

# Campus B-01 Wireless Lab Guide

## WiFi setup



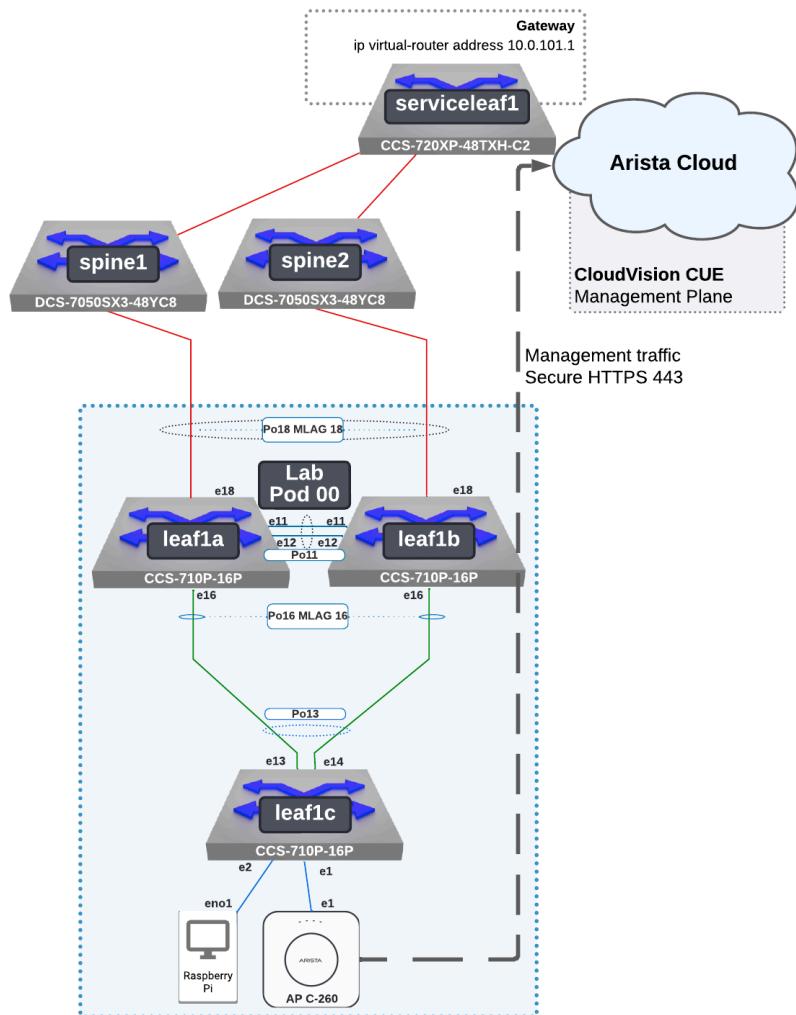
### Links:

1. This Lab Guide:
  - a. <https://github.com/arista-rockies/Workshops/tree/main/Campus>
2. Lab Floor Plan Download:
  - a. <https://tinyurl.com/wififloorplan> [Arista-rockies Github]

# Table of Contents

<b>Arista WiFi Solution Diagram.....</b>	<b>2</b>
<b>1. CloudVision Cognitive Unified Edge CV-CUE Access.....</b>	<b>3</b>
Launchpad.....	4
Add a User and Assign Privileges.....	5
Assign User Privileges.....	6
WiFi Device Registration - Reference section.....	10
2. CV-CUE CloudVision Wifi Access.....	12
3. Assign AP Name.....	15
4. Managing the Configuration Hierarchy.....	17
Customize the Locations Hierarchy:.....	17
Creating Folders:.....	18
Creating Floors:.....	19
Move AP to destination folder.....	23
5. Creating an SSID.....	27
6. Troubleshooting.....	34
7. Floor Plans.....	42
8. Dashboard - Client Journey.....	46

# Arista WiFi Solution Diagram



**Prerequisites:** The Arista Wireless AP management plane (CUE) is hosted within Arista's public cloud presence, worldwide. In order to complete this lab section, a default gateway is preconfigured by event staff to facilitate internet connectivity.

For more information on the TCP/UDP ports and protocols involved for management functions, see the links below:

<https://wifihelp.arista.com/post/access-point-wireless-manager-communication>

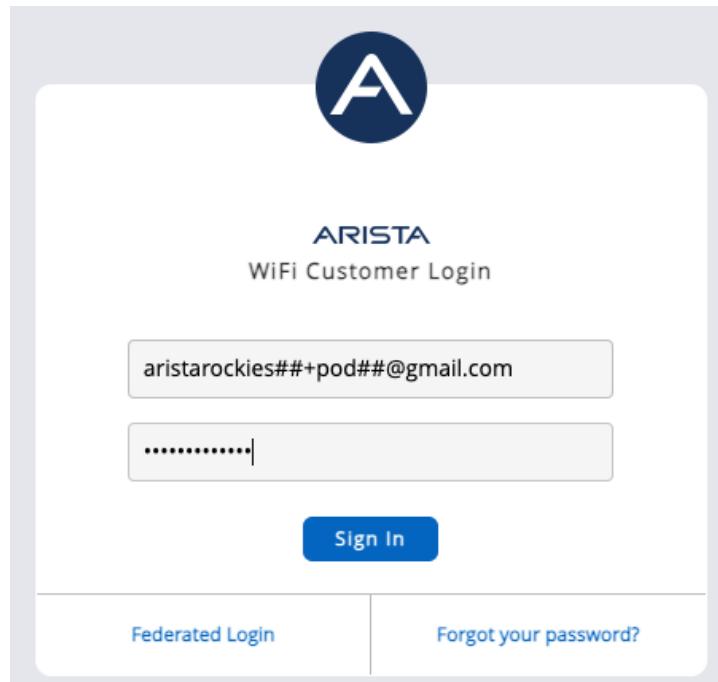
<https://wifihelp.arista.com/post/tcp-and-udp-ports-used-by-arista-wi-fi-products>

# 1. CloudVision Cognitive Unified Edge CV-CUE Access

Go to the Arista CloudVision CUE portal via: <https://launchpad.wifi.arista.com/>

User Login is: *[Provided by event staff]*

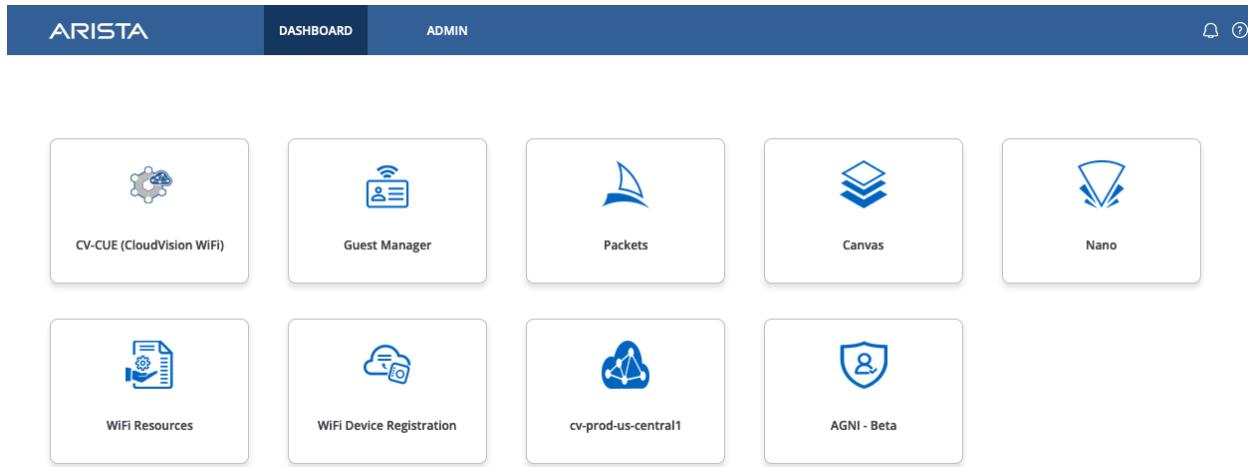
User Passwords are: *[Provided by event staff]*



Click **Sign In**

# Launchpad

Launchpad is the portal to access your Arista cloud services including **WiFi Management** (CV-CUE) and **AGNI** (Network Access Control). When you open the launcher, you are presented with management applications on the Dashboard menu and access controls with the Admin menu.



## Dashboard Applications Summary:

- **CV-CUE (CloudVision WiFi)** - Wireless management and monitoring
- **Canvas** is used for access portal splash pages, and marketing Campaign management.
- **Guest Manager** Analyze and report on user activity within your environment.
- **Nano** allows you to manage your environment from your smartphone
- **Packets** is an online packet capture (.pcap) debug tool allowing you to examine the association and packet information.
- **WiFi Resources** includes documentation and eLearning has 6 ½ hours of training, also included.
- **WiFi Device Registration** is the process for importing APs onto your account
- **AGNI - Beta** Arista Guardian for Network Identity (Network Access Control)

# Add a User and Assign Privileges

First, use the Admin menu to add a user.

Click on the **Admin** Tab at the top of the Launchpad window:

The screenshot shows the Arista Launchpad interface with the Admin tab highlighted by a red box. Below the tabs, there is a navigation bar with 'Users' (highlighted), 'Keys', 'Profiles', 'Logs', and 'Settings'. A message below the navigation bar says 'Click a row to edit user account and its privileges. Click on : icon for more user account management options.' There is a 'New User' button and a search bar. A table below lists users with columns: Full Name, Login ID, Email, Last Login, and Active Profile. One user is listed: 'User1 Pod13' with email 'aristarockies1+pod13@gmail.com', last login '08/09/2024 10:31 AM', and active profile 'Admin'. A help icon is also present.

Overview of Launchpad Admin menu:

- **Users** - Assign Access to users with different access levels as well as to specific folders
- **Keys** - Used with API integrations
- **Profiles** - Defines Access levels to CV-CUE, LaunchPad, and Guest Manager
- **Logs** - Download User Action Logs
- **Settings** - Lockout Policy, Password Policy, and 2-Factor settings
- **Account Settings** - Change your Timezone and Change your password.

CloudVision CUE authenticates users via SAML directory integration or via the Launchpad identity providers. These can be customized with local users in Launchpad or directory single-sign-on users.

<https://arista.my.site.com/AristaCommunity/s/article/Integrating-Third-Party-SAML-Solution-Providers-with-Arista-CV-CUE>

Under the Admin tab, Users section, Click **New User**

This screenshot is similar to the one above, showing the Admin tab and the Users section. However, the 'New User' button is now highlighted with a red box. The rest of the interface, including the table of users, remains the same.

Let's create a fake user as an example. Complete at least the following fields with false information: **Login ID**, **Email address**, **first name**, and **timezone** then click **Save in the lower right**.

Save and continue to configure service privileges.

Login ID: \* aristarock@gmail.com

Email: \* aristarock@gmail.com

First Name: \* Adrian

Last Name: Balboa

Timezone: \* America/Denver (GMT -06:00)

User Type : Local

Cancel Save

When you click Save, a welcome email message will be sent to the user with access link. Next let's assign privileges to the newly created user.

## Assign User Privileges

aristarock@gmail.com

Email: \* aristarock@gmail.com

First Name: \* Adrian

Last Name: Balboa

Timezone: \* America/Denver (GMT -06:00)

User Type : Local

And click the toggle to the right of **Wireless Manager** to enable this service for the newly created user.

The screenshot shows the Arista Cloud UI interface. At the top, there's a navigation bar with tabs: 'Users' (which is selected), 'Keys', 'Profiles', 'Logs', and 'Settings'. Below the navigation bar, the user 'aristarockie' is selected. On the right, there are two tabs: 'Account Info' and 'Service Privileges' (which is selected). Under 'Service Privileges', there's a section titled 'Select Profile:' with a dropdown menu set to 'Custom'. A note below says 'You can assign privileges only on those services on which you have highest role.' Below this, there are four service icons: 'Launchpad', 'Wireless Manager' (which has a red box around its toggle switch), 'Guest Manager', and another 'Wireless Manager' icon. Each service has an 'OFF' toggle switch below it.

- Set User Role: **Viewer**
- Check the boxes for **Wi-Fi Access Management** and/or **WIPS Management**.
- Select the default top level locations

The screenshot shows the Arista Cloud UI interface under the 'Services' section, specifically for 'Wireless Manager'. At the top, there's a navigation bar with tabs: 'Users' (selected), 'Keys', 'Profiles', 'Logs', and 'Settings'. Below the navigation bar, the user 'aristarockie' is selected. A note says 'Profile: Custom'. Under 'Services', the path 'Services > Wireless Manager' is shown. On the left, there are sections for 'User Role' (set to 'Viewer'), 'Wi-Fi Access Management' (checkbox checked), 'WIPS Management' (checkbox checked), and 'Allowed Locations' (dropdown open, showing 'Locations' and 'Staging Area' with checkboxes, where 'Locations' is checked and highlighted with a red box). At the bottom, there are 'Cancel' and 'Save' buttons.

**Click Save to save the user permissions**

Click **Users** to return to the list of all users.



Click the 3-dots icon next to the newly created example user and click Lock / Unlock to toggle whether this user is allowed to log in

Full Name	Login ID	Email	Last Login	Active Profile
Rockies Balboa	aristarockie@gmail.com	aristarockie@gmail.com		Custom
Adrian Balboa	aristarockie@gmail.com	aristarockie@gmail.com		Custom
Arista Rockies4+Pod1	aristarockies4+pod1@gmail.c...	aristarockies4+pod1@gmail.com	07/18/2024 3:56 PM	Admin
Arista Rockies2+Pod1	aristarockies2+pod1@gmail.c...	aristarockies2+pod1@gmail.com	07/30/2024 5:35 PM	Admin
Arista Rockies3+Pod1	aristarockies3+pod1@gmail.c...	aristarockies3+pod1@gmail.com	06/11/2024 1:11 PM	Admin

Delete the example user by selecting the 3-dots again

Full Name	Login ID	Email	Last Login	Active Profile
Rockies Balboa	aristarockie@gmail.com	aristarockie@gmail.com		Custom
Adrian Balboa	aristarockie@gmail.com	aristarockie@gmail.com		Custom
Arista Rockies4+Pod1	aristarockies4+pod1@gmail.c...	aristarockies4+pod1@gmail.com	07/18/2024 3:56 PM	Admin
Arista Rockies2+Pod1	aristarockies2+pod1@gmail.c...	aristarockies2+pod1@gmail.com	07/30/2024 5:35 PM	Admin
Arista Rockies3+Pod1	aristarockies3+pod1@gmail.c...	aristarockies3+pod1@gmail.com	06/11/2024 1:11 PM	Admin

Click **Yes** to confirm the prompt

**Confirm**

*This will delete the user permanently. Are you sure you want to continue?*

No      Yes

Click **Settings** to view additional authentication configuration options such as 2-Factor Authentication and password policies:



Users    Keys    Profiles    Logs    **Settings**

#### Lockout Policy:

Maximum failed login attempts:  in  minutes

Lockout period:  minutes

Message displayed on lockout:

#### Password Policy:

##### ▼ Password Strength

Minimum password length:  characters

Password Complexity:

- At least 1 number
- At least 1 lower-case letter
- At least 1 upper-case letter
- At least 1 special character (! @ # \$ % ^ & \* () = + { } : ; < > , ` - ? \_ | . )
- Not contain the username, firstname and lastname

##### ► Password Expiry / Uniqueness

#### Opt-Outs:

- I do not want Arista Networks to access my account as Administrator.

#### 2-Factor Authentication:

- 2-Factor Authentication
- Force 2-Factor Authentication

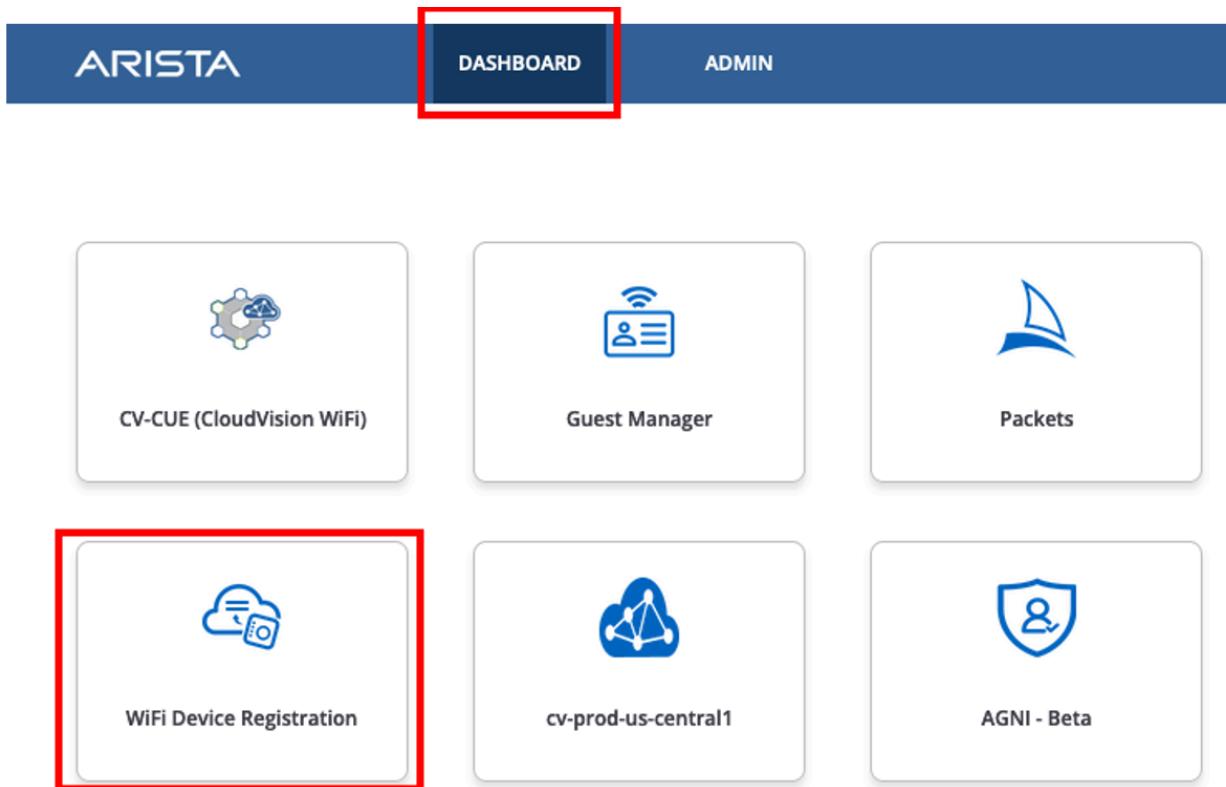
#### Allowed IPv4 Addresses for Log In:

Do not make any further changes in the Settings menu.

## WiFi Device Registration - Reference section

**Reference information below - these steps have already been done for you by event staff**

**\*Note:** Arista AP serial numbers are automatically assigned to the user's CV-CUE staging area when purchased. In addition, specific devices can be registered for management using the [WiFi Device Registration](#) function, accessible from Launchpad Dashboard.



Device registration requires both the Serial Number and Registration Key information found on the back of the APs. Additionally, a CSV containing this information can be uploaded for bulk registration operations.

The screenshot shows the Arista WiFi Device Registration interface. At the top, there's a blue header bar with the Arista logo on the left and "WIFI DEVICE REGISTRATION" on the right. Below the header, a dark blue navigation bar has "Access Points" highlighted in white. Underneath is a light blue "Import" button. The main content area has a light gray background and a table header row with columns for "Serial Number" and "Service". A single entry is listed: "E4D12452" under Serial Number and "Wireless Manager" under Service.

Within the Import Function you can provide individual AP serials and keys or upload a CSV.

This screenshot shows the same Arista WiFi Device Registration interface, but the "Import" button is now highlighted in blue. Above it are two buttons: "Upload CSV" and "Sample CSV". Below these buttons is a table with three columns: "Serial Number", "Registration Key", and "Operation Status". Two entries are shown: "UUUUUUUUUUUU" and "UUUUUUUUUUUU".

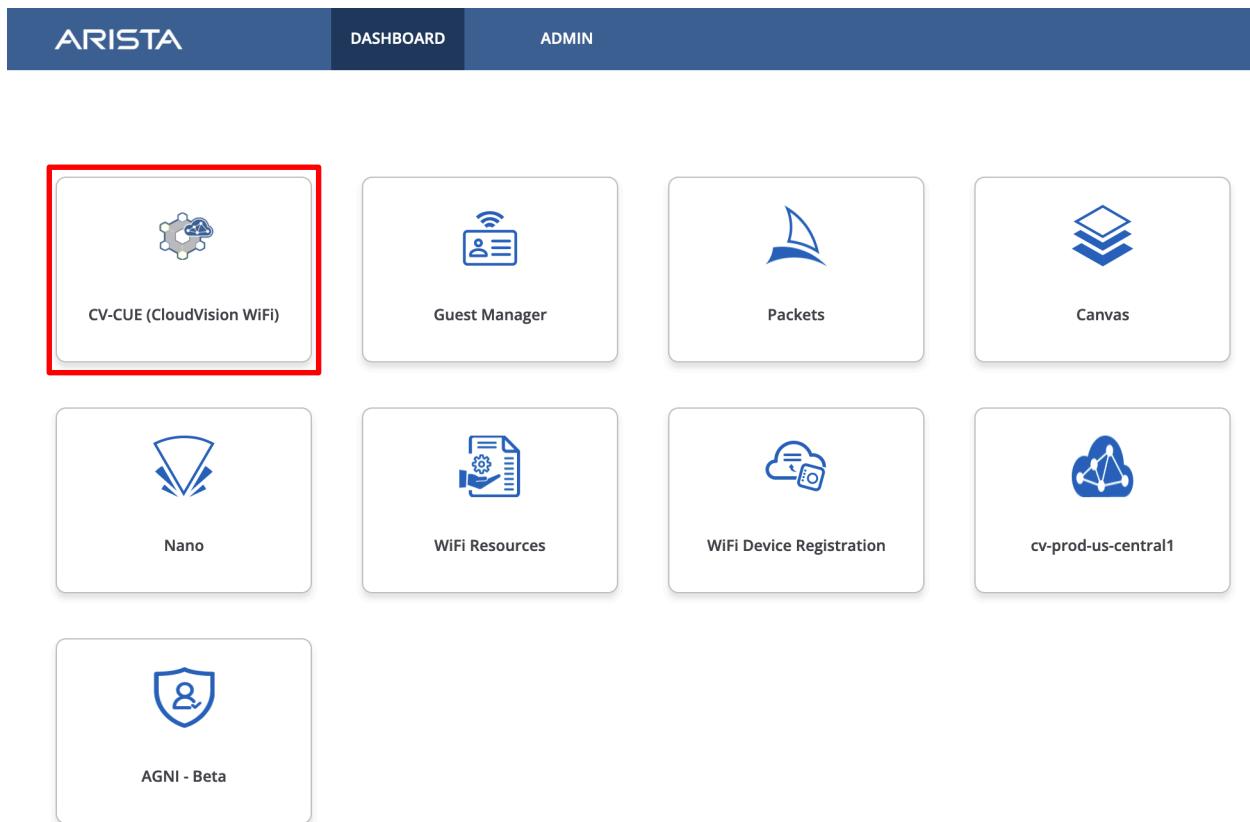
End of Section 1 Exercise: CV-CUE Access

The next section begins on the following page.

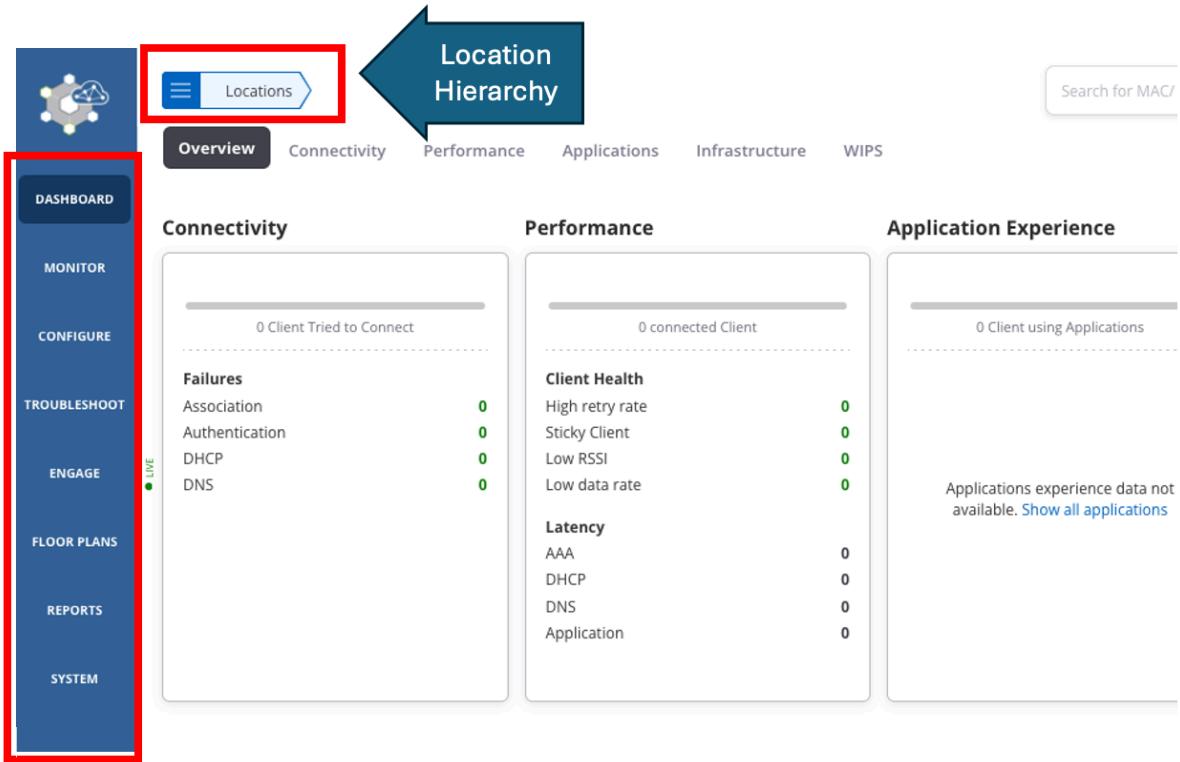
## 2. CV-CUE CloudVision Wifi Access

CloudVision CUE - Cognitive Unified Edge, provides the management plane and monitoring functions for the Arista WiFi solution.

Click on the **CV-CUE (CloudVision WiFi)** Tile in the LaunchPad from the Dashboard menu.



When the CV-CUE interface launches, you are presented with an initial dashboard to monitor your wireless environment at a glance, we will revisit these metrics later in the lab. Since this is a new setup the initial dashboard screen will be mostly empty.



Use the left menu bar to select monitoring and configuration functions.

Take careful note of the **Locations Hierarchy** indicator throughout the user interface. This indicates which container you are monitoring or configuring.

The primary menu navigation functions are the following:

**Dashboard** - Alerts, Client Access, Infrastructure health, Application Experience, and WIPS

**Monitor** - Monitor and explore Clients, APs, Radios, SSIDs, Application traffic, Tunnels

**Configure** - WiFi SSIDs, APs and Radios, Tunnels, RADIUS, and WIPS settings

**Troubleshoot** - Client connection test, packet trace, live debug logs, historic logging

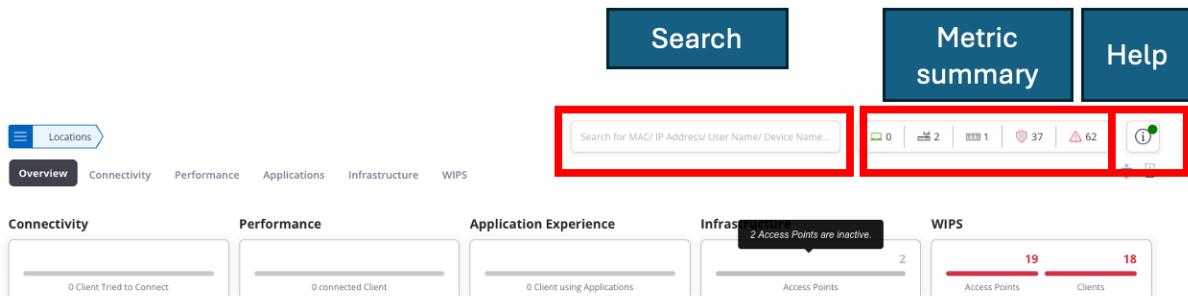
**Engage** - User insights, Presence, Usage, 3rd party integrations

**Floor Plans** - Floor layouts and AP location map view

**Reports** - Detailed information for Infrastructure APs/Radios, Client Connectivity and Experience, WIPS detections

**System** - Locations Hierarchy, AP Groups, 3rd party server settings, keys and certificates

In addition to the menu bar navigation and Locations Hierarchy, the UI provides a common Search bar, Metric summary, and Help button throughout workflows.



End of lab section.

### 3. Assign AP Name

Access points that successfully receive an IP address, DNS, and default gateway, via DHCP, and have connectivity over HTTPS/TCP/443 to CV-CUE will be shown within CV-CUE under **Monitor > WiFi**



Select the **Access Points** section and observe the discovered AP and default name “Arista\_” and the last 3 bytes of the MAC address.

Customize the AP’s name by clicking the **3-dots menu** and **Rename**

A screenshot of the CV-CUE interface. On the left, there's a sidebar with 'DASHBOARD', 'MONITOR' (selected and highlighted with a red box), and 'CONFIGURE'. The main area shows 'Locations' (selected), 'Clients', 'Access Points' (highlighted with a red box), and 'Radios'. Below that, it says '1 Access Points' and has a 'Access Points Explorer' button. A red box highlights the 'Access Points' button. At the bottom, there's a table with a single row for 'Arista\_30:42:2F'. To the right of the table is a context menu with options: Troubleshoot, Certificate, Customize, Configure Alert, Update Firmware, Assign/Reassign to a Group, Locate (Early Access), Remove Access Points from Group, Reboot, and Rename. A red box highlights the three-dot menu icon next to the AP entry in the table.

Give the AP a name such as: “POD-##-FL1” where ## is a 2 digit character between 01-20 that was assigned to your lab/Pod.

The screenshot shows a network management interface with a sidebar on the left containing 'DASHBOARD', 'MONITOR' (which is selected), and 'CONFIGURE' buttons. The main area has a header with 'Locations' (selected), 'WiFi', 'Clients', 'Access Points' (selected), 'Radios', 'Active SSIDs', 'Application Visibility', and 'Tu'. Below this, it says '1 Access Points' with a refresh icon and a link to 'Access Points Explorer'. A table lists one access point: 'POD-01-FL1' with MAC address '30:86:2D:30:42:2F'. The table has columns for Name, Update, and MAC Address.

Name	Update	MAC Address
POD-01-FL1	<input checked="" type="checkbox"/>	30:86:2D:30:42:2F

## Lab Section Completed.

---

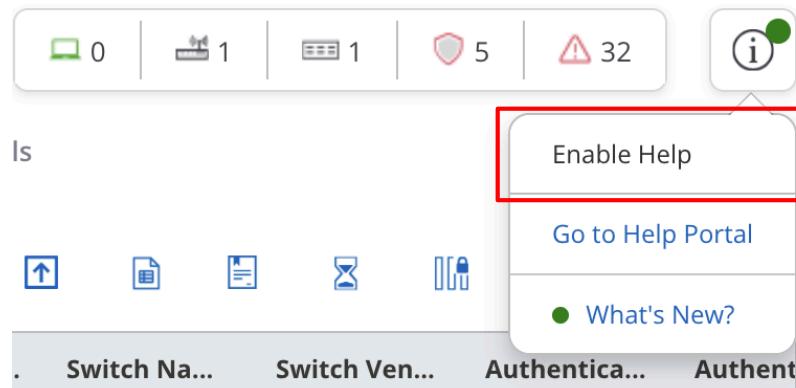
## 4. Managing the Configuration Hierarchy

In CloudVision CUE the configuration is hierarchical.

Shared configuration is added and edited at the parent containers. These settings are inherited down the hierarchy. For example, a guest SSID you wish to be configured on all devices can be configured at the top.

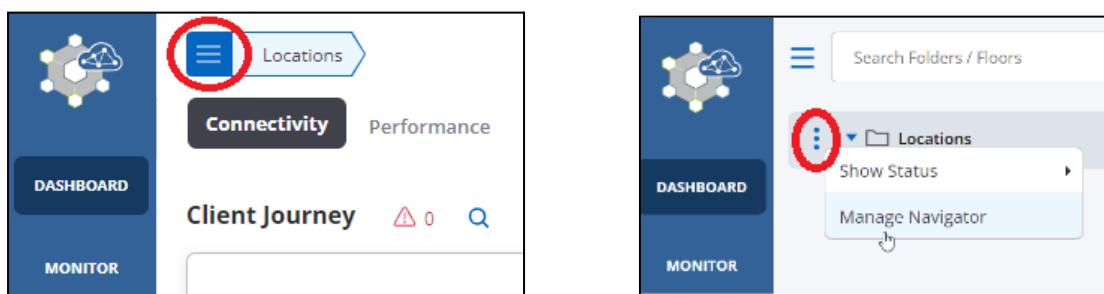
Child containers can define the sites, buildings, functions, or any other logical construct of the wireless network and allows you to add settings at those specific levels.

**\*Note:** At any time you can go to the question mark on the top right and choose “Enable Help” to make fields have notations, or search in the “Go To Help Portal”.



### Customize the Locations Hierarchy:

Expand the “Locations” pane by clicking on the hamburger icon toward the top left of the screen. Now select the three dots to the left of “Locations” and click on “Manage Navigator”.



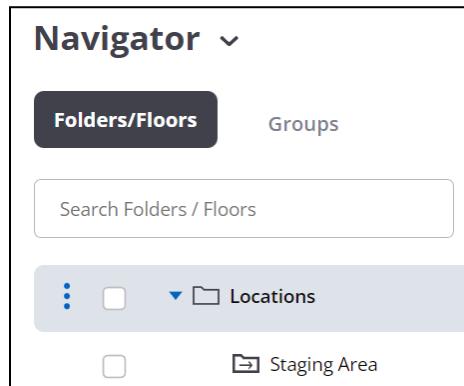
“Manage Navigator” is where you create and manage the hierarchy of: **Folders, Floors, and Groups.**

- **Folders** typically represent a company, branch office name, or division.
- **Floors** are straightforward and are where maps are placed.
- **Groups** are a way to customize the configuration of specific device types.
  - For example, a branch location may have a unique configuration for Outdoor APs
  - Create a Group for the Outdoor APs, put the APs into that group and override the part of the configuration that is unique to the group.

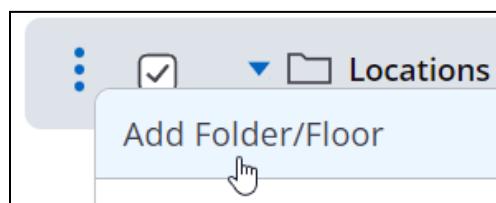
## Creating Folders:

Let's lay out a simple example Organization hierarchy to keep configurations and customizations of the wireless infrastructure.

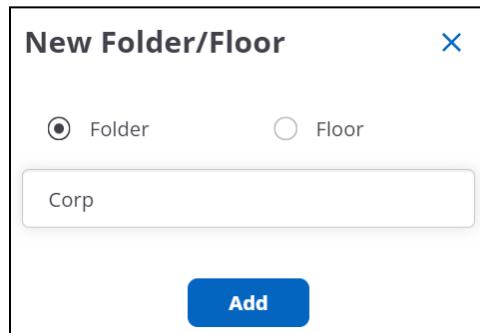
**\*Note:** A default “Staging Area” folder exists at the Locations root. This is where unconfigured access points reside prior to being assigned to specific locations/floors.



Add a folder for your Company Name. In the “Navigator”, select the 3 dots next to “Locations”:



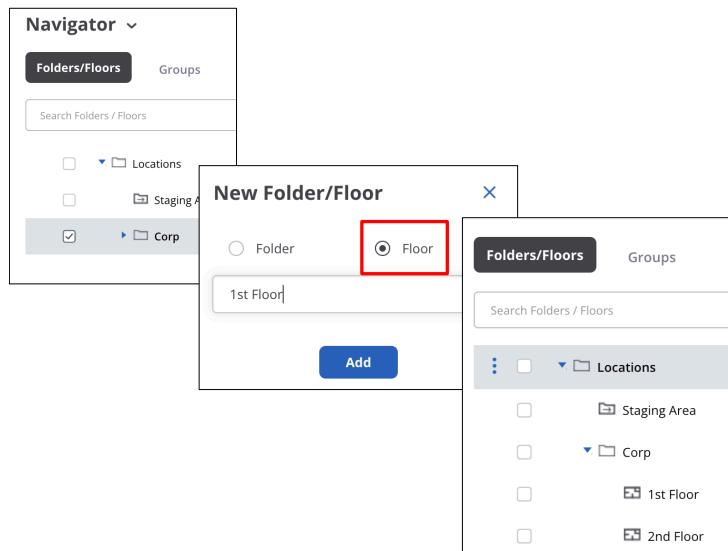
Select “**Add Folder/Floor**” and then name your new Folder “**Corp**”.



You can optionally nest folders to further define your organization and configuration containers.  
Note: the folder level is the

## Creating Floors:

Next, create 2 floors called “**1st Floor**” and “**2nd Floor**”. Right click on the word “**Corp**” to expose the menu. Be sure to click the “**Floor**” radial button (the default is “**Folder**”)



**\*Note:** It's also possible to add multiple floors at once using the “**Add Multiple Folders/Floors**” menu option:

**Locations**

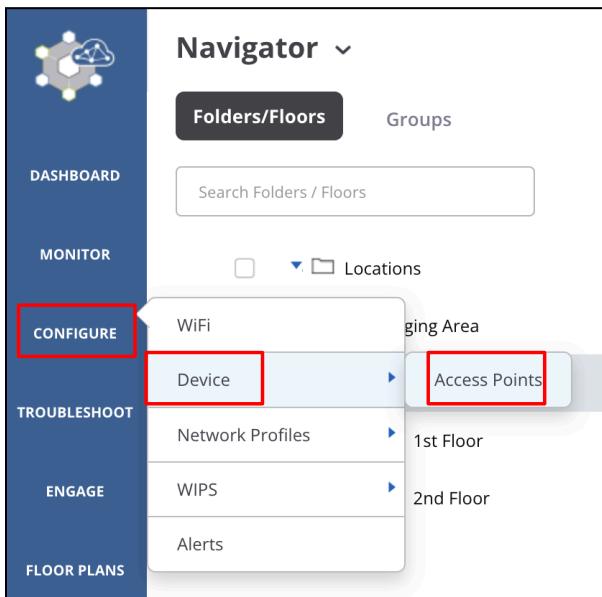
- Type folder/floor names in the text area below, one name per line, to add new entries to the selected folder.
- Use the Tab key on the keyboard to create a hierarchical tree.
- You can also copy & paste from a text editor.
- See sample

	Corp
1	1st Floor
2	2nd Floor

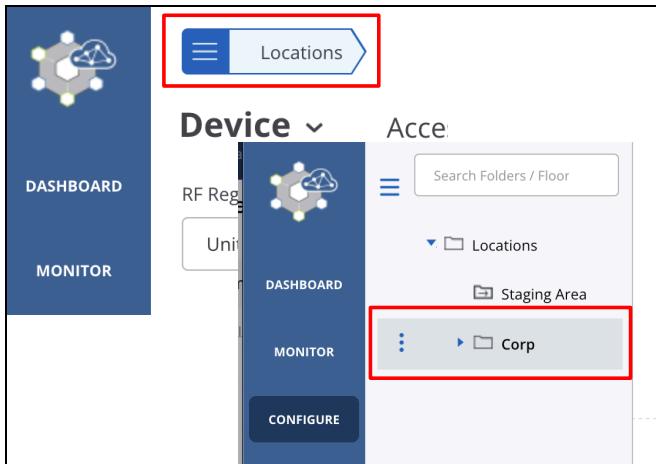
## **Important:**

**For this workshop event, we will be reducing WiFi Radio channel width and transmit power levels to avoid interference with the hosting facility.**

To customize these power settings: Navigate to the **Configure**, **Device**, **Access Points** menu to customize the Corp Folder Settings.



Once in that menu, ensure that Corp is selected from the tree structure on the left. If you do not see the tree structure, click the hamburger icon next to “Location” in the top left to expose the tree.

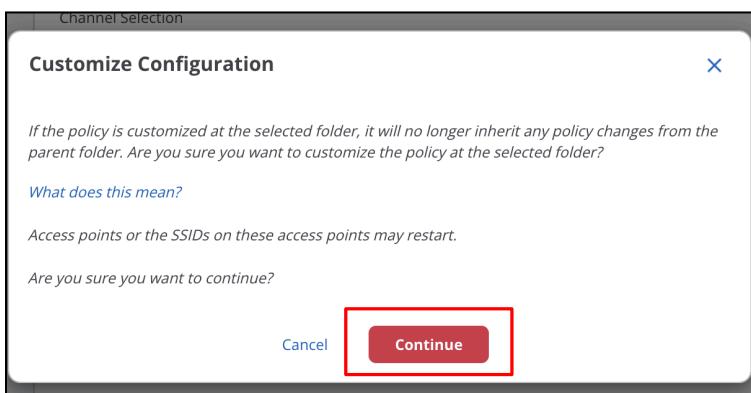


You will also need to click the message at the bottom of the screen to enable modification of the configuration that is being inherited from the top level:

**"Click here to enable editing and customize the policy"**



Then click **“Continue”** to confirm.



Set the following parameters under the **WiFi Radios** tab, **5GHz frequency**, make sure you have the “**Corp**” level selected/highlighted in the tree:

- Channel Settings: Candidate Channels: **All Channels**
- Channel Width: **20MHz**
- Transmit Power Selection: **Manual**
- EIRP: **4 dBm**

**Device** ▾ Access Points General Security WiFi Radios IOT Radios LAN Ports More

Search for MAC / IP Address/ User Name/ Device Name... 0 1 0 0 32 ⓘ

2.4 GHz 5 GHz 6 GHz ⋮

### Channel Settings

Channel Selection  Auto  Manual

Candidate Channels  All Channels  Use All Non-DFS Channels

26	40	44	48	52	56
60	64	100	104	108	112
116	120	124	128	132	136
140	144	148	152	156	160
165					

**Selection Mode \***  
 Scheduled  Periodic  
 Second ACS Time Slot  
First Time Slot (HH:MM) \*  
04 ⏺ 00 ⏻

Note: Follows the timezone of the selected location.

Dynamic Channel Selection  
 Use DFS History in Channel Selection

### Capability

Protocol 802.11ax

**Channel Width**  20MHz  20/40MHz  20/40/80MHz  20/40/80+80MHz  20/40/80/160MHz

Guard Interval 0.8 microseconds

### 802.11ax Enhancements

Downlink MU-MIMO  Downlink OFDMA  BSS Color  
 Uplink MU-MIMO  Uplink OFDMA  
 Spatial Reuse (SR)

### Transmit Power Selection

Auto  Manual  
ERP \* 4 dBm [4-30] ⏺  Specify External Antenna Gain

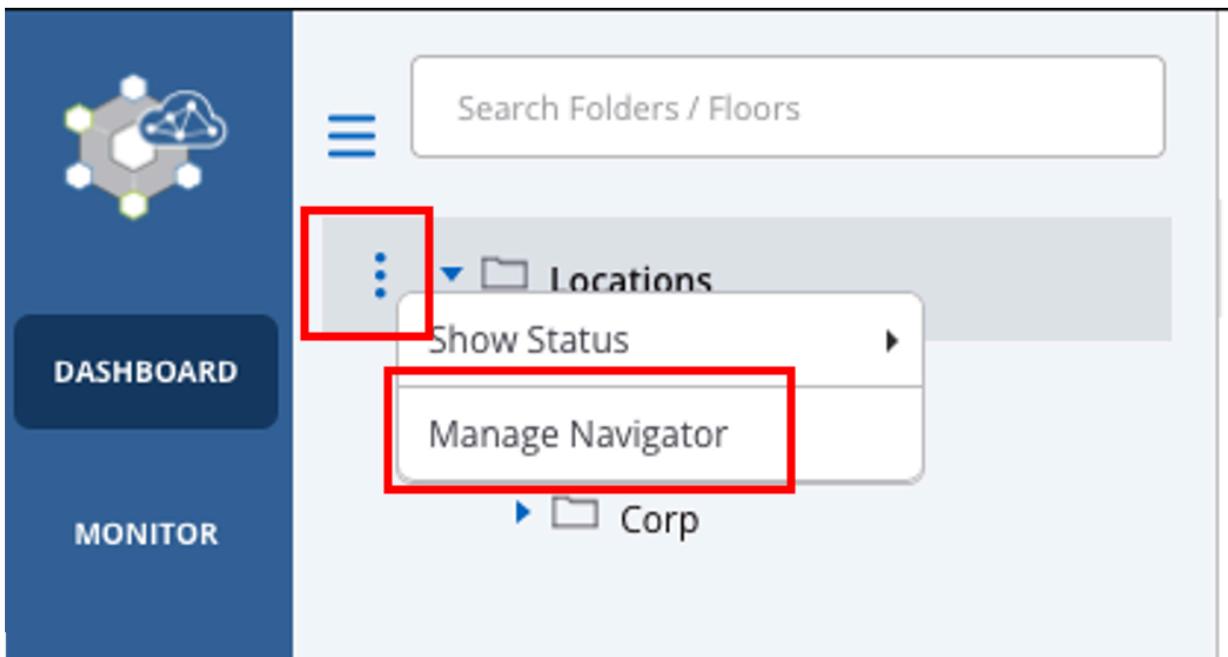
**Smart Steering**

Click “Save” at the bottom of the page then click “Continue” to confirm.

The screenshot shows a configuration page for an Access Point. It includes fields for EIRP (set to 4 dBm) and a checkbox for specifying external antenna gain. A note at the bottom states: "Configuration is customized at the selected folder. Inherit configuration from parent folder?". Below the configuration area are buttons for "Client Steering Common Parameters", "Revert to Previous Settings", and a prominent blue "Save" button, which is highlighted with a red rectangular border.

## Move AP to destination folder

Click “Locations” in the tree structure and choose “Manage Navigator”



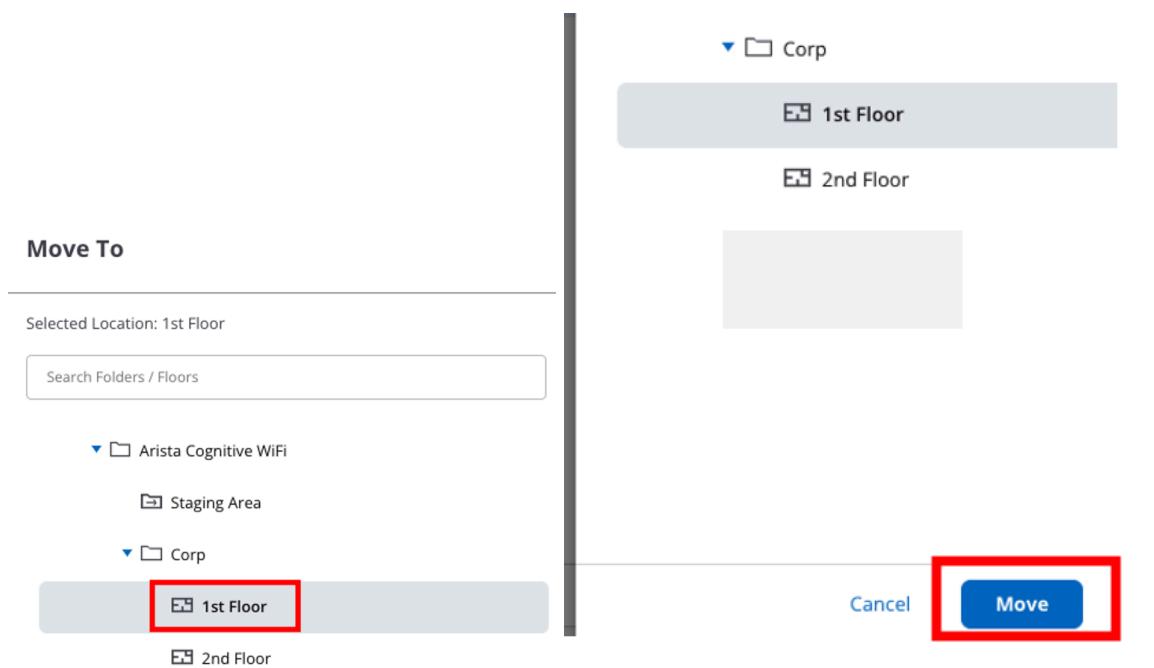
Move your AP into the “1st Floor” floor you created. To move your AP from the staging area, click on the “Staging Area” folder, and select “Show Available Devices”.

The screenshots show the Arista Cognitive WiFi interface. The left sidebar includes DASHBOARD, MONITOR, CONFIGURE (selected), TROUBLESHOOT, ENGAGE, FLOOR PLANS, REPORTS, and SYSTEM. The right pane has a 'Navigator' header and tabs for 'Folders/Floors' (selected) and 'Groups'. A search bar says 'Search Folders / Floors'. Under 'Locations', there's a tree view with a checked checkbox next to 'Staging Area'. A context menu is open over 'Staging Area' with three options: 'Add Folder/Floor', 'Add Multiple Folders/Floors', and 'Show Available Devices'. The bottom screenshot shows the 'Show Available Devices' dialog with a table titled '1 Access Points' containing one row for 'POD-01-FL1'.

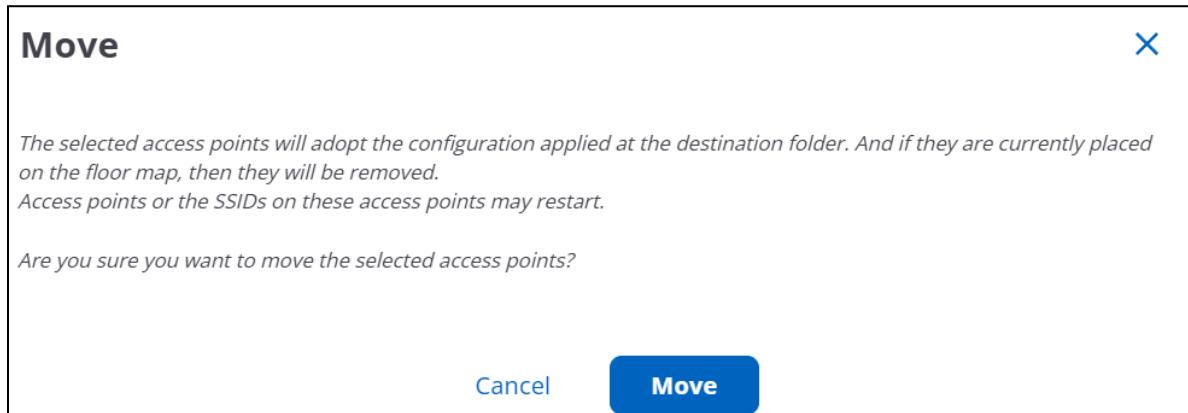
Next, click on the AP name, select “Move” and then select the “1st Floor” folder you created earlier, and then click the “Move” button at the bottom of the screen.

The screenshots show the Arista Cognitive WiFi interface. The left sidebar includes DASHBOARD, MONITOR, CONFIGURE (selected), TROUBLESHOOT, and ENGAGE. The right pane has a 'Navigator' header and tabs for 'Folders/Floors' (selected) and 'Groups'. A search bar says 'Search Folders / Floors'. Under 'Locations', there's a tree view with a checked checkbox next to 'Staging Area'. The right pane also shows a '1 Access Points' dialog for 'POD-01-FL1', which lists the MAC address '30:86:2D:0C'. Below the table are buttons for 'Assign/Reassign to a Group', 'Remove Access Points from Group', and 'Move' (which is highlighted with a red box).

In the following dialog, select your **1st Floor** and click **Move** to assign the AP.



You'll see a pop-up message to confirm the move. Click “Move” again to finish the process:



You can verify the move by selecting the “**1st Floor**” folder and then “**Show Available Devices**”.

The screenshot shows the Cisco Meraki interface for managing network devices. A context menu is open over a folder named "1st Floor". The menu options are: "Add Folder/Floor", "Add Multiple Folders/Floors", "Show Available Devices", and "Add Group". The "Add Group" option is highlighted with a cursor icon. Below the menu, the "Navigator" section is visible, showing a tree view of locations and floors. The "1st Floor" node is selected and highlighted in grey. To the right, a table titled "1 Access Points" lists a single entry: "POD-01-FL1".

Name
POD-01-FL1

Moving APs into the folders ensures the child devices inherit the configuration of the parent hierarchy structure. This means your pod's AP radios will have the channel and power settings applied as a shared configuration.

**LAB COMPLETE.**

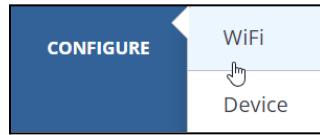
The next section begins on the following page.

## 5. Creating an SSID

In this lab, we will be working in the “**WiFi**” configuration area. This list is a summary of the steps, detailed steps follow the list.

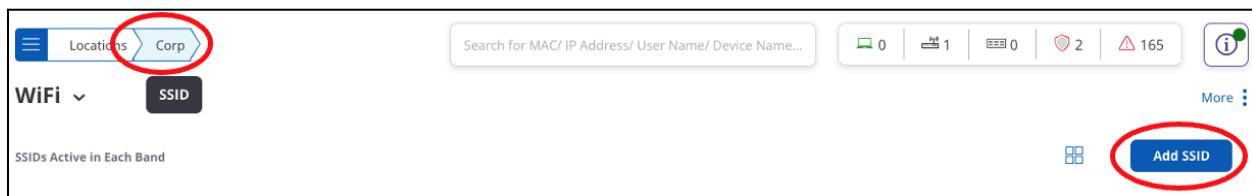
- 1) Navigate to Configure > WiFi
- 2) Click “**Add SSID**” to create a new SSID (WPA2 PSK) with your **ATD-##-PSK** as the name (where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod.)
- 3) Click the “**Security**” tab, change the dropdown from “Open” to “**WPA2**”
- 4) Use **AristaCampus** as the passkey.

Hover your cursor over the “**Configure**” menu option on the left side of the screen, then click “**WiFi**”.



At the top of the screen, you will see where you are in the location hierarchy. If you aren't on “**Corp**”, click on the three lines (hamburger icon) next to “**Locations**” to expand the hierarchy and choose/highlight the “**Corp**” folder. Now click the “**Add SSID**” button on the right hand side of the screen.

With the hierarchy menu collapsed:

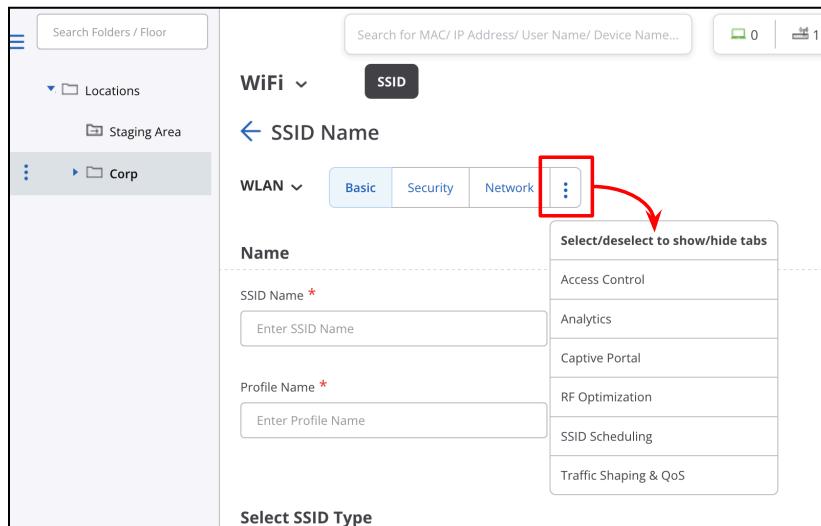


Or, with the hierarchy menu expanded:



Once on the “SSID” page, configuration sub-category menu options will appear across the top of the page related to WiFi (the defaults are “Basic”, “Security”, and “Network”). You can click on these sub-category names to change configuration items related to that area of the configuration.

While we won’t be conjuring them here - In addition to “Basic”, “Security”, and “Network” configuration options, there are additional categories available. To make them visible, click on the 3 dots next to “Network” and you can see the other categories that are available to configure (i.e. “Analytics”, “Captive Portal”, etc.).



Back within the “Basic” menu option, name the SSID “ATD-##-PSK” (where ## is a 2 digit character between 01-20 that was assigned to your lab/Pod.).

The “Profile Name” is used to describe the SSID and should auto-fill with the SSID’s name.

**Name**

SSID Name \*

ATD-01-PSK

Profile Name \*

ATD-01-PSK

Since this is our corporate SSID, leave the “**Select SSID Type**” set to “**Private**”, but note this is where you would change it to “**Guest**” if needed. Select **Next** at the bottom.

**Next**

In the “**Security**” sub-category, change the association type to “**WPA2**”, select the “**PSK**” radio button, enter the passkey of “**AristaCampus**”, then select “**Next**” at the bottom of the screen.

WLAN ▾ Basic Security Network :

Select Security Level for Associations  
In the 6 GHz band, WiFi 6E does not support security methods older than WPA3 (WPA2, Opt

WPA2 PSK UPSK 802.1X

Enter a Passphrase \*

AristaCampus

>Password Policy

Moderate

**Next**

In the “**Network**” configuration sub-category, we’ll leave the “**VLAN ID**” set to “**0**”, which means it will use the native VLAN. If the switchport the AP is attached to is trunked, you could change this setting to whichever VLAN you want the traffic tagged with.

#### Network Mode:

Select “**Bridged**” mode for this lab.

For reference

- NAT - often used for Guest traffic to default gateway
- L2 / L3 Tunnel - Guest Anchor, tunneled corporate traffic, and traffic inspection

The rest of the settings can be left at the default values.

Click the “Save & Turn SSID On” button at the bottom of the page.

WLAN ▼ Basic Security Network :

VLAN \*

VLAN ID  VLAN Name

0 [0 - 4094]

Network Mode

Bridged  NAT  L2 Tunnel  L3 Tunnel

**Save & Turn SSID On**

## Please Read!

Only select the “5 GHz” option on the next screen (uncheck the 2.4 GHz box if it’s checked), then click “Turn SSID On”.

Turn SSID On - ATD-01-PSK

Select the frequency bands for this SSID

2.4 GHz  5 GHz  6 GHz

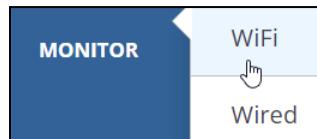
**Turn SSID On**

It will take a minute or two for the SSID to enable. You can check if the SSID has been enabled and add or disable SSIDs from the “Configure”, “WiFi” menu

The screenshot shows the WiFi configuration interface. On the left, a sidebar menu includes DASHBOARD, MONITOR, **CONFIGURE**, TROUBLESHOOT, ENGAGE, FLOOR PLANS, REPORTS, and SYSTEM. The CONFIGURE tab is selected. In the main area, a search bar at the top right says "Search Folders / Floors". Below it, a tree view under "Locations" shows "Staging Area" and "Corp". Under "Corp", there are "1st Floor" and "2nd Floor". A highlighted box labeled "WiFi" is shown in the tree view. To the right, a "WiFi" dropdown menu is open, showing "SSID" and "SSIDs Active in Each Band" (2.4 GHz, 5 GHz, 6 GHz). Below this, a detailed view of the WiFi profile "ATD-01-PSK" is displayed, including its profile name, type (Private), security (WPA2 (PSK)), location, frequency band (5 GHz), and radio counts.

Profile Name	Type	Security	Location	Frequency Band	No. of 2.4 GHz Radios	No. of 5 GHz Radios	No. of 6 GHz Radios	Access Points
ATD-01-PSK	Private	WPA2 (PSK)	//Locations/Corp	5 GHz	0	0	0	0

After you turn on the SSID, hover your cursor over “**Monitor**” in the left hand side menu, and then click “**WiFi**”.



Now, in the menu options at the top of the page, look at the “**Radios**” menu option. The **5 GHz radio should be “thumbs up”** and **2.4 and 6 GHz radios should be “thumbs down”**? It may take a minute or two for the radio to become active.

The screenshot shows the WiFi management interface with the Radios tab selected. The table lists two access points, both named 'POD-01-FL1'. The 'Frequency' column indicates 5 GHz and 2.4 GHz respectively.

Status	Access Point Name	AP MAC Address	IP Address	Channel	Tx. Power (dBm)	Frequency
<span>Green</span>	POD-01-FL1	30:86:2D:30:4...	10.0.101.109	44	0	5 GHz
<span>Red</span>	POD-01-FL1	30:86:2D:30:4...	10.0.101.109	--	0	2.4 GHz

Check the “Active SSIDs” menu at the top of the screen. Is your SSID listed?

The screenshot shows the WiFi management interface with the Active SSIDs tab selected. It displays one active SSID, 'ATD-01-UPSK', which uses WPA2 security and PSK authentication. There is one 5 GHz radio associated with this SSID.

SSID	Security	Authentication	5 GHz Radios	2.4
ATD-01-UPSK	WPA2	PSK	1	

Next, go ahead and connect your phone to the SSID (PSK is “AristaCampus”). Navigate to the “Clients” menu at the top of the screen and you should see your device.

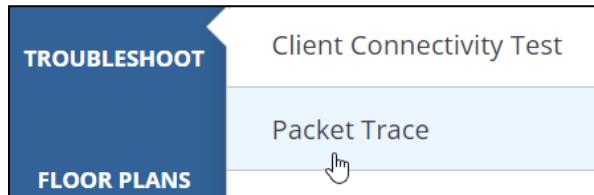
The screenshot shows the WiFi management interface with the Clients tab selected. It displays one client device, with details including User Name, MAC Address, Locally Ad..., IPv4 Address, and IPv6 Addresses.

Status	Name	User Name	MAC Address	Locally Ad...	IPv4 Address	IPv6 Addresses
<span>Green</span>	4A:91:0E:7E:FB:C4	--	4A:91:0E:7E:FB:C4	Yes	192.168.1.20	fe80::81f:cbd6:e9ac:8

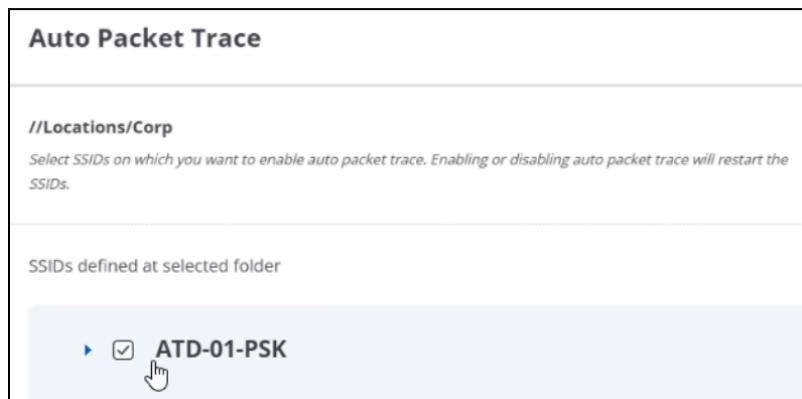
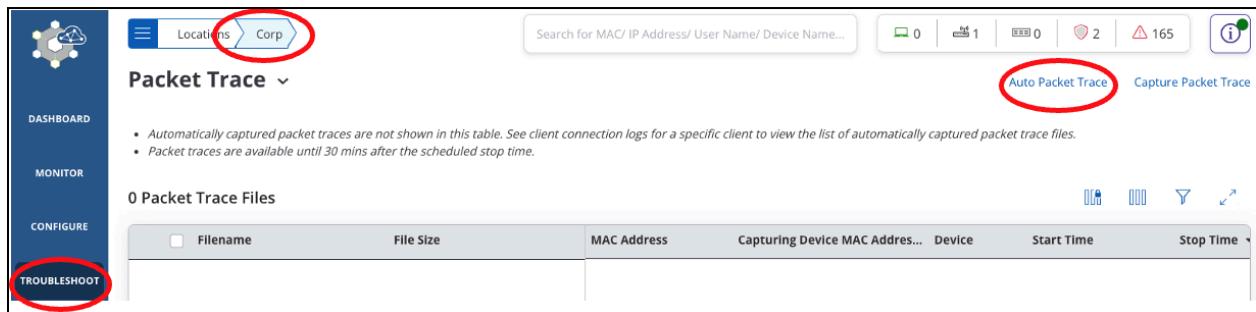
The next section begins on the following page.

## 6. Troubleshooting

Make sure you are at the “**Corp**” folder in the hierarchy, and then hover over “**Troubleshoot**” in the left hand menu, then click “**Packet Trace**”.



On the top right hand side of the window, click “**Auto Packet Trace**” and select the checkbox for the **SSID** you created earlier (**ATD-##-PSK**). Click “**Save**” at the bottom of the window. If you don't see the SSID listed, make sure you are in the correct folder in the navigation pane.

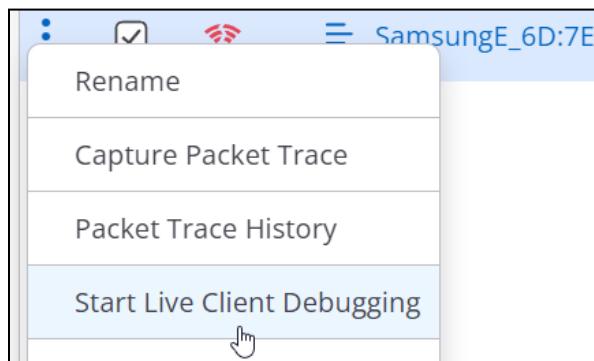


**Save**

Next, connect your device to the AP and type in the wrong PSK. Hover your cursor over the “Monitor” menu on the left hand side of the screen, then click “WiFi”. Now click on “Clients” at the top of the page. You should see your device trying to connect.

The screenshot shows the Arista Cognitive WiFi interface. On the left sidebar, the "MONITOR" option is selected. The main header shows "Arista Cognitive WiFi... Corp". Below the header, there are tabs for WiFi, Clients (which is selected), Access Points, Radios, Active SSIDs, and Application Visi. Under the WiFi tab, it says "1 Clients" and there is a "Client Explorer" button. A table lists one client: "Failed to connect" (MAC address 4A:91:0E:7E:FB:C4) with the error message "Incorrect PSK" and the timestamp "Jul 21, 2024 12:53:57 PM".

Select on the three dots next to the device name and select “Start Live Client Debugging”.



Select “30 Minutes” in the “Time Duration” drop down box, select the “Discard Logs” radio button, then click “Start”.

The "Live Client Debugging" dialog box. It contains a "Select Time Duration" dropdown set to "30 Minutes". Below it is a "Location" field with the value "/Locations" and a "Change Location" link. At the bottom, there is a "Select Action After Stop/Timeout" section with two radio buttons: "Discard Logs" (selected) and "Archive Logs".

**Start**

Next, try connecting the device again with the **wrong PSK**. Watch and review the Live Client Debugging Log.

Download log file to view historical log entries from start time till now.			
1	Client MAC: 96:88:		
2	SSID : LAB-01-WPA2		
3	BSSID : 30:86:2D:8F:C2:81		
4	AP NAME : C-360-AP1		
5	Chan : 136		
6	Time : 2023.12.28 17:09:27 (EST)		
7	Tdiff(msec)	Timestamp	Event
8	0	2023.12.28 17:09:27	AP received authentication request from client at [-63]db
9	54	2023.12.28 17:09:27	AP received (re)association request from client
10	54	2023.12.28 17:09:27	Client successfully (re)associated
11	55	2023.12.28 17:09:27	Signals a new WPA or WPA2 exchange
12	55	2023.12.28 17:09:27	Setting PMK from PSK as this is a WPA or WPA2 PSK authentication
13	55	2023.12.28 17:09:27	First phase of WPA/WPA2 4-Way Handshake Completed
14	87	2023.12.28 17:09:27	Invalid MIC received from client in msg 2/4 of 4-Way Handshake
15	174	2023.12.28 17:09:27	First phase of WPA/WPA2 4-Way Handshake Completed
16	174	2023.12.28 17:09:27	Invalid MIC received from client in msg 2/4 of 4-Way Handshake
17	1152	2023.12.28 17:09:28	First phase of WPA/WPA2 4-Way Handshake Completed
18	1256	2023.12.28 17:09:28	Invalid MIC received from client in msg 2/4 of 4-Way Handshake
19	2160	2023.12.28 17:09:29	First phase of WPA/WPA2 4-Way Handshake Completed
20	2262	2023.12.28 17:09:29	Invalid MIC received from client in msg 2/4 of 4-Way Handshake
21	3170	2023.12.28 17:09:30	Maximum retries of 1/4 msg reached
22	3274	2023.12.28 17:09:30	Node Left

After that fails, try again with the **correct PSK ("AristaCampus")**. Review the logs.

Stop the Live Client Debugging:



You can verify live client debugging is enabled for a specific client by hovering over its entry in the Monitor, WiFi section

The screenshot shows the Arista Cognitive WiFi interface. On the left is a sidebar with icons for Dashboard, Monitor (selected), Configure, and Troubleshoot. The main area has a header with a menu icon, the text "Arista Cognitive WiFi... Corp", and tabs for WiFi (selected), Clients (highlighted in dark blue), Access Points, and Radios. Below this, a sub-header says "1 Clients" with a refresh icon and a "Client Explorer" button. A table lists one client: "4A:91:0E:7E:FB:C4". A tooltip "Live Client Debugging in progress." appears over this row. The table columns are Status, Name, and User Name.

Once your device has successfully connected to the AP, click on the View Properties button under the Name Column to learn more about the specific client

This screenshot is similar to the previous one but includes a tooltip. The tooltip, which appears over the "View properties" button in the client table, contains the text "Successfully connected". The rest of the interface is identical to the first screenshot.

## **4A:91:0E:7E:FB:C4 (4A:91:0E:7E:FB:C4)**

---

### ▼ Basic

Name: 4A:91:0E:7E:FB:C4  
User Name: --  
MAC Address: 4A:91:0E:7E:FB:C4  
IPv4 Address: 192.168.1.206  
IPv6 Addresses: fe80::81f:cbd6:e9ac:84d0  
VLAN: 0  
Status: Successfully connected  
Location: //Arista Cognitive WiFi/Corp  
Classification: Authorized  
OS: Apple iOS / iPadOS  
Vendor: Unknown  
Tag: --  
First Detected: Jul 21, 2024 12:45:56 PM  
Connected/Disconnected Since: ↑ Jul 21, 2024 12:53:38 PM  
Band Capability: 2.4 GHz, 5 GHz

The screenshot shows the Arista Cognitive WiFi dashboard interface. On the left, there's a sidebar with 'DASHBOARD', 'MONITOR' (which is currently selected), and 'CONFIGURE' buttons. The main area has a header with 'Arista Cognitive WiFi...' and 'Corp'. Below the header, there are tabs for 'WiFi', 'Clients' (which is selected and highlighted in dark grey), and 'Access Points'. A large button labeled 'Client Explorer' is present. The 'Clients' section displays a table with columns 'Status' and 'Name'. One row is visible, showing a blue square icon for status, a green Wi-Fi icon, and the MAC address '4A:91:0E:7E:FB:C4'. The MAC address is highlighted with a red rectangle.

After you click on the client name you can gather additional information such as Root Cause Analysis, Client Events, Data Rate, Top Apps by Traffic, Client Traffic Volume, Application Experience, etc.

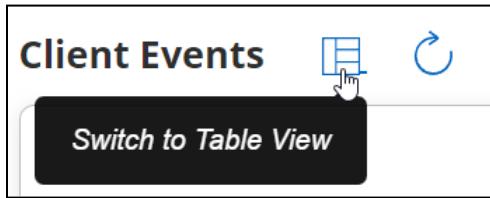
The screenshot shows the 'Network Usage' page for the client with MAC address 4A:91:0E:7E:FB:C4. At the top, there's a search bar and a message to 'Upgrade to our latest client details page now!'. Below the search bar, a timeline shows the client's network activity from July 21, 2024, 1:08 PM. The timeline includes markers for 'Authentication', 'Association', 'Client Steering', and 'Prevention'. A tooltip on the timeline provides detailed information about the client's last 15 minutes of data, including its location (//Arista Cognitive WiFi/Corp) and frequency band (5 GHz). The bottom of the page has a footer stating 'This insight was generated on Jul 21, 2024 1:06:43 PM based on the last 15 minutes of client's data.'



The client is not facing any issue at the moment.

*This insight was generated on Jul 21, 2024 1:06:43 PM based on the last 15 minutes of client's data.*

Scroll down a little to the “Client Events” section select the icon to “Switch to Table View”.



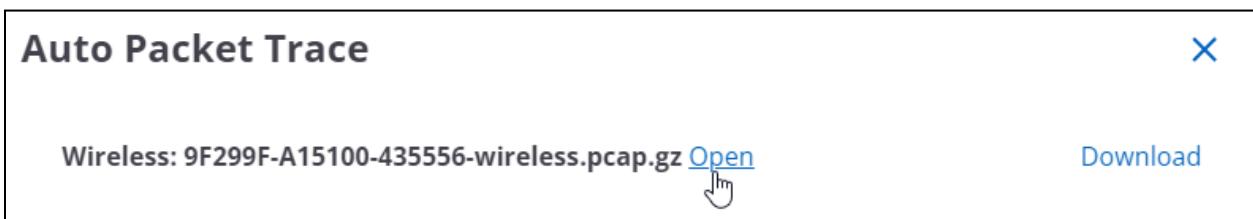
Here you can see the success/failure messages, DHCP information, and other events. Scroll down to the failed incorrect PSK entry and select “View Packet Trace” in the “Packet Capture” column (you may have to scroll to the right).

Timestamp	Event	BSSID	AP Name	Location	SSID	Frequency Band ...	Chann...	Packet Capture
Jul 21, 2024 01:13:46.906 PM	Client is assigned the IP address 192.168.1.206.	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	
Jul 21, 2024 01:13:46.906 PM	Client is assigned the IP address fe80::81fc:bd6c%1	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	
Jul 21, 2024 01:13:46.669 PM	The client was assigned VLAN 0	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	
Jul 21, 2024 01:13:46.622 PM	Client successfully (re)associated.	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	
Jul 21, 2024 01:13:46.572 PM	Authentication Failure	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	<a href="#">View Packet Trace</a>
Jul 21, 2024 01:13:46.535 PM	AP received authentication request from client	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	
Jul 21, 2024 01:13:34.825 PM	The access point reached the maximum retry limit	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	
Jul 21, 2024 01:13:34.789 PM	The access point reached the maximum retry limit	30:86:2D:0D:0F:81	POD-01-FL1	//Arista Cognitive WiFi...	ATD-01-PSK	5 GHz	157	

You should see a packet trace that you can download. Click on “View Packet Trace”.

Select “Open” to open the file right within CV-CUE / Packets. You will be in the “Visualize” section of Packets.

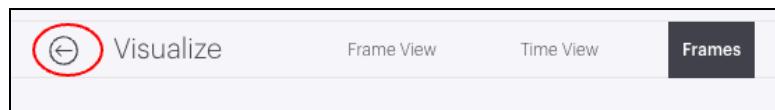
You can also download the trace and view it with Wireshark if you have it installed.



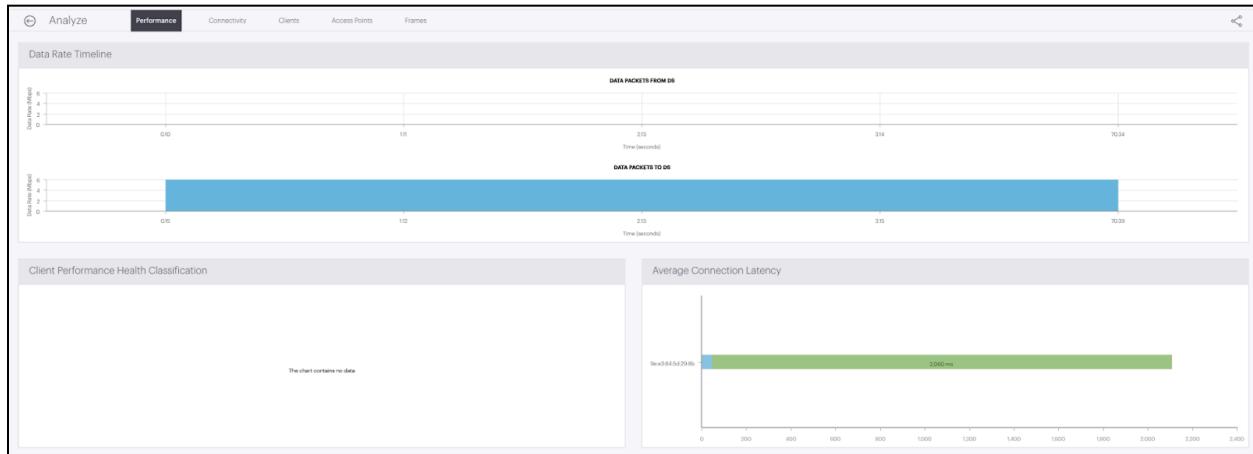


Click on “**Time View**” and “**Frames**” to look through the data and at the trace to see how Arista can help you troubleshoot.

Next, click on the back arrow icon to look at the “**Analyze**” feature.



Explore the “**Analyze**” feature by clicking on the various menu options and reviewing the data.

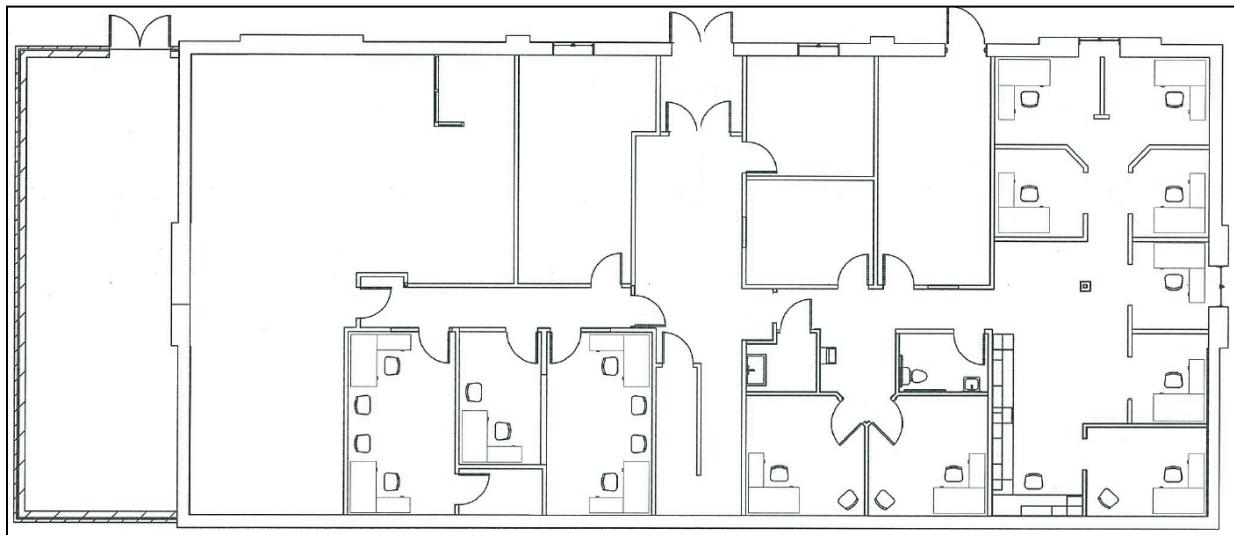


The next section begins on the following page.

## 7. Floor Plans

Utilize the floor plan image file provided in the Workshop Files download location and shown on the title page of this guide. Save that image to your computer.

Floor plan image example:



In the left hand menu, click on “**Floor Plans**”. Make sure to set the location level to be “**1st Floor**”. Click the “**Add Floor Plan**” button in the upper right corner of the screen.

The screenshot shows the software interface for managing floor plans. On the left, a vertical sidebar lists navigation options: DASHBOARD, MONITOR, CONFIGURE, TROUBLESHOOT, ENGAGE, FLOOR PLANS (which is highlighted with a red box), and REPORTS. The main area has a search bar at the top. Below it, a tree view shows Locations > Staging Area > Corp > 1st Floor (also highlighted with a red box) > 2nd Floor. To the right, there's a section titled "Upload Floor Plan" with an "Upload Image" button (highlighted with a red box) and a note about supported formats (.jpg, .png, .gif, .bmp, .svg). Below this is a "Floor Plan Dimensions" section with "Unit" set to "Feet", and fields for "Length (Horizontal)\*" and "Width (Vertical)\*". At the top right, there's another search bar for MAC/ IP Address/ User Name.

Utilize the file provided by the lab guide link for the floor plan image.

Enter floor name as “**1st Floor**”, click the “**Upload Image**” button to import the floor plan image, and use the following dimensions: Floor Plan Dimensions: Unit: **Feet**, Length: **120**, Width: **50**

Click “**Save**” at the bottom of the screen.

Add Floor Plan

Floor Name \*

Upload Floor Plan

Supported Formats: jpg, png, gif, bmp  
\_Demo 1st Floor.png

Supported Format: .spm file created in the WiFi Planner tool

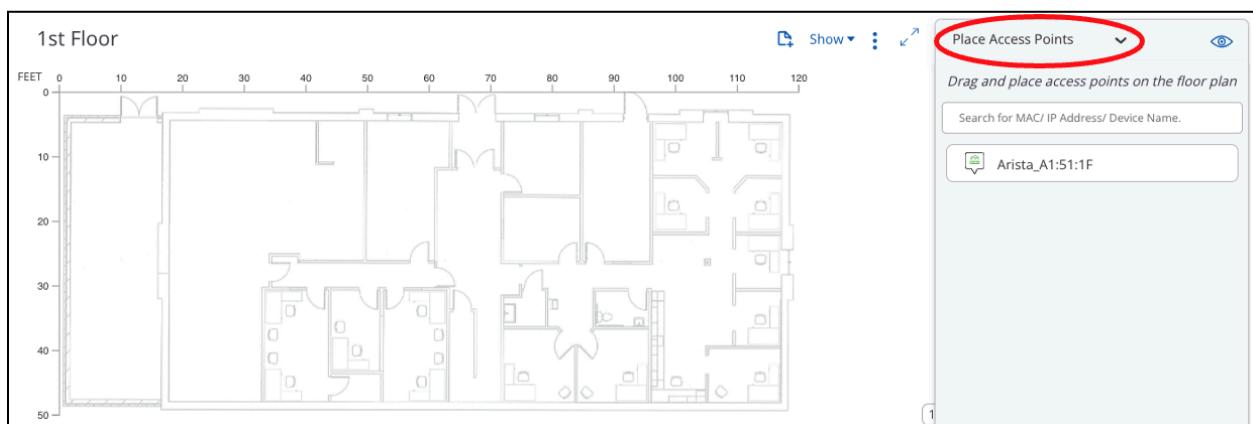
Floor Plan Dimensions

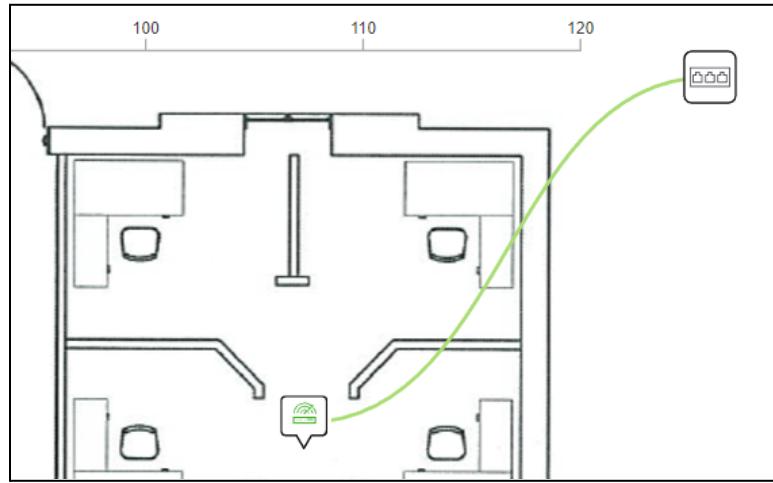
Unit  Length (Horizontal)  Width (Vertical)

**Save**

Next, drag the AP onto the map, from the right hand side menu, to see how easy placing APs is.

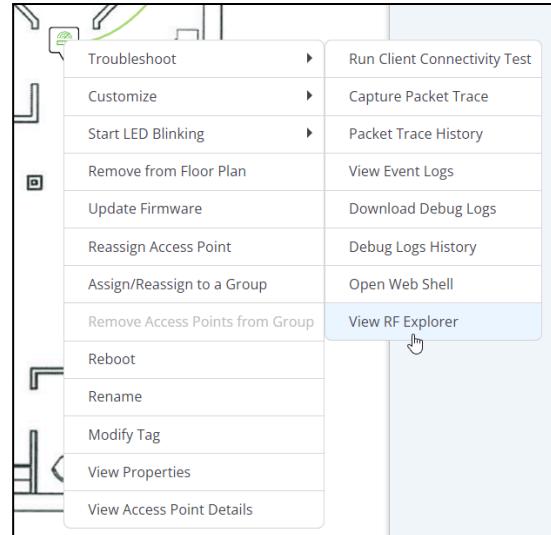
If you do not see an AP, it is because your AP is assigned to another location (folder) and you'll need to move it to the “**1st Floor**” folder (see page 8). Or, you may have the incorrect menu selected in the upper right hand corner of the screen - choose “**Place Access Points**”.



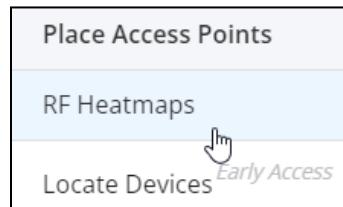


Hover over the AP image to get more information and then right-click on the AP image to see more options.

<b>Status</b>	<b>Active</b>
<b>Name</b>	<b>Arista_A1:51:1F</b>
<b>Model</b>	<b>C-110</b>
<b>Update</b>	<b>Device Firmware Up to Date</b>
<b>MAC Address</b>	
<b>IP Address</b>	<b>10.11.0.103</b>
<b>Alternative IPs</b>	<b>--</b>
<b>Build</b>	<b>13.0.2-28.37</b>
<b>Connected Since</b>	<b>7:04 AM</b>
<b>Last Booted At</b>	<b>7:01 AM</b>
<b>Group</b>	<b>--</b>
<b>Link Speed</b>	<b>1 Gbps</b>
<b>Power Source</b>	<b>PoE+</b>
<b>Connected Port</b>	<b>Ethernet31</b>



Next, explore the other menu options like **RF Heatmaps** (in the menu on the upper right hand side of the screen).

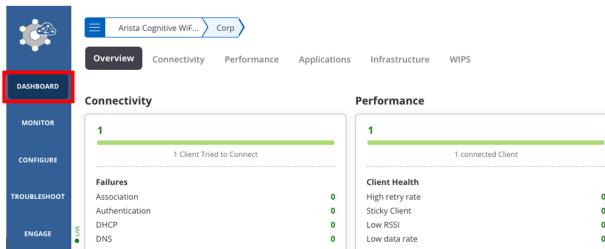




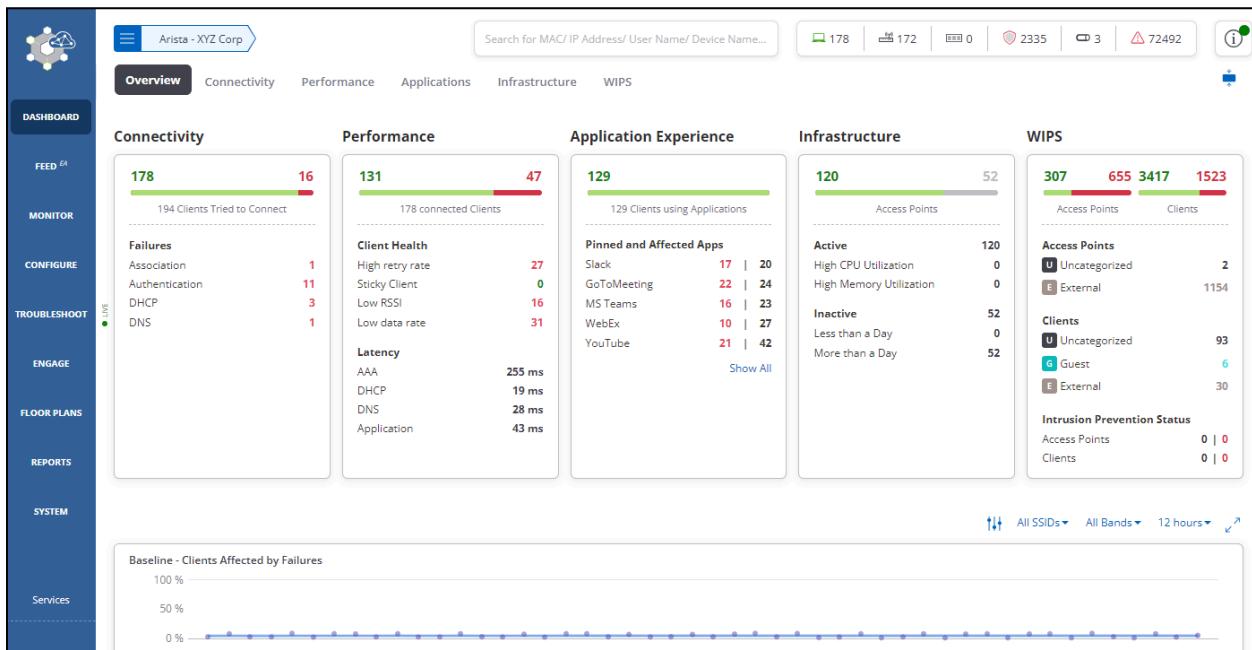
## 8. Dashboard - Client Journey

Now that a client device is connected to the WiFi network we can use the dashboard functions to gain insight to the client's journey:

Within, click on the “**Dashboard**” menu option on the left hand side of the screen. This opens the Dashboard Overview screen which provides us with numerous metrics for our wireless environment.



An example of a busy environment is shown below providing a spot check of healthy areas versus problems and alerts at a glance.

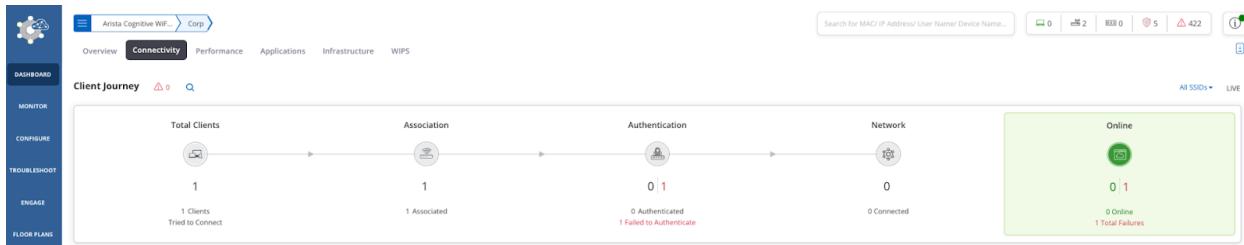


A common request for WiFi administrators is to assist when clients are unable to connect to the network. Let's use the Dashboard and Connectivity troubleshooting workflows.

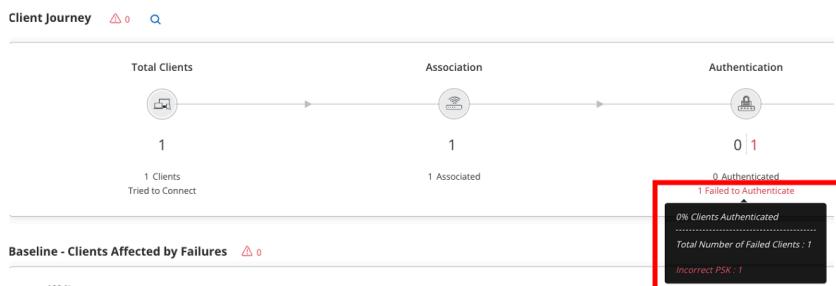
Select the “**Connectivity**” tab at the top to view the “**Client Journey**”.

Your lab environment will report a live view of any successful or failed client associations.

The example below shows a common mis-configuration of the PSK on the client device (from earlier section)



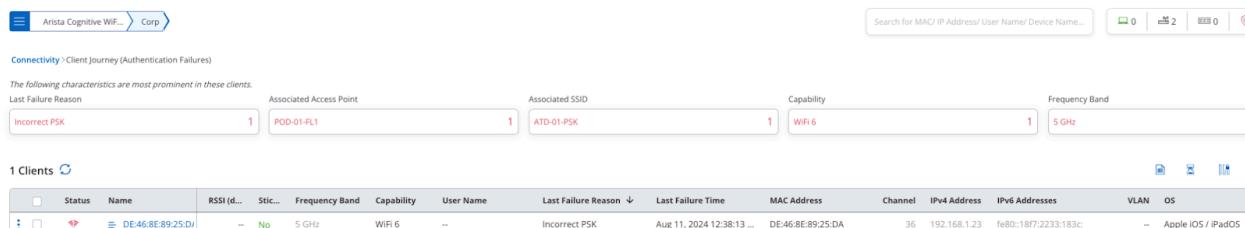
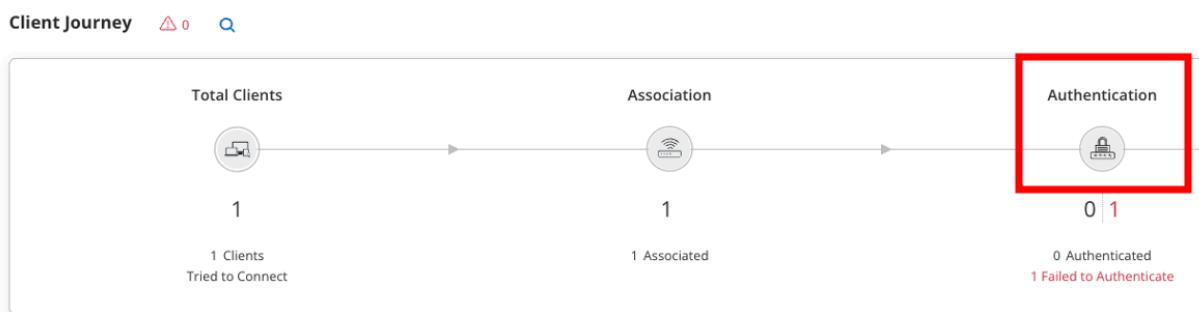
If you hover over the red warning message additional details will appear



Here the administrator is directed exactly to the problem.

Try correcting the PSK to the correct value and viewing the updated dashboard client journey.

Select the Authentication icon to present a list of clients failing at this stage of the journey:



Client MAC, frequency, failure reason, last failure, and device operating system are all presented to the administrator for troubleshooting.

Select the client device MAC for a timeline view of the client journey, and Root Cause Analysis recommendation.



[Connectivity > Client Journey \(Authentication Failures\)](#) > DE:46:8E:89:25

The following characteristics are most prominent in these clients.

Last Failure Reason

Incorrect PSK	1	P
---------------	---	---

As:

1 Clients

	Status	Name	RSSI (d...)	Stic...
		<a href="#">DE:46:8E:89:25:DA</a>	--	No

Search for MAC/ IP Address/ User Name/ Device Name... DE:46:8E:89:25:DA

Connectivity > Client Journey (Authentication Failures) > (DE:46:8E:89:25:DA)

Upgrade to our latest client details page now!

The client is facing connectivity issues because of the following reasons:  
Incorrect PSK - Wrong passphrase.

This insight was generated on Aug 11, 2024 12:47:49 PM based on the last 15 minutes

Client Events Roaming Explorer



Note that the root cause engine points the user to misconfigured key.

After the client configuration is updated to the correct key, the client Events view will update and show additional metrics and network quality analysis. For example, latency to the DHCP and DNS services is recorded and alerted on if it diverges from baseline.

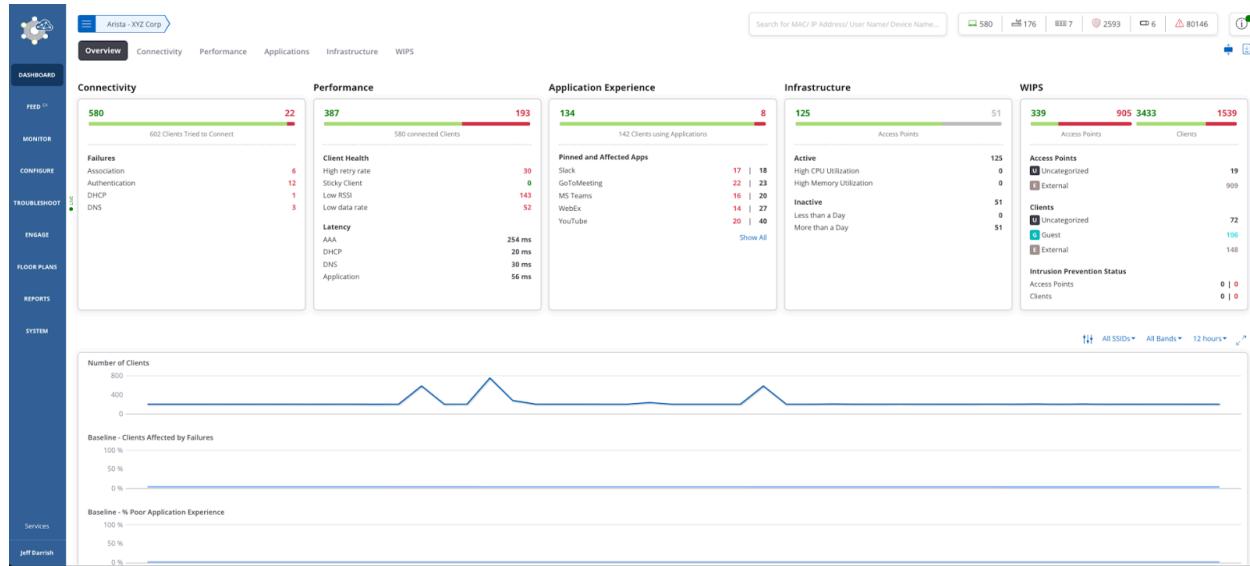
Hover over a recent successful client association to view metrics on demand

The screenshot shows the Arista Cognitive WiFi Client Journey Online interface. At the top, there's a navigation bar with 'Arista Cognitive WiFi Corp' and a search bar. Below it, a network diagram shows a client (DE-46:8E:89:25.DA) connected to an access point (POD-01-FL1), which is connected to a switch (arista720.0). A red box highlights a callout for 'Average Latencies IPv4' and 'DHCP: 5ms'. Another red box highlights a callout for 'Average Latencies IPv6' and 'DHCP: -'. Below the network diagram, a message states: 'The client is facing connectivity issues because of the following reasons: High DHCP Latency - The client faced high DHCP Latency issue in the last 15 minutes.' A timestamp indicates the insight was generated on Aug 11, 2024, at 12:49:37 PM.

**Client Events**

The 'Client Events' section displays a timeline from 12:30 to 12:48. It includes sections for Network, Authentication, Association, Client Steering, and Prevention. A red box highlights a specific event entry in the timeline.

A busy example is shown below highlighting the types of connectivity failures challenging environments may show.

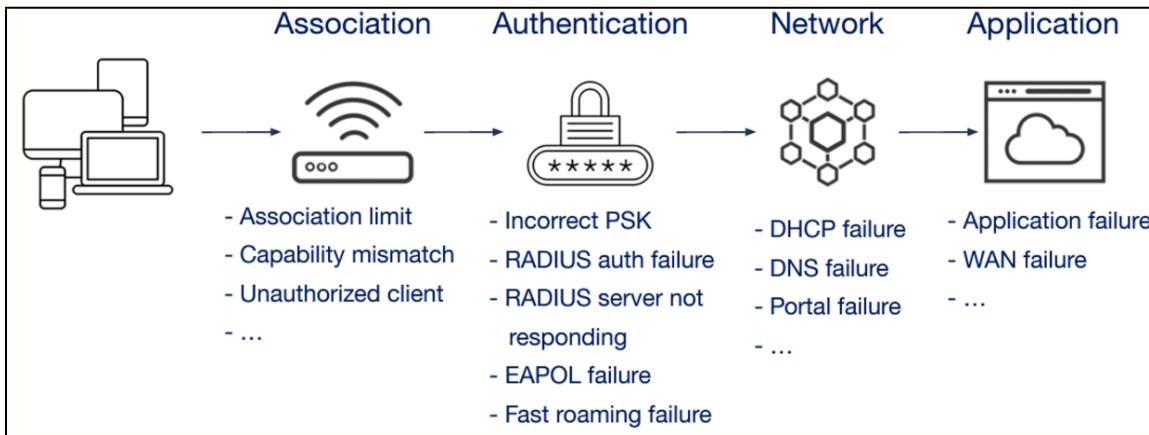


Here you can see the two basic types of issues, issues associating with the WiFi network, and networked application performance issues once they are connected.

The “**Client Journey**” shows a live view of the users that are currently on, or trying to connect to, the wireless LAN. Browse the dashboard and look around at the baselines, and other data

that is displayed.\***Note:** you can choose different baseline time frames - from 12 hours up to 1 month.

Here is a sample of what our “Root Cause Analysis” engine detection categories are which will ultimately populate the data in the “Client Journey” section:



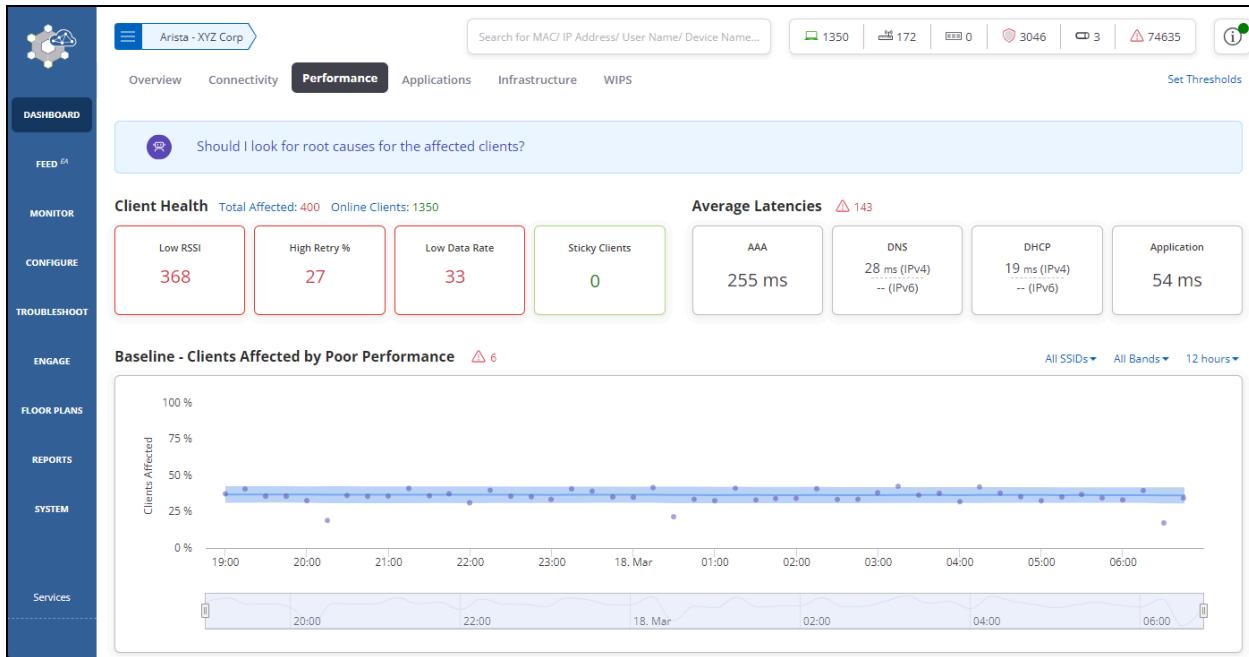
Here is some more information on the root cause analysis engine:

- RCA App Note

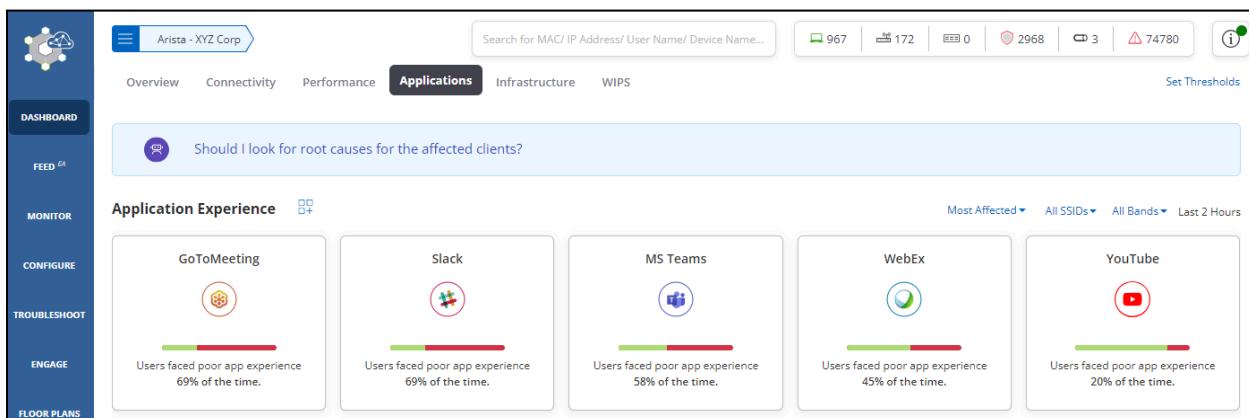
<https://www.arista.com/assets/data/pdf/Whitepapers/Arista-RCA-App-Note.pdf>

Next, click the back button in your browser to return to the main Dashboard page, then click on “Performance” in the menu at the top of the screen

The performance dashboard shows you clients that may be having a sub optimal WiFi experience, and the average latencies for network activities like RADIUS, DHCP, and DNS.



Next, click on “**Applications**” in the menu at the top of the screen.



Arista CloudVision CUE leverages CloudVision’s data lake architecture with streaming telemetry, elastic cloud services, and intelligent Access Points, to offer next generation AI enabled troubleshooting workflows, such as:

- Network Baselineing - Baselines network behavior and automatically detects and highlights anomalies, using ML algorithms.
- Root Cause Analysis Engine - Automatically detects and classifies Wi-Fi clients’ connection failures and pinpoints the root cause in real-time.
- Single Client Inferencing - Identifies clients facing poor QoE, based on RF, network and application KPIs and performs root cause analysis as well as

- providing remediation recommendations for specific clients.
- Automatic Packet Capture - Proactively captures packet traces to help diagnose problems; traces are stored alongside related failures or symptoms to simplify troubleshooting later.
- Client Emulation and Network Profiling - Takes advantage of the multi-function radio, present in most Arista Wi-Fi APs, turning it into a client to run a wide variety of tests and proactively identify problems before users do.

For more information on the “**Application Experience**” that we use to determine the experience users have with these common real-time business applications:

- Talk on QoE for conferencing apps  
[Classifying Voice and Video Experience in Wi-Fi | WLPC Phoenix 2018](#)
- Talk on QoE for web (TCP) apps  
[Web QoE: App Performance in WiFi Networks | WiFi-KS](#)
- QoE Whitepaper  
[Arista whitepaper on App QoE](#)

## LAB GUIDE COMPLETE