.
- Fixed Web Sessions not timing out/expiring.
- Fixed the Site Survey to display SSIDs with commas.

Improvements

- Updated OvrC agent to improve internet outage reconnection reliability.
- Updated the API for DHCP lease time for the built-in guest network feature.
- Updated error messages for various fields throughout the local UI.
- Updated the System Name requirements to no longer allow a period (.) or hyphen (-) as the first or last character.
- Updated the connected client list to show clients connected to the built-in guest network.
- Updated MC/BC default value logic and threshold.

- Added support for OWE as a security mode for SSIDs.
- Improved logic around the display of an unknown hostname in the client list.

Firmware v1.3.00 Release Notes

Release date	2024-11-07
Firmware version	1.3.00
Product SKUs affected	AN-520-AP-I AN-520-AP-I-1

Fixes

- Fixes the OvrC Wi-Fi Management Site Survey Tool.

Firmware v1.2.00 Release Notes

Release date	2024-04-25
Firmware version	1.2.00
Product SKUs affected	AN-520-AP-I AN-520-AP-I-1

Improvements

- Updated the NTP server options.
- Updated form field validation for ACL blacklist/whitelist accepted characters.
- Added more advanced settings to support IoT heavy installations (DTIM + Directed MC/BC threshold).
- Added the ability to select radios for the primary SSID.

- Various security updates.
- International models: Updated the country code.

Fixes

- Fixed a caching issue where a default UI screen would show up when refreshing the browser window.
- Fixed an issue where Site Surveys took longer to complete than expected when DFS was enabled.

Firmware v1.0.12 Release Notes

Release date	2022-12-06
Firmware version	1.0.12
Product SKUs affected	AN-520-AP-I AN-520-AP-I-1

- This is the initial release

AN-820 Series Access Point Firmware

Release Notes

[Click here to download the latest firmware version.](#)

Firmware v2.0.05 Release Notes

Release date	2026-08-27
Firmware version	2.0.05
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

Feature Adds

Added Wireless Bridge Mode, enabling point-to-point wireless connectivity between two x20 access points. Also compatible with x30 access points.

[Click here](#) to learn more about Wireless Bridge Mode configuration in OvrC.

Fixes

- Improved macOS client connectivity by addressing Wi-Fi power-save related gateway packet loss.
- Improved MAC Filter reliability when denying clients from the Connected Clients list.
- Fixed Web UI accessibility when using a management VLAN.
- Fixed SSID schedule enforcement for combined SSIDs.
- Resolved an issue where the AP's LED may continue flashing yellow after a firmware update.

- Resolved an issue that could prevent access to the default IP address (192.168.20.253).
- Additional stability and compatibility improvements.
- Cybersecurity vulnerability fixes and improvements.

Firmware v1.4.00 Release Notes

Release date	2025-05-29
Firmware version	1.4.00
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

Fixes

- Resolved various cybersecurity issues.
- Fixed Web Sessions not timing out/expiring.
- Fixed the Site Survey to display SSIDs with commas.

Improvements

- Updated OvrC agent to improve internet outage reconnection reliability.
- Updated the API for DHCP lease time for the built-in guest network feature.
- Updated error messages for various fields throughout the local UI.
- Updated the System Name requirements to no longer allow a period (.) or hyphen (-) as the first or last character.
- Updated the connected client list to show clients connected to the built-in guest network.
- Updated MC/BC default value logic and threshold.

- Added support for OWE as a security mode for SSIDs.
- Improved logic around the display of an unknown hostname in the client list.

Firmware v1.3.00 Release Notes

Release date	2024-11-07
Firmware version	1.3.00
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

Fixes

- Fixes the OvrC Wi-Fi Management Site Survey Tool.

Firmware v1.2.00 Release Notes

Release date	2024-04-25
Firmware version	1.2.00
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

Improvements

- Updated the NTP server options.
- Updated form field validation for ACL blacklist/whitelist accepted characters.
- Added more advanced settings to support IoT heavy installations (DTIM + Directed MC/BC threshold).
- Added the ability to select radios for the primary SSID.

- Various security updates.
- International models: Updated the country code.

Fixes

- Fixed a caching issue where a default UI screen would show up when refreshing the browser window.
- Fixed an issue where Site Surveys took longer to complete than expected when DFS was enabled.

Firmware v1.0.5 Release Notes

Release date	2023-12-07
Firmware version	1.0.5
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

Improvements

- Resolved an issue that caused all client devices to unexpectedly disconnect from the AP, prompting some devices to enter the network password

Firmware v1.0.2 Release Notes

Release date	2022-12-07
Firmware version	1.0.2
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

Improvements

- DFS default value set to Disabled. (The state of the DFS value does not change after updating the firmware. If the AP is reset to factory after the firmware update, the DFS value is set to Disabled)
- Improved device latency and connection stability
- Updated Security
- UI fixes and improvements

Fixes

- Resolved 2.4GHz radio client handshake
- Fixed Radio configuration when set to Wireless “N” using OvrC
- Fixed Gateway Connection Monitor
- Resolved a bug so the “System Name” now updates correctly

Firmware v1.0.1 Release Notes

Release date	2022-09-13
Firmware version	1.0.11
Product SKUs affected	AN-820-AP-I AN-820-AP-I-1

- This is the initial release

AN-520 Series Outdoor Access Point

Firmware Release Notes

[Click here to download the latest firmware version.](#)

Firmware v2.0.05 Release Notes

Release date	2026-08-27
Firmware version	2.0.05
Product SKUs affected	AN-520-AP-O AN-520-AP-O-I

Feature Adds

Added Wireless Bridge Mode, enabling point-to-point wireless connectivity between two x20 access points. Also compatible with x30 access points.

[Click here](#) to learn more about Wireless Bridge Mode configuration in OvrC.

Fixes

- Improved macOS client connectivity by addressing Wi-Fi power-save related gateway packet loss.
- Improved MAC Filter reliability when denying clients from the Connected Clients list.
- Fixed Web UI accessibility when using a management VLAN.
- Fixed SSID schedule enforcement for combined SSIDs.
- Resolved an issue where the AP's LED may continue flashing yellow after a firmware update.

- Resolved an issue that could prevent access to the default IP address (192.168.20.253).
- Additional stability and compatibility improvements.
- Cybersecurity vulnerability fixes and improvements.

Firmware v1.4.00 Release Notes

Release date	2025-05-29
Firmware version	1.4.00
Product SKUs affected	AN-520-AP-O AN-520-AP-O-1

Fixes

- Resolved various cybersecurity issues.
- Fixed Web Sessions not timing out/expiring.
- Fixed the Site Survey to display SSIDs with commas.

Improvements

- Updated OvrC agent to improve internet outage reconnection reliability.
- Updated the API for DHCP lease time for the built-in guest network feature.
- Updated error messages for various fields throughout the local UI.
- Updated the System Name requirements to no longer allow a period (.) or hyphen (-) as the first or last character.
- Updated the connected client list to show clients connected to the built-in guest network.
- Updated MC/BC default value logic and threshold.

- Added support for OWE as a security mode for SSIDs.
- Improved logic around the display of an unknown hostname in the client list.

Firmware v1.3.00 Release Notes

Release date	2024-11-07
Firmware version	1.3.00
Product SKUs affected	AN-520-AP-O AN-520-AP-O-1

Fixes

- Fixes the OvrC Wi-Fi Management Site Survey Tool.

Firmware v1.2.00 Release Notes

Release date	2024-04-25
Firmware version	1.2.00
Product SKUs affected	AN-520-AP-O AN-520-AP-O-1

Improvements

- Updated the NTP server options.
- Updated form field validation for ACL blacklist/whitelist accepted characters.
- Added more advanced settings to support IoT heavy installations (DTIM + Directed MC/BC threshold).
- Added the ability to select radios for the primary SSID.

- Various security updates.
- International models: Updated the country code.

Fixes

- Fixed a caching issue where a default UI screen would show up when refreshing the browser window.
- Fixed an issue where Site Surveys took longer to complete than expected when DFS was enabled.

Firmware v1.0.12 Release Notes

Release date	2023-03-02
Firmware version	1.0.12
Product SKUs affected	AN-520-AP-O AN-520-AP-O-1

- This is the initial release