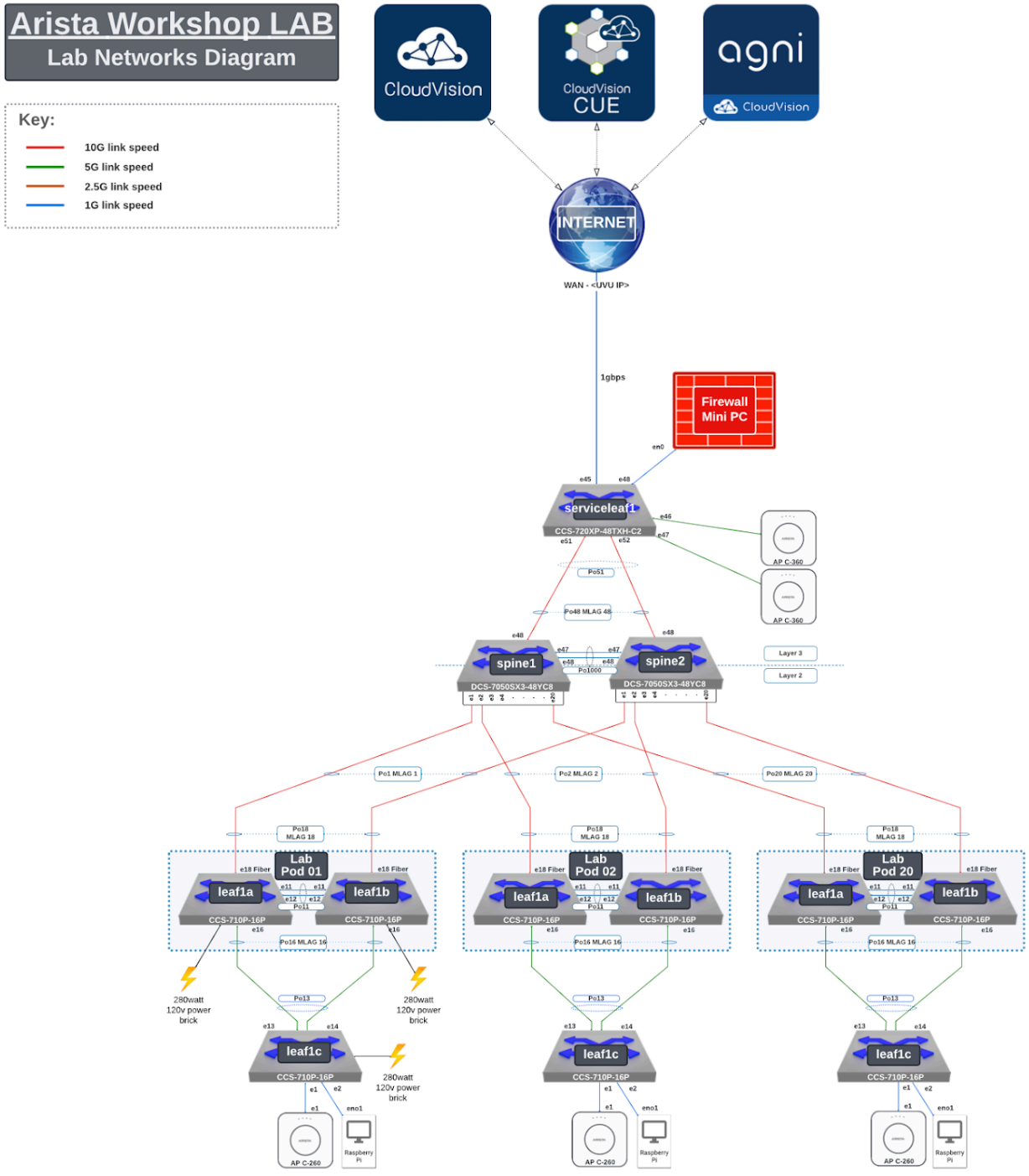
Campus C-01 AGNI Lab Guide
EAP-TLS Wireless Policy

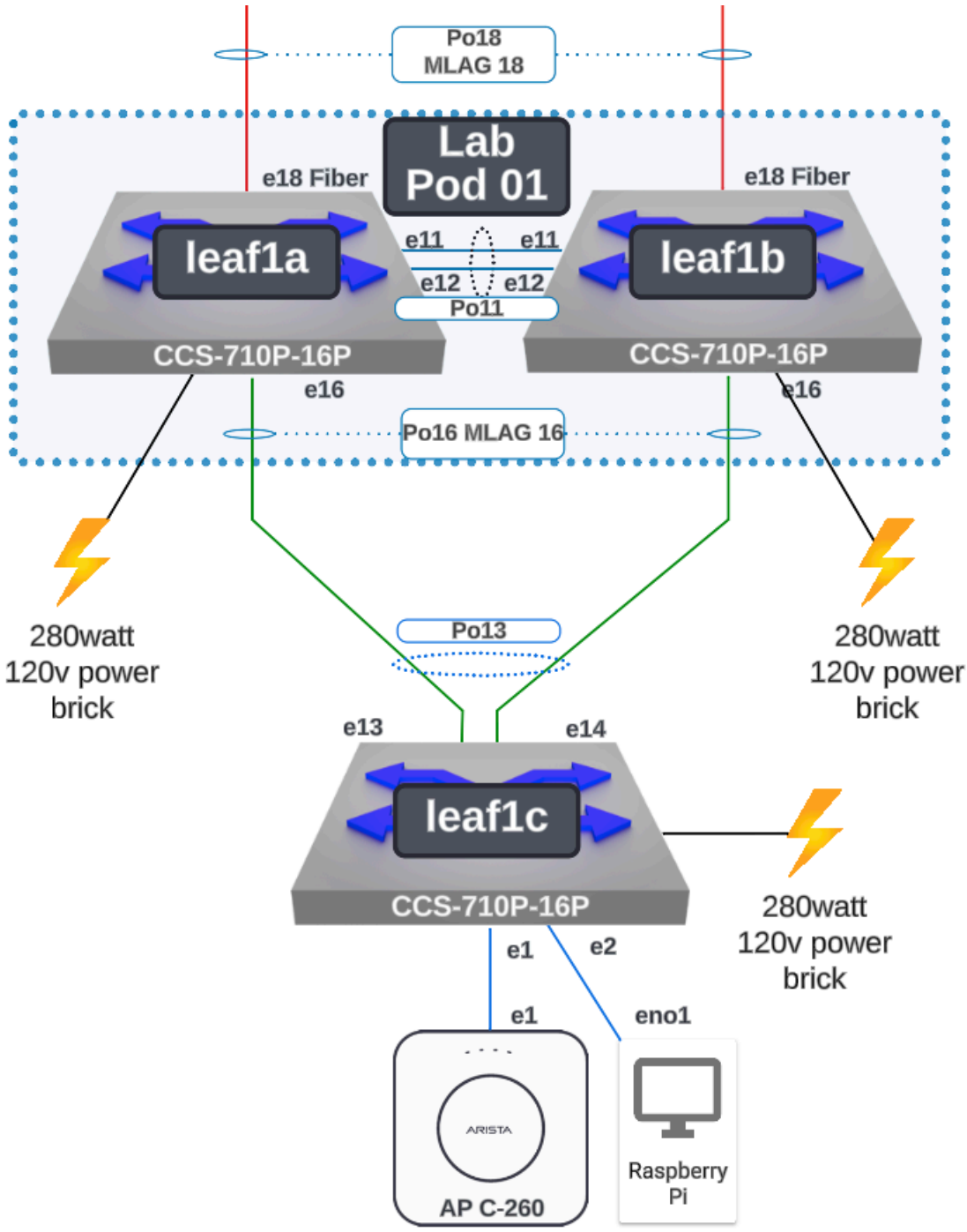
This Lab Guide:
https://github.com/arista-rockies/Workshops/tree/main/Campus

Table of Contents

Full Lab Topology



POD Topology

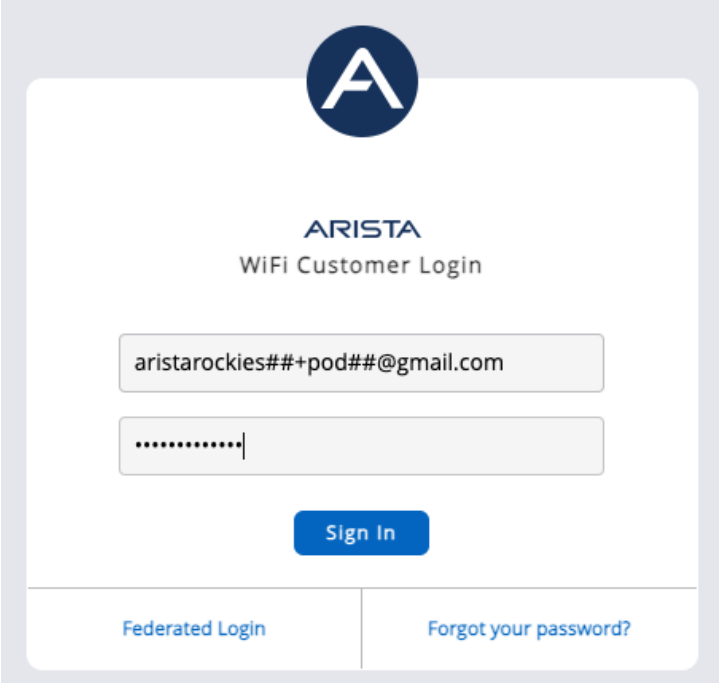


NAC Lab #1 - Create EAP-TLS Wireless Policy

1. CloudVision Cognitive Unified Edge CV-CUE Access

Go to the Arista GUI via: https://launchpad.wifi.arista.com/

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

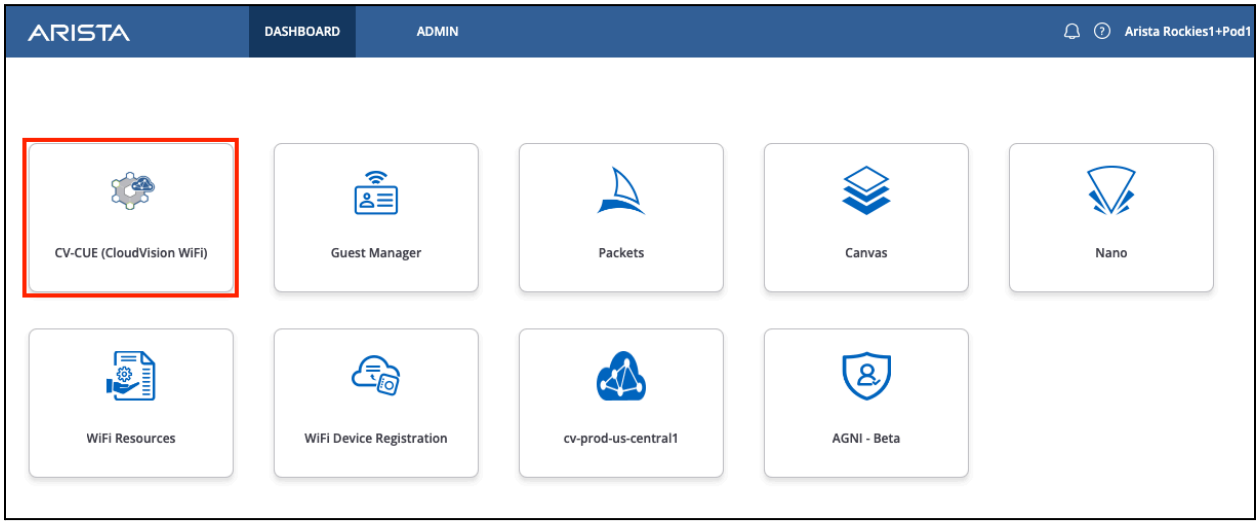


Click **Sign In**

Launchpad

When you open the launcher, you are presented with multiple applications. Each of these applications, with the exception of CloudVision and AGNI, are included with the CV-CUE subscription. CloudVision and AGNI are available from the LaunchPad with their respective subscriptions.

Dashboard tab:



Descriptions for the tiles are below:

- **CV-CUE (CloudVision WiFi)** this is the Wireless Manager
- **Guest Manager** looks at the users and how they are interacting with your environment.
- **Packets** is an online .pcap debug allowing you to examine the packet information.
- **Canvas** is used for Campaigns.
- **Nano** allows you to manage your environment from your smartphone
- **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)

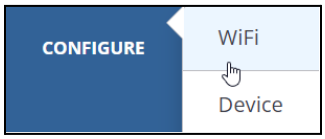
Select CV-CUE (CloudVision WiFi)

2. Create an EAP-TLS SSID

The “**Configure**” section of CV-CUE is broken into several parts, including “**WiFi**”, “**Alerts**”,“**WIPS**”, etc. “**Alerts**” is where syslog and other alert related settings are configured, and “**WIPS**” is where the policies are configured for the WIPS sensor.

In this lab, we will be working in the “**WiFi**” configuration area. Create an SSID (WPA2 802.1X) with your **ATD-##-EAP** as the name (where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod).

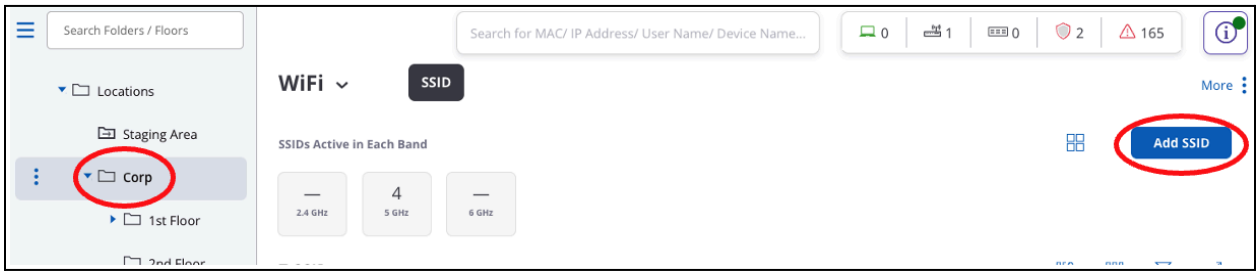
Hover your cursor over the “**Configure**” menu option on the left side of the screen, then click “**WiFi**”.



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.

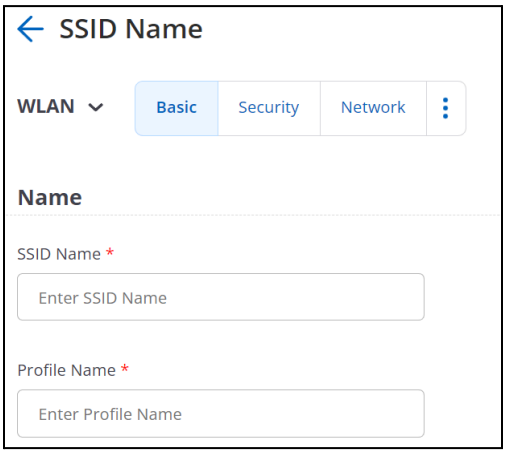
With the hierarchy menu collapsed:

Or, with the hierarchy menu expanded:

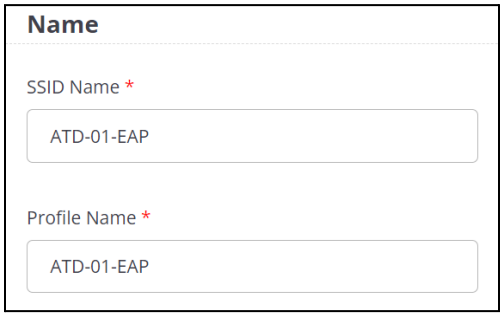


Once on the “**SSID**” page, configuration sub-category menu options will appear across the top of the page related to WiFi (the defaults are “**Basic**”, “**Security**”, and “**Network**”). You can click on these sub-category names to change configuration items related to that area of the configuration.

To make additional categories 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.).

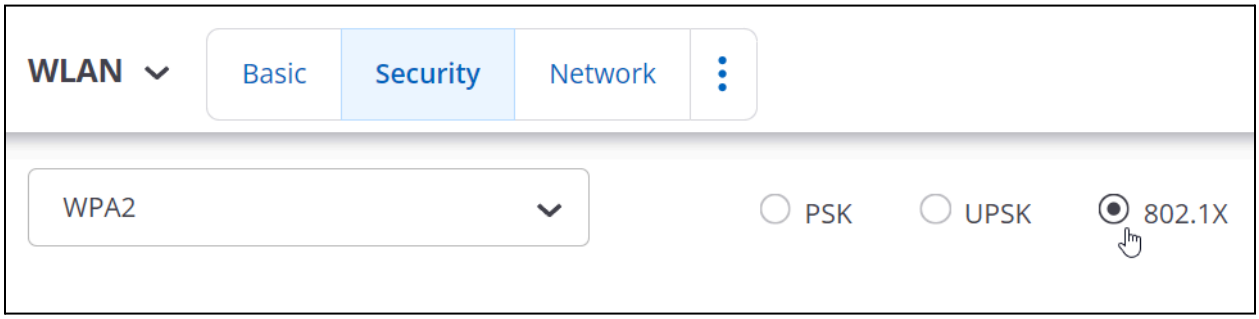


In the “**Basic**” sub-category option, name the SSID “**ATD-##-EAP”** (where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod). The “**Profile Name**” is used to describe the SSID and should have been auto-filled for you.

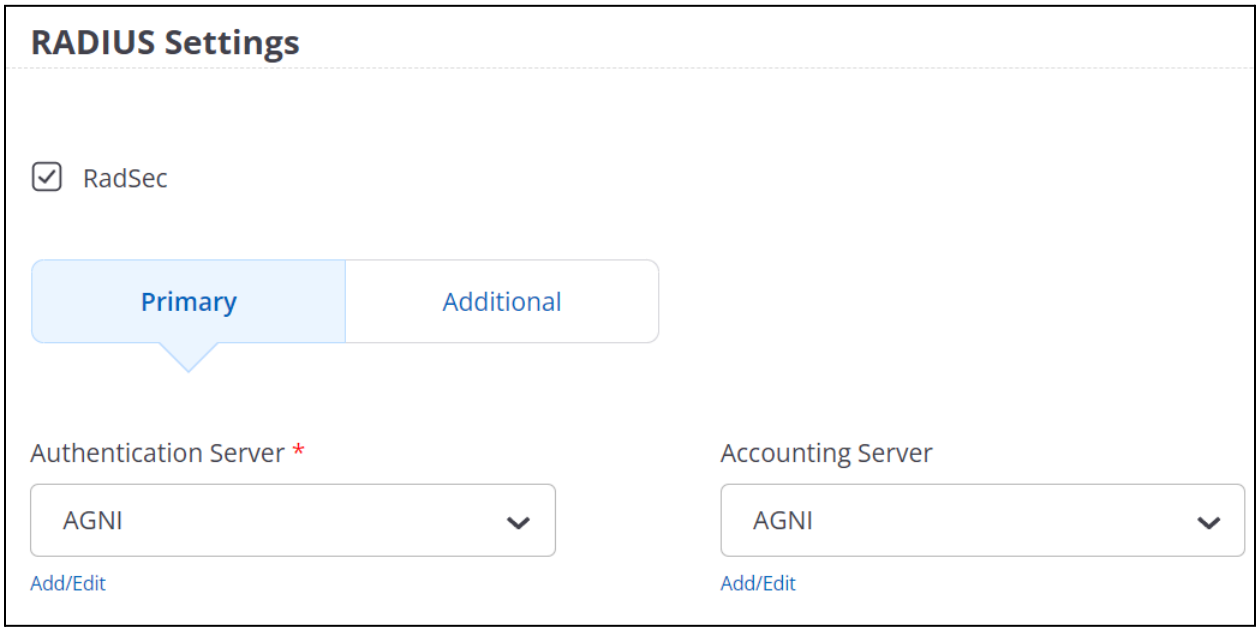


Since this is our corporate SSID, leave the “**Select SSID Type**” set to “**Private**”, but note this is where you would change it to “**Guest**” if needed. Select **Next** at the bottom.

In the “**Security**” sub-category, select WPA2 and change the association type to “**802.1X**”.



Next, under **RADIUS Settings** check **RadSec** and select **AGNI** in the drop down box under Authentication and Accounting Server

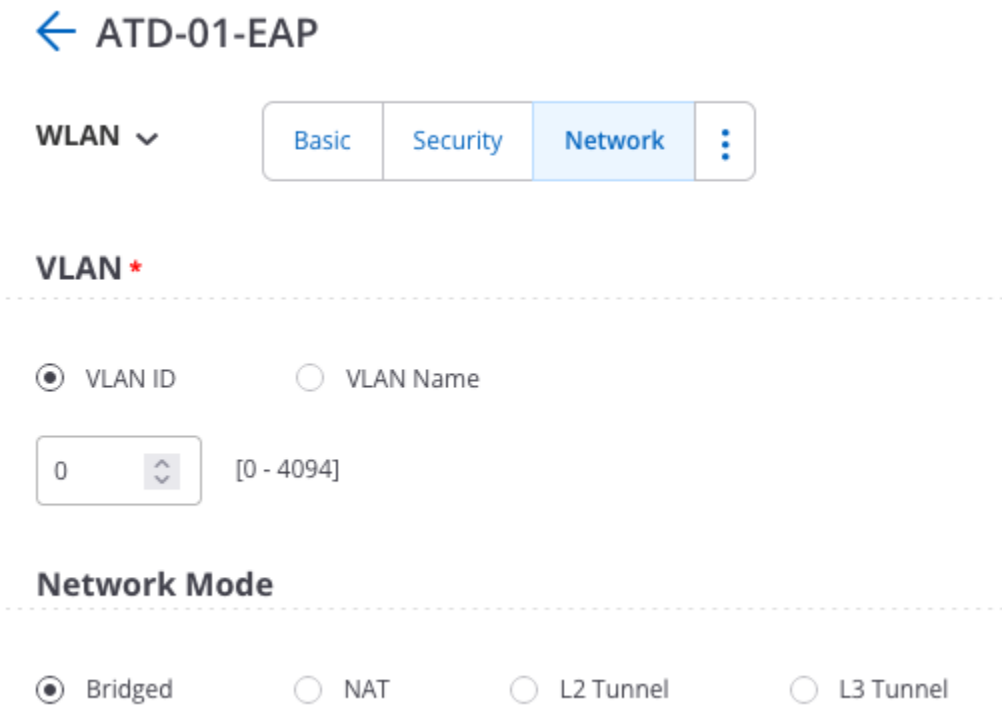


The AGNI Radius Profile is already configured for your use. See Section B for more information on setting up the AGNI Radius Profile.

Select “**Next”** at the bottom of the screen.

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 mapped to.

We are using “**Bridged**” mode in this lab.



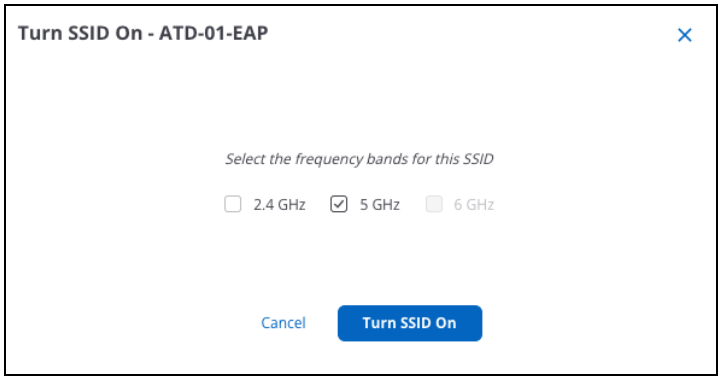
You could use “NAT” (often done for Guest) or “L2 Tunnel” / “L3 Tunnel” (as you would see for a Guest Anchor or tunneled corporate traffic).

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

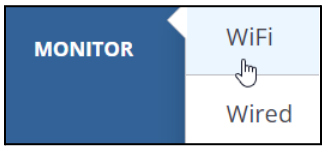
Click the “**Save & Turn SSID On”** button at the bottom of the page.

On the pop-up page, click “**Customize**” if that option appears, otherwise skip to the next step.

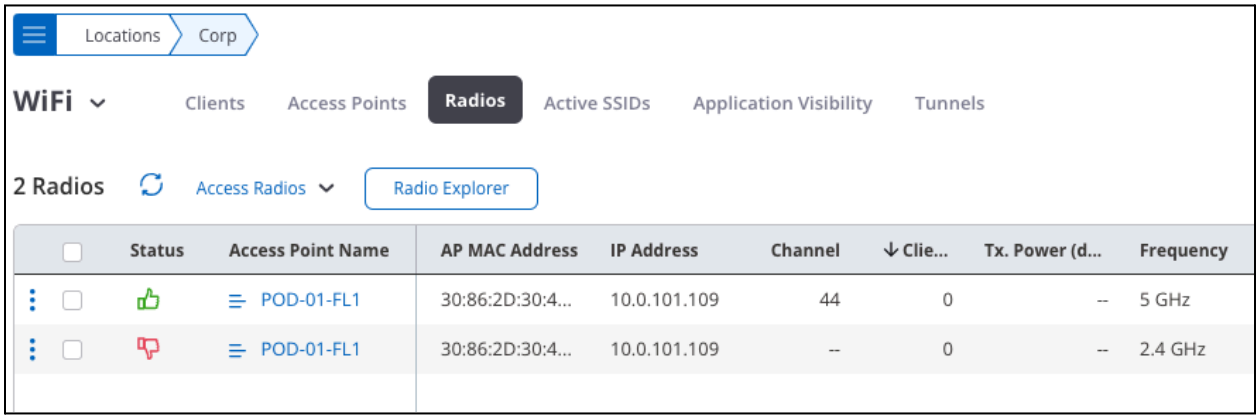
Only select the “5 GHz” option on the next screen (**uncheck** the 2.4 GHz box if it’s checked), then click “**Turn SSID On**”.



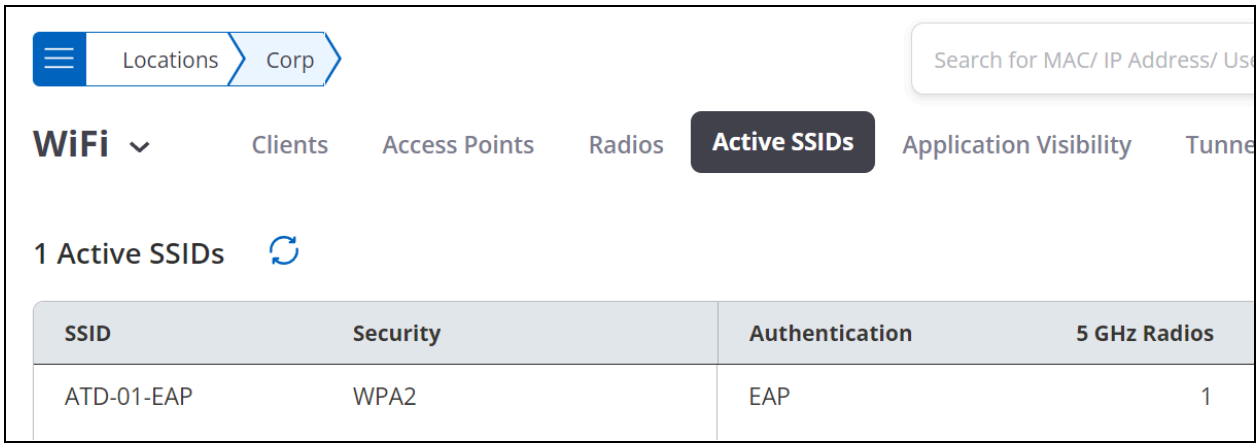
After you turn on the SSID, hover your cursor over "**Monitor**" in the left hand side menu, and then click "**WiFi**".



Now, in the menu options at the top of the page, look at the "**Radios**" menu option. Is the 5 GHz radio "up" and 2.4 GHz radio "down"? It may take a minute or two for the radio to become active.



Check the "**Active SSIDs**" menu at the top of the screen. Is your SSID listed?

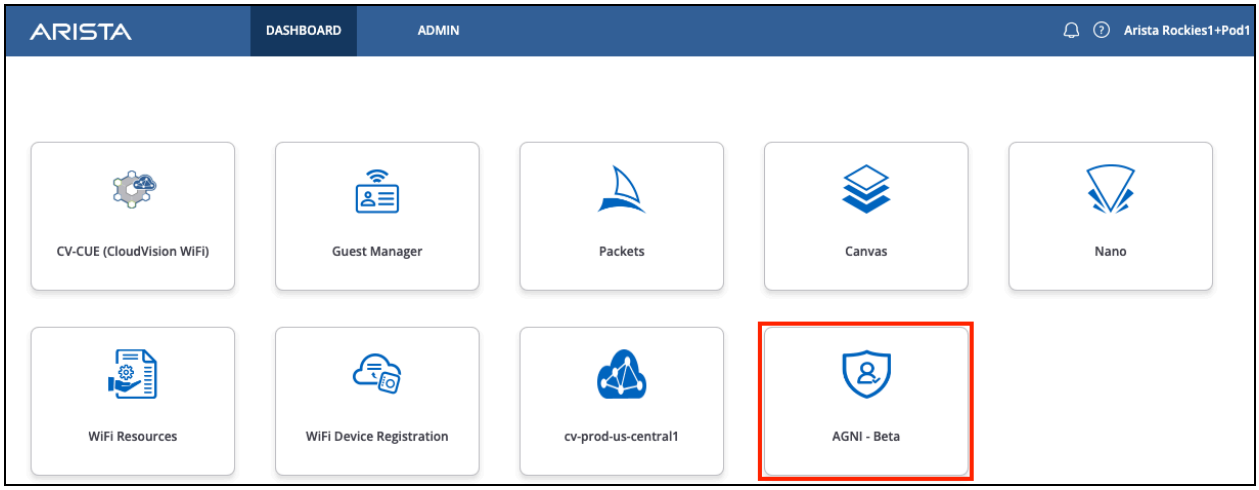

Locations
Corp
Search for MAC/ IP Address/ Use
WiFi
Clients
Access Points
Radios
Active SSIDs
Application Visibility
Tunne
1 Active SSIDs
SSID
Security
Authentication
5 GHz Radios
ATD-01-EAP
WPA2
EAP
1

3. CloudVision AGNI Access

Launchpad

Go back to the LaunchPad, and select the AGNI - Beta tile.

Dashboard tab:

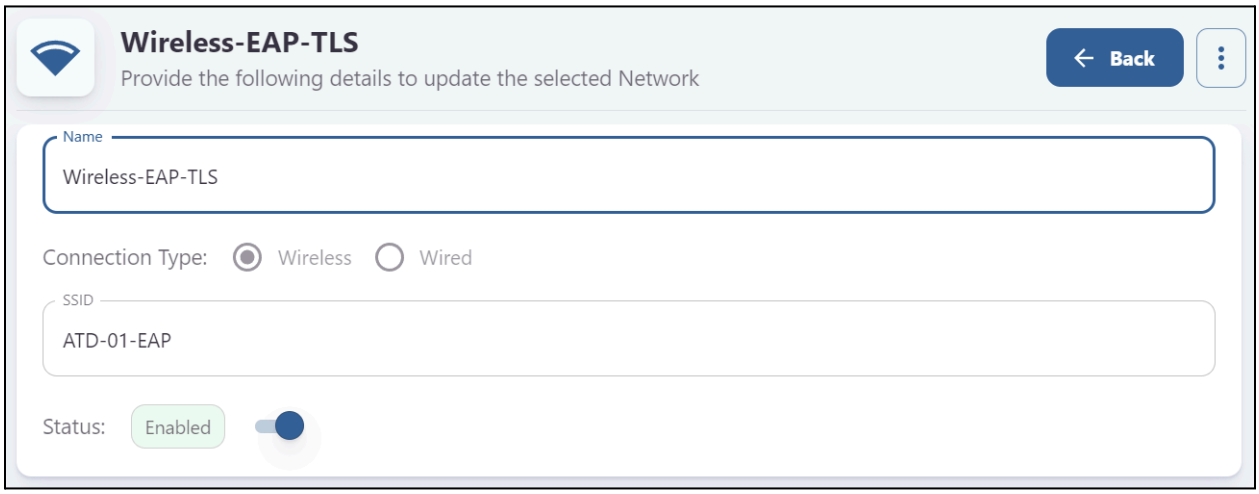


Select AGNI - Beta.

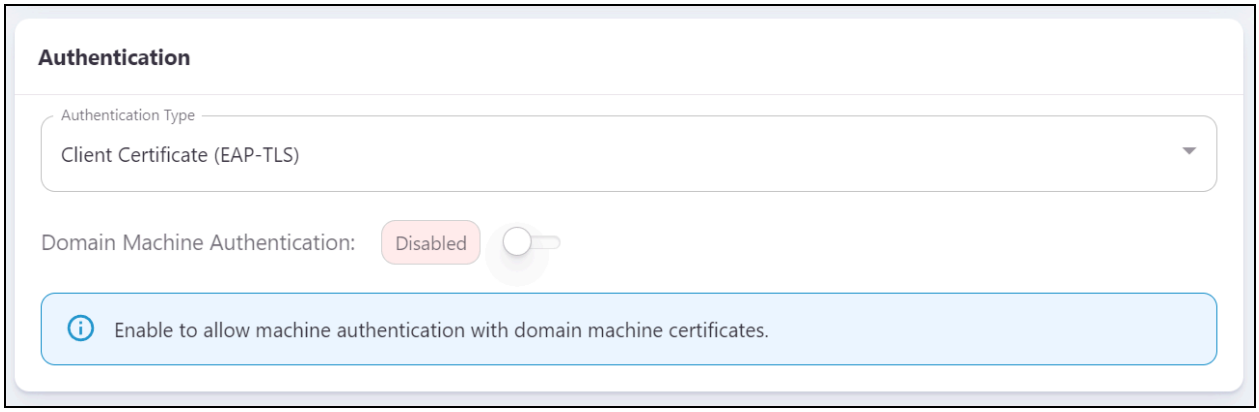
4. Create AGNI Networks & Segments for the EAP-TLS Wireless Policy

Click on **Networks** and select **+ Add Network**

Type in the name **Wireless-EAP-TLS**
Select Connection Type: **Wireless**
SSID needs to match what you created in CV-CUE type **ATD-##-EAP**

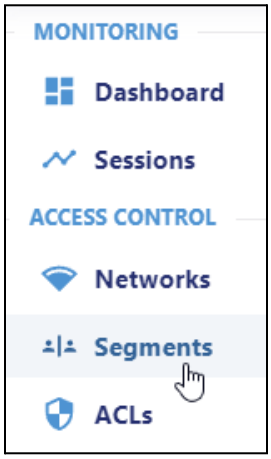


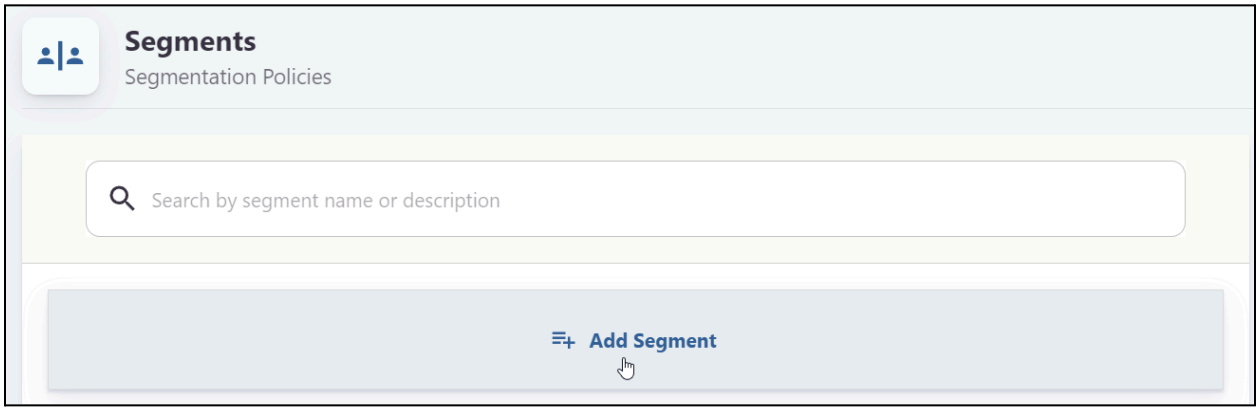
For Authentication select **Client Certificate (EAP-TLS)**



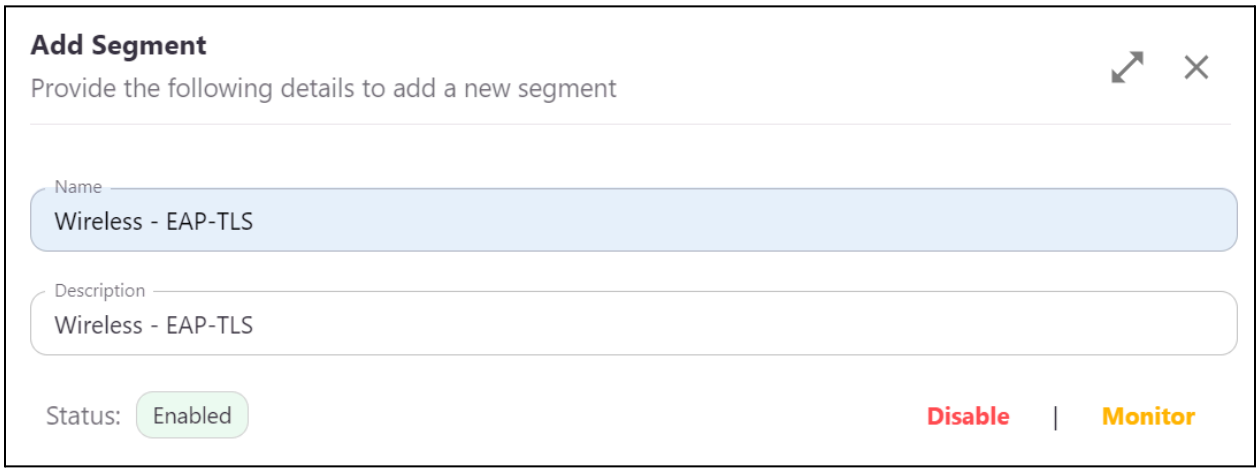
Click on **Add Network** at the bottom of the screen.

Next, click on **Segments** and then **+ Add Segment**



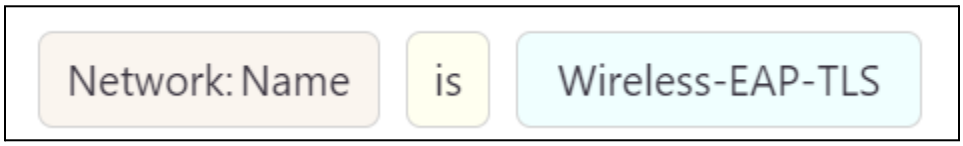


Next, type in the name: **Wireless - EAP-TLS** and the Description as well.



Next, let's **Add Conditions**. ***Note:** Adding more than one condition means MATCH ALL

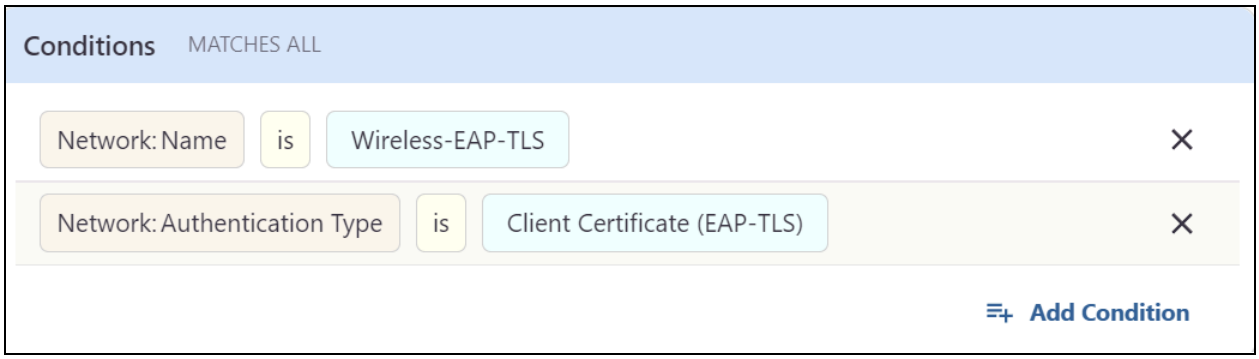
Select, **Network, Name, Is, Wireless-EAP-TLS** from the drop down lists.



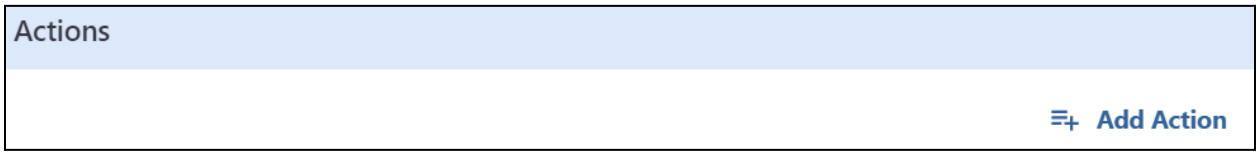
Let's add one more condition.

Select, **Network, Authentication Type, Is, Client Certificate (EAP-TLS)** from the drop down lists.

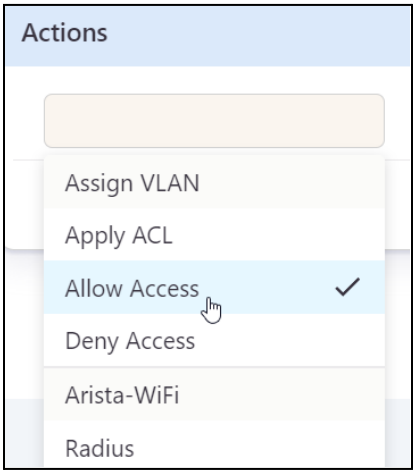
Your Conditions should now look like this.



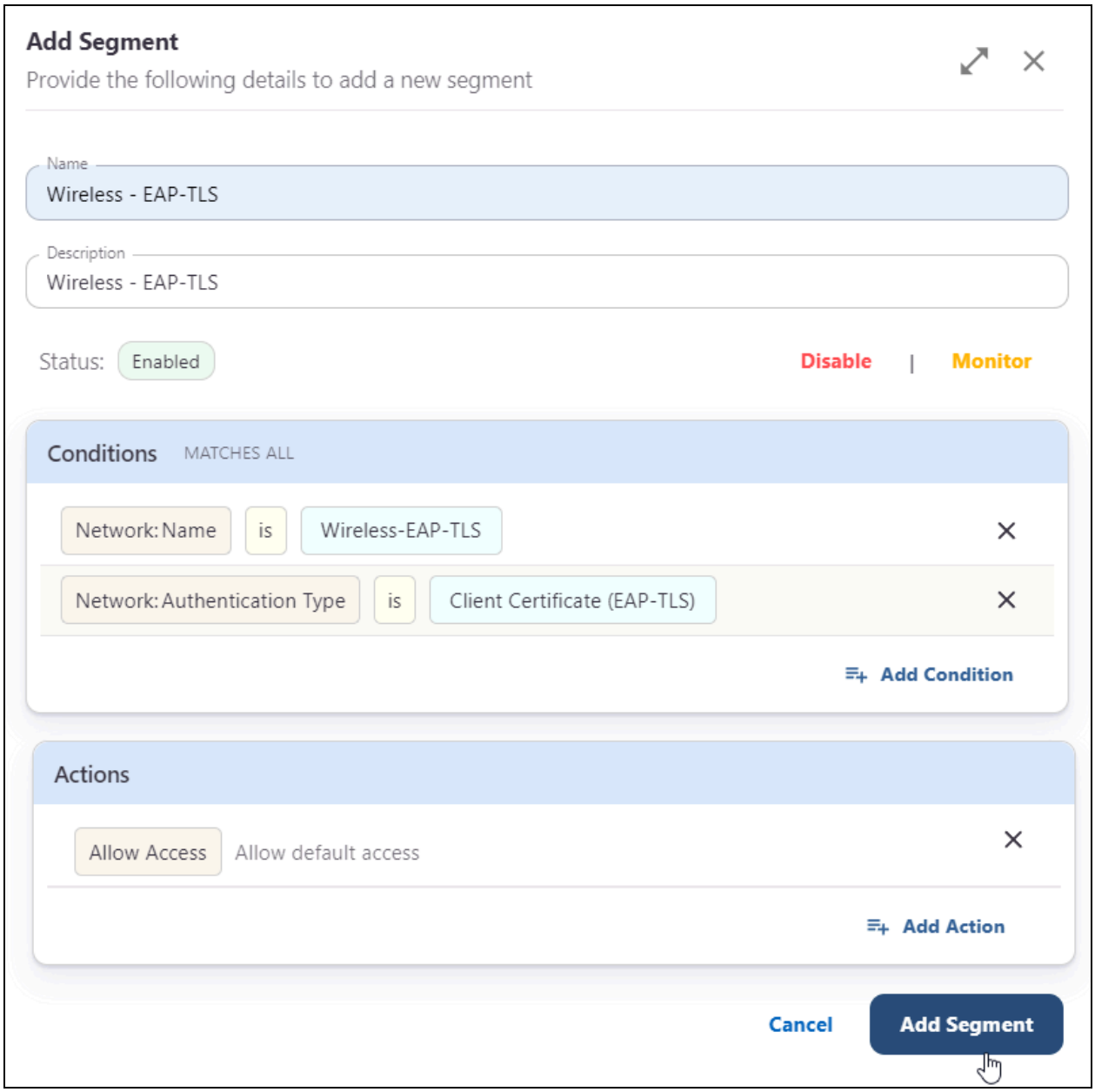
Under Actions select **Add Action**.



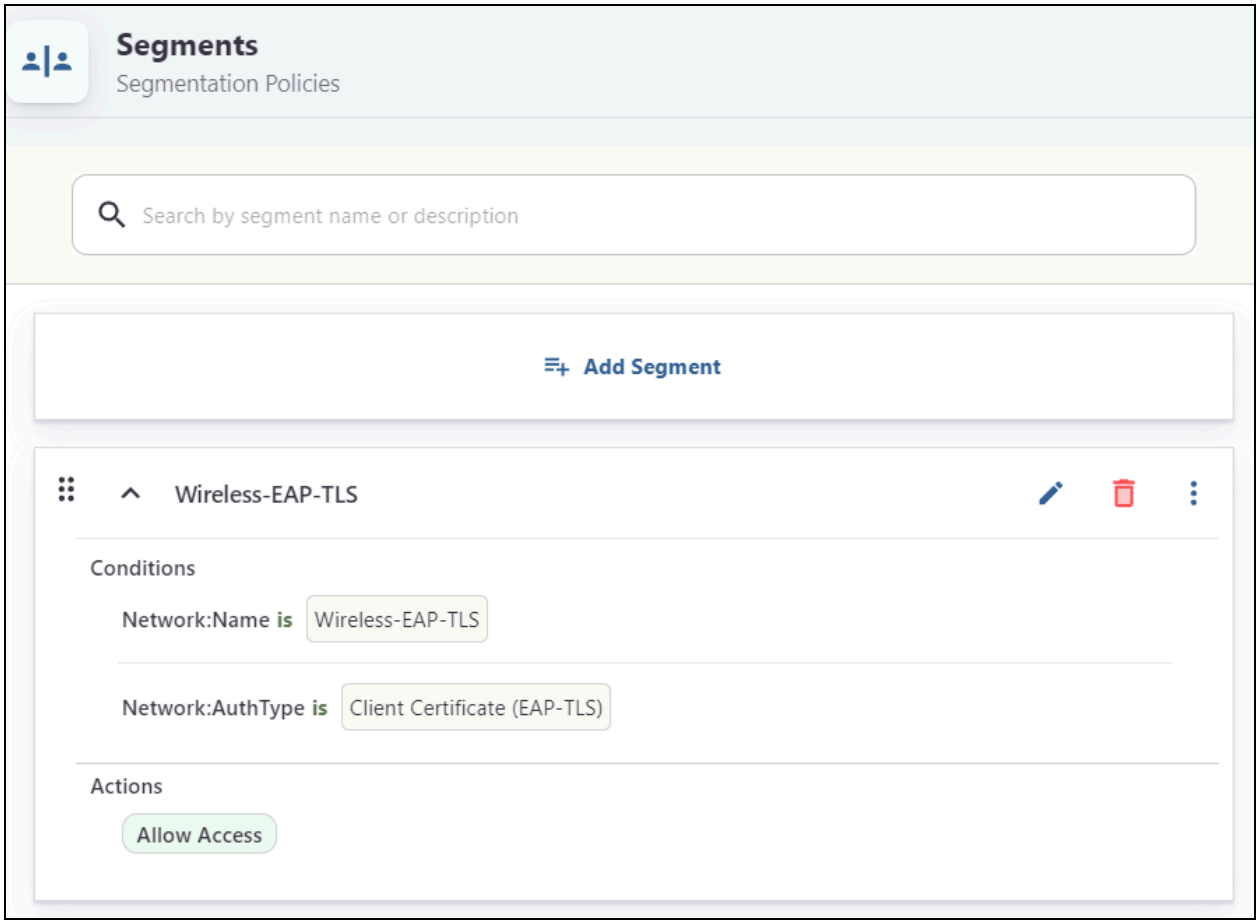
Select Allow Access.



Finally, select Add Segment at the bottom of the page.

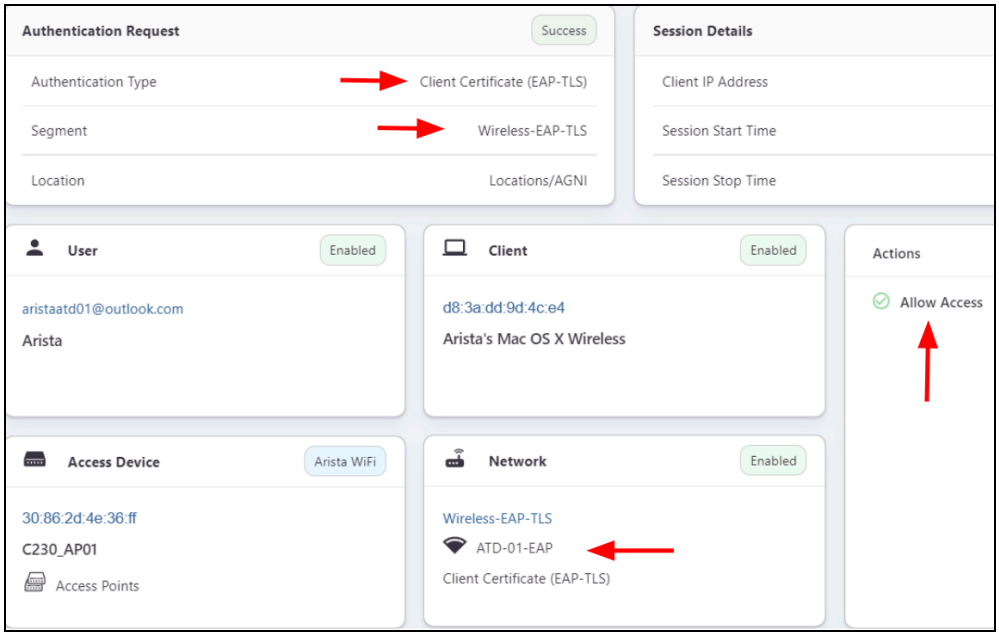


You should now be able to expand and review your segment.



Next, click on **Sessions** to see if your ATD Raspberry Pi has a connection via the Wireless connection. ***Note:** The Client Certificate has already been applied to the Raspberry Pi and is configured to connect to the SSID **ATD-##-EAP**.

If you don't see any new sessions within 2 minutes AGNI, power cycle the Raspberry Pi.



NAC LAB #1 COMPLETE

Additional Information

A. RadSec: Installing the AP Certificate

What is RadSec?

- CloudVision AGNI integrates with network infrastructure devices (wired switches and wireless access points) through a highly secure TLS-based RadSec tunnel.
- Port 2083
- The highly secure and encrypted tunnel offers complete protection to the communications that happen in a distributed network environment. This mechanism offers much greater security to AAA workflows when compared with traditional RADIUS environment workflows, which are not encrypted.

https://www.arista.com/en/support/toi/eos-4-27-0f/14891-radius-dynamic-authorization-over-tls

Click on the AGNI Tile from the LaunchPad and it will open a new Tab.

*Note: When applying the Certificate to the AP it is recommended to have both the CV-CUE and AGNI windows opened side by side.

The Arista's C-2xx (except the C-250/C-260) and C-3xx Series APs include a TPM chip. Here is a video explaining the setup process.

RadSec Tunnel with TPM chip APs

RadSec Tunnel with Arista AP using Custom certificate (non-TPM chip AP's)

The RADIUS protocol uses UDP as underlying transport layer protocol whereas RadSec is a protocol that supports RADIUS over TCP and TLS. Therefore, by design in order to create a TLS connection between two devices certificates are used.
With the proliferation of IoT devices, mobile users, and remote access, networks have become more complex and diverse, making traditional RADIUS susceptible to eavesdropping and man-in-the-middle attacks. RadSec's integration of secure Transport Layer Security (TLS)

encryption addresses these vulnerabilities, providing a robust defense against unauthorized access, data interception, and tampering.

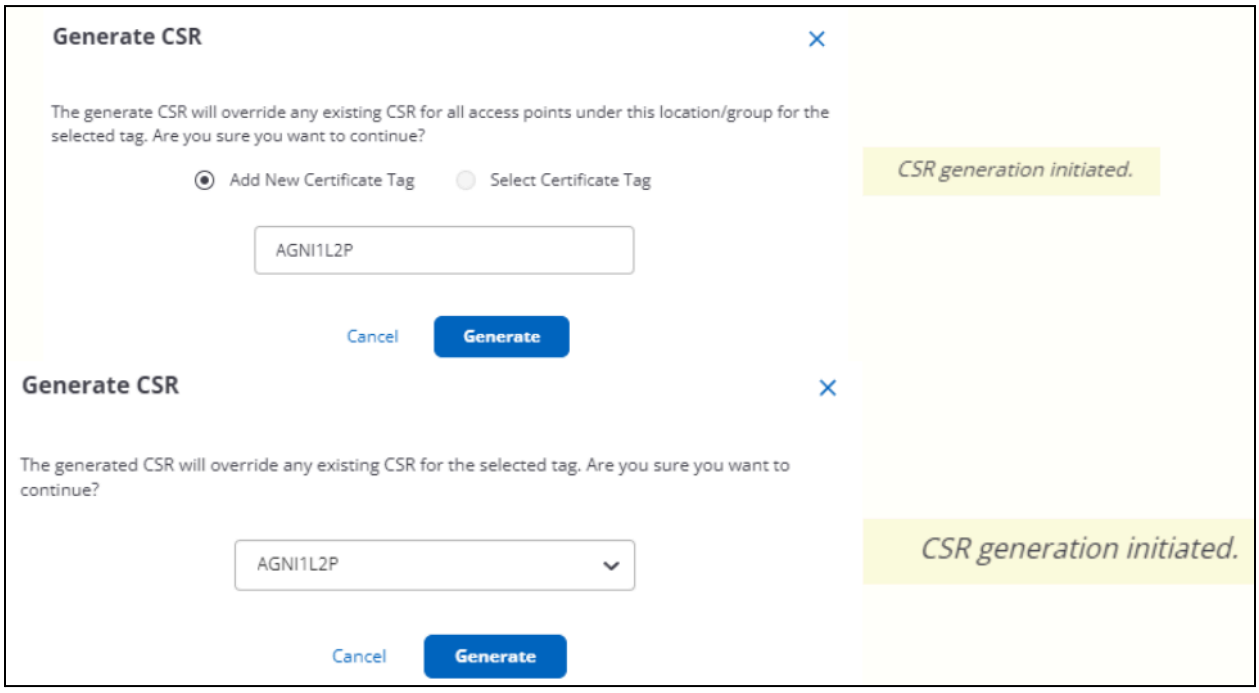
Arista C-2xx (except the C-250/C-260), O-2xx, and C-3xx already have a TPM chip which has the required certificate that can be used for RadSec. However, if the TPM chip does not exist then, starting from 15.0.0 CV-CUE supports Custom Certificate Management for Access Points.

Here is a Summary of the Steps:

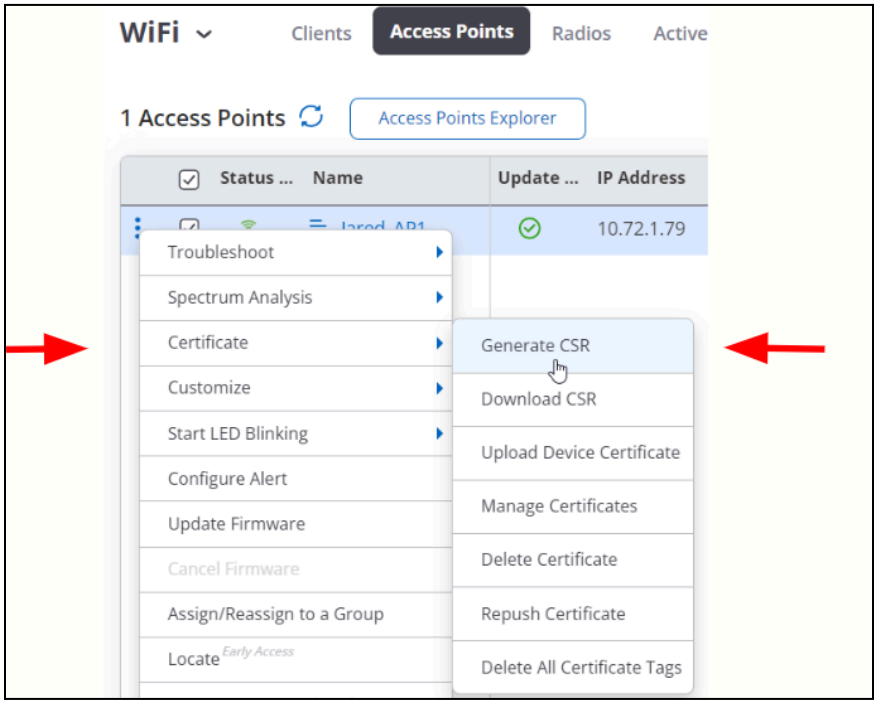
- Launchpad - Add AP and assign the Service
- CV-CUE - Create a Folder and move the AP
- CV-CUE - Generate CSR TAG and then Download CSR (.zip) - Unzip it for the .CSR
- AGNI - Add the device as a new AP under Access Devices
- AGNI - Click on your AP and then select Get Client Certificate
- AGNI - Upload the CSR and Generate Certificate
- CV-CUE - Click on your AP and Upload Device Certificate and select TAG and AP.pem file
- AGNI - Under Administration click on RadSec settings and download Cert and copy hostname
- CV-CUE - In your Folder, Create a RADIUS RadSec server and apply the RadSec Cert from AGNI and Select your CSR TAG - FQDN: radsec.beta.agni.arista.io
- CV-CUE - Create an SSID and point to the RADIUS client you created using WPA2 802.1X RadSec.
- AGNI - Create a User Account
- AGNI - Add Client
- AGNI - Under Networks - I recommend starting with just a MAC auth example to make sure everything is running like you expected and point it to your SSID

First we Generate a CSR in CV-CUE. Click on Monitor and then WiFi

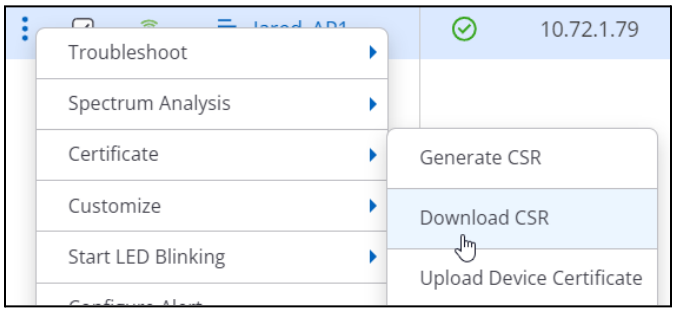
On Right hand side on top and click on Certificate Actions

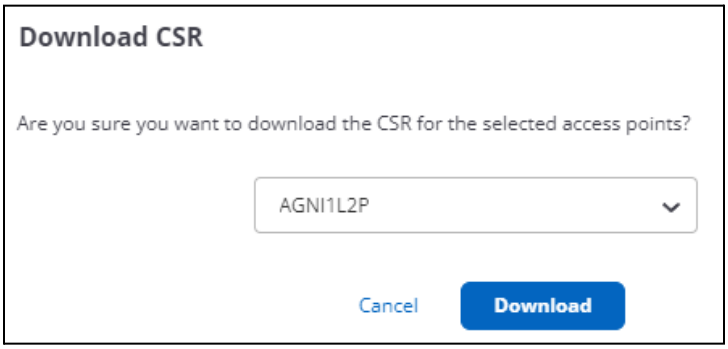


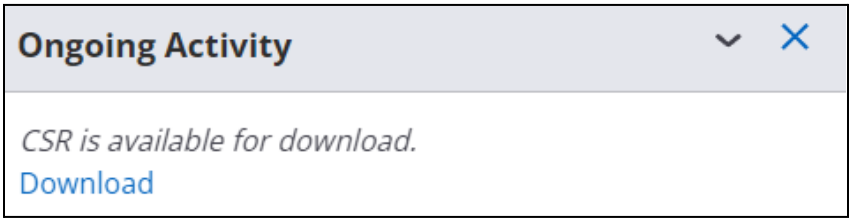
Next, Right Click on the AP and select Generate CSR and select your Certificate Tag.



Next, Right Click on the AP and select Download CSR and select your Certificate Tag.



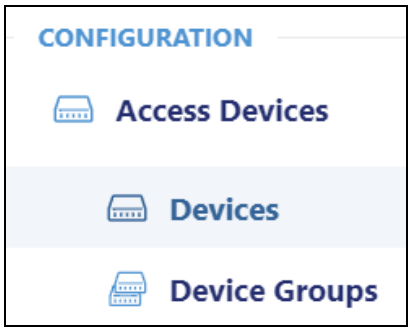


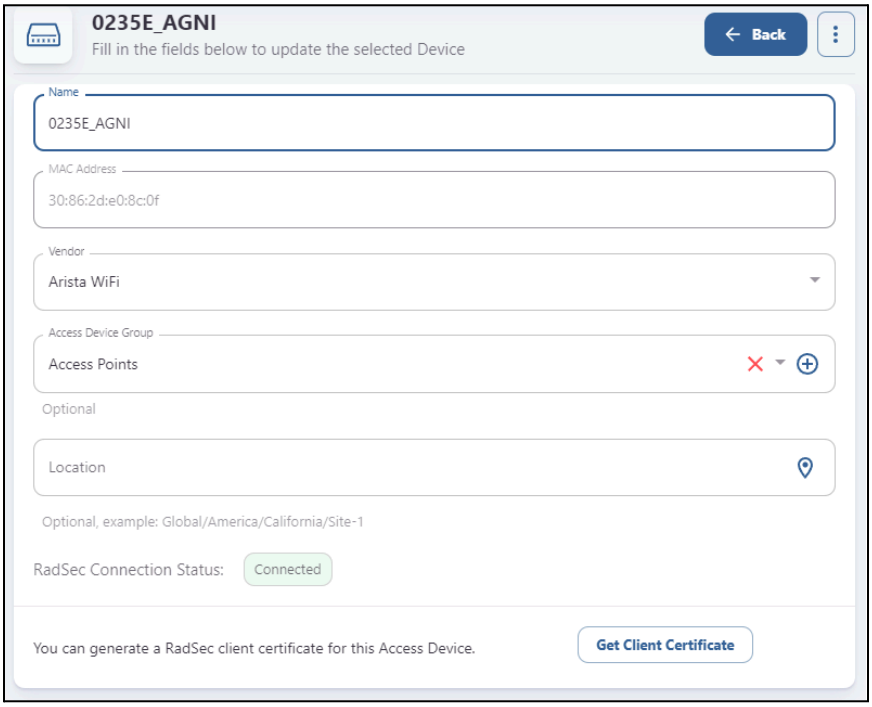


Unzip the CSR File

AGNI - Click on Access Devices and Select the AP.

Access Devices → Devices → Select AP → Get Client Certificate





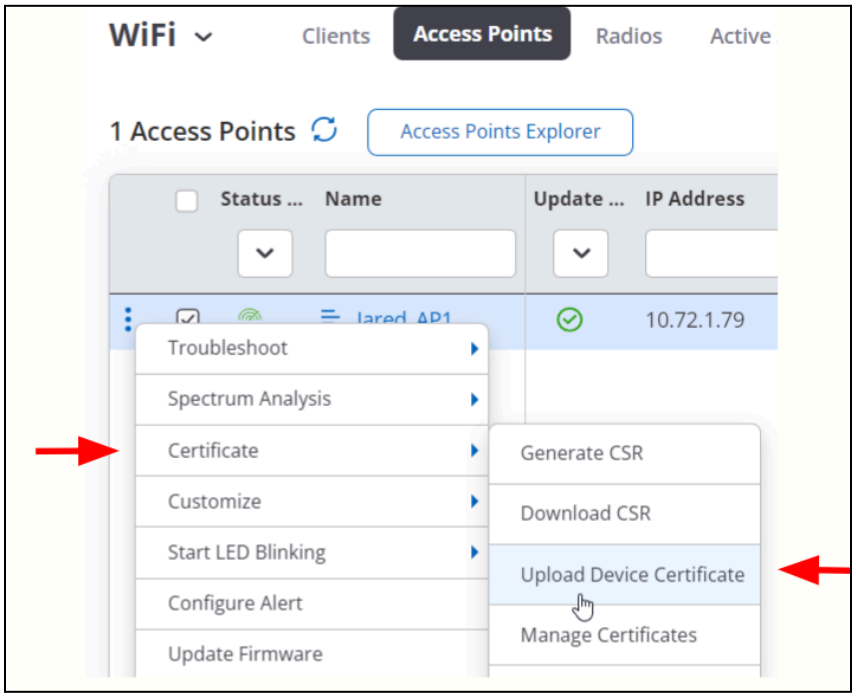
Select **Get Client Certificate.**

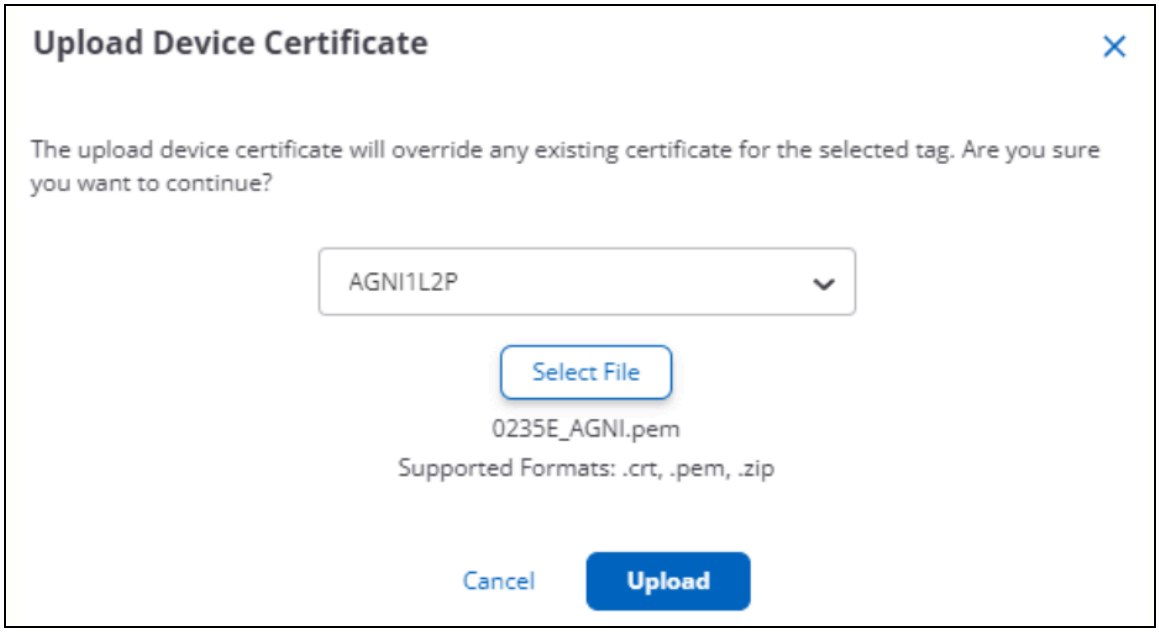
Next, Select Generate Certificate: **Use CSR (Single Device)**, and Select Action: **Upload CSR File,** and browse to and select the CSR file that you unzipped earlier in the process.

Select **Generate Certificate** and the AP Client Certificate will be created and downloaded to your device.

CV-CUE - Upload the Device Certificate

Go to Monitor → WiFi → Access Points → Select AP → Certificate → Upload Device Certificate, and upload the Client/Device Certificate that was downloaded to your device. Use the same Certificate Tag as when you Downloaded the CSR above.





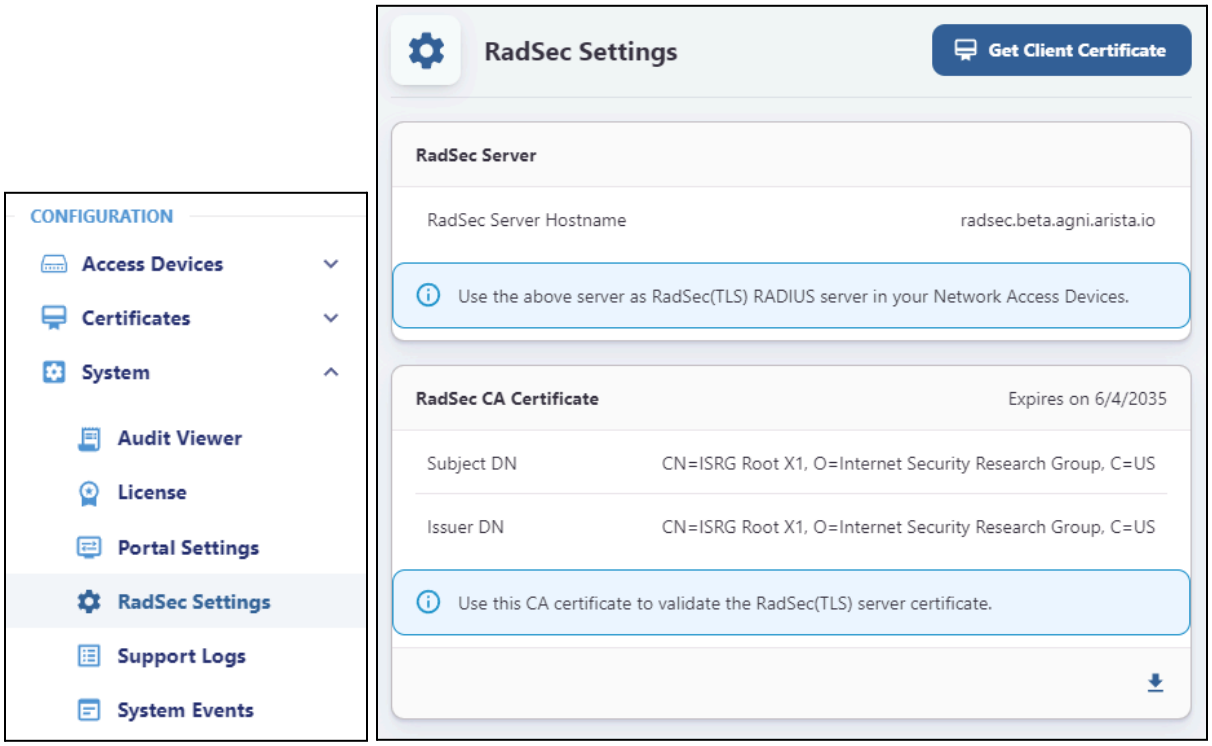
Next, in AGNI click on Access Devices and then Devices look at the RadSec Status.

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS	UPDATE TIME
1	**0235E_AGNI**	30:86:2d:e0:8c:0f	Arista WiFi			7/5/2023 15:50:47

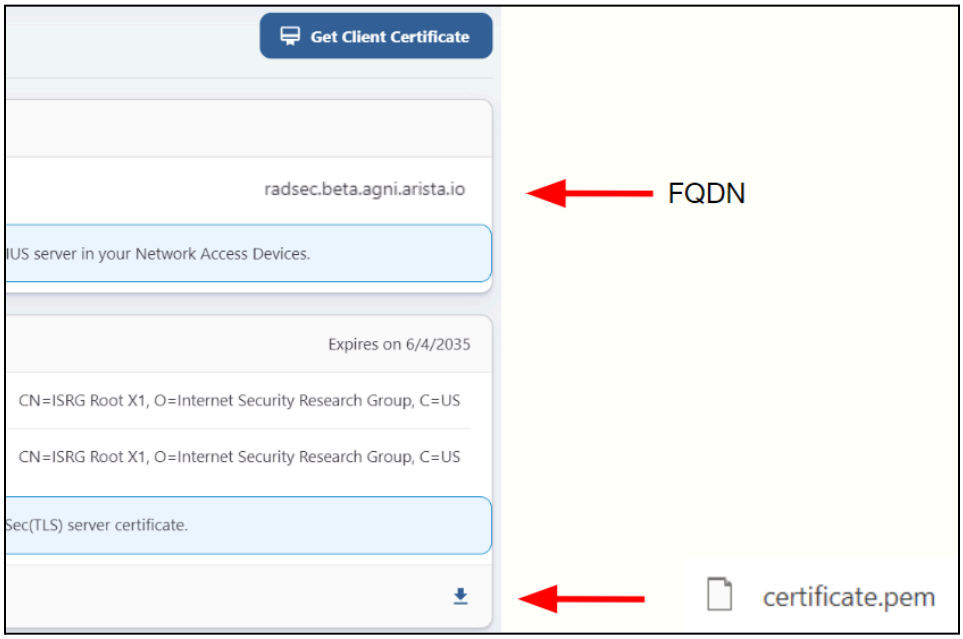
If the AP does not connect, issue a reboot.

B. Setup Radius RadSec Server

In AGNI - Click on **Configuration - System - RadSec Settings** on the left hand side.

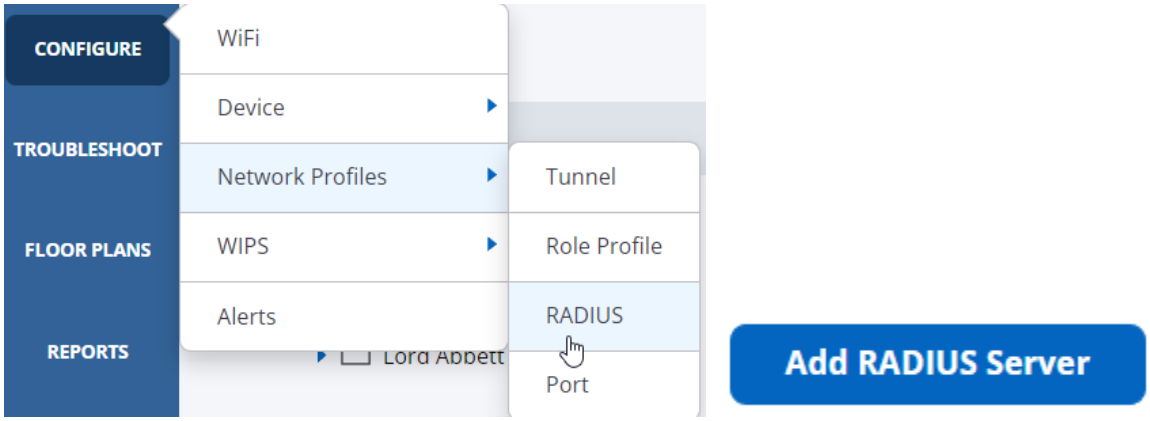


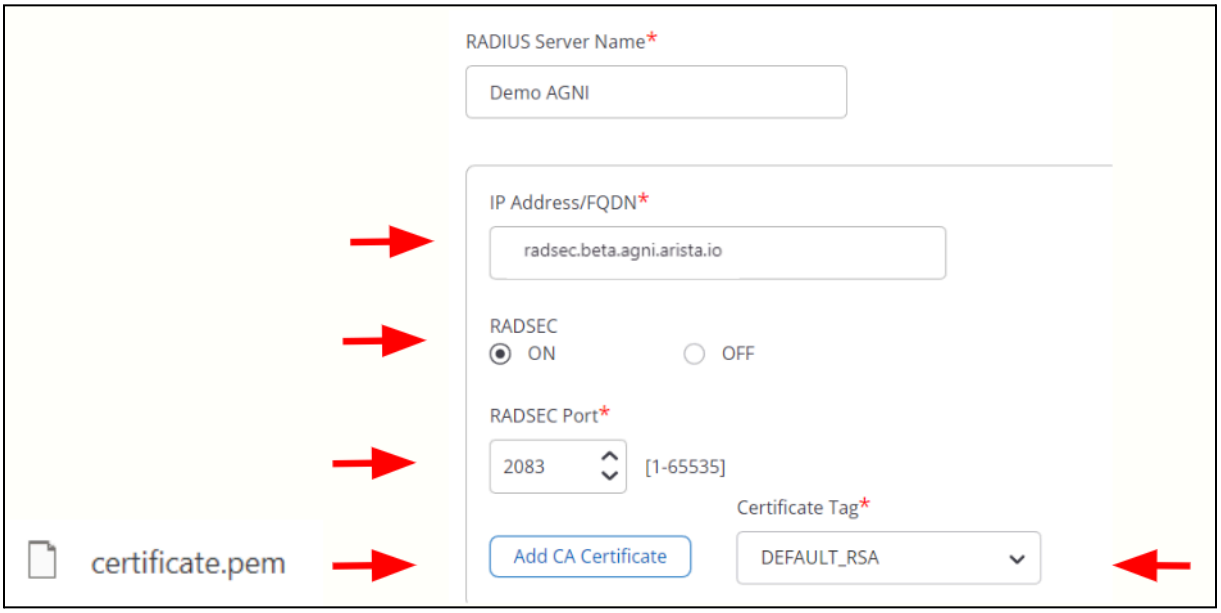
Copy the FQDN (**radsec.beta.agni.arista.io**) and Download the Certificate at the bottom.



Next, go back to CV-CUE and let's set up a RadSec Server.

Configure → Network Profiles → RADIUS



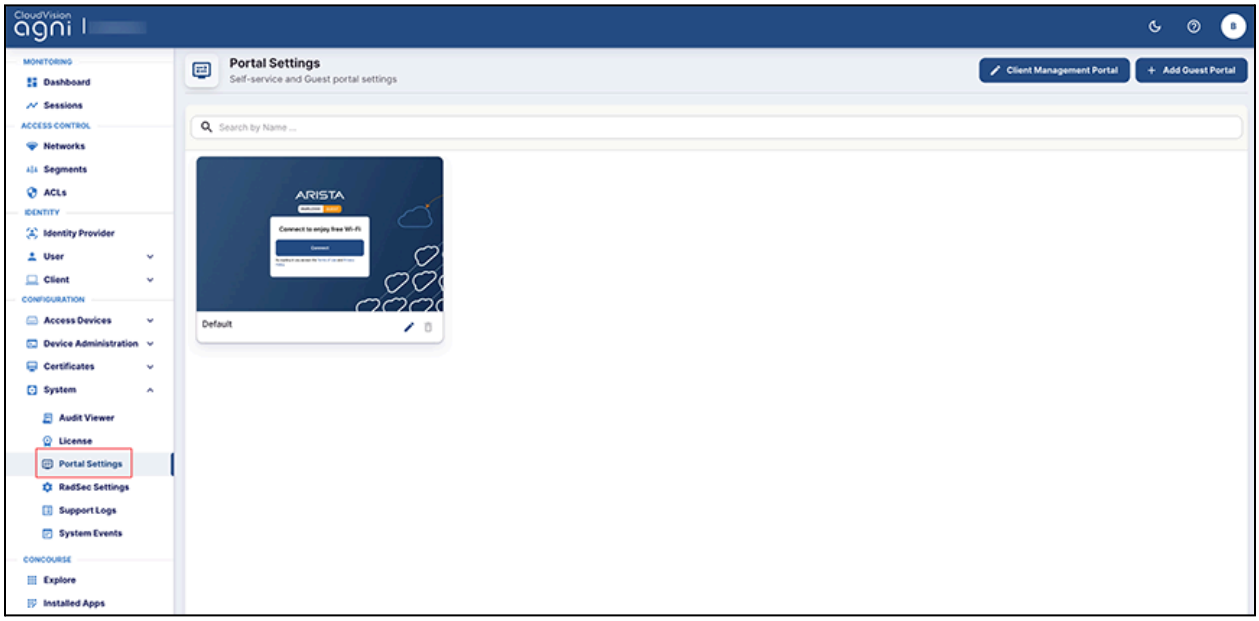


C. Create an AGNI Guest Captive Portal

Next, we'll configure a Guest Captive Portal using AGNI for wireless clients. To configure the guest portal, you must configure both AGNI and CV-CUE.

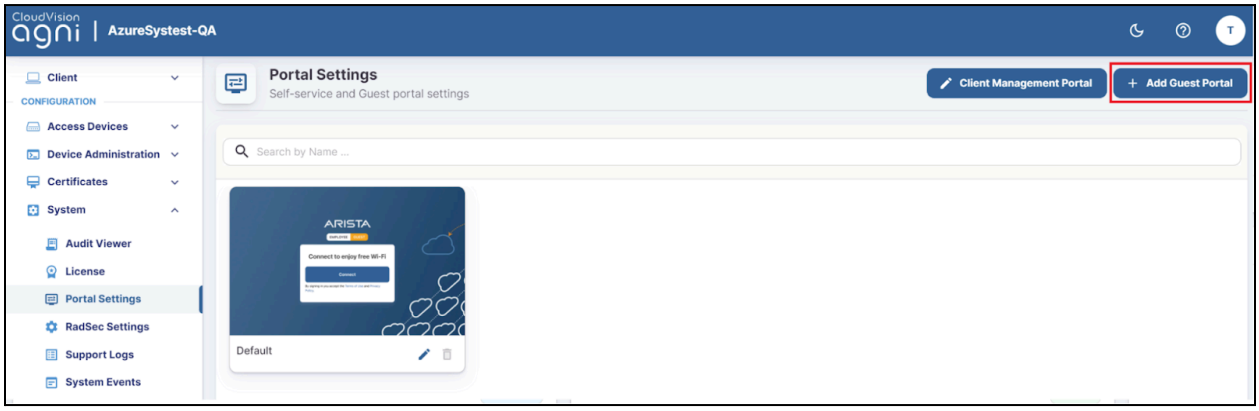
Configuring AGNI

Log in to AGNI and navigate to **Configuration > System > Portal Settings.**

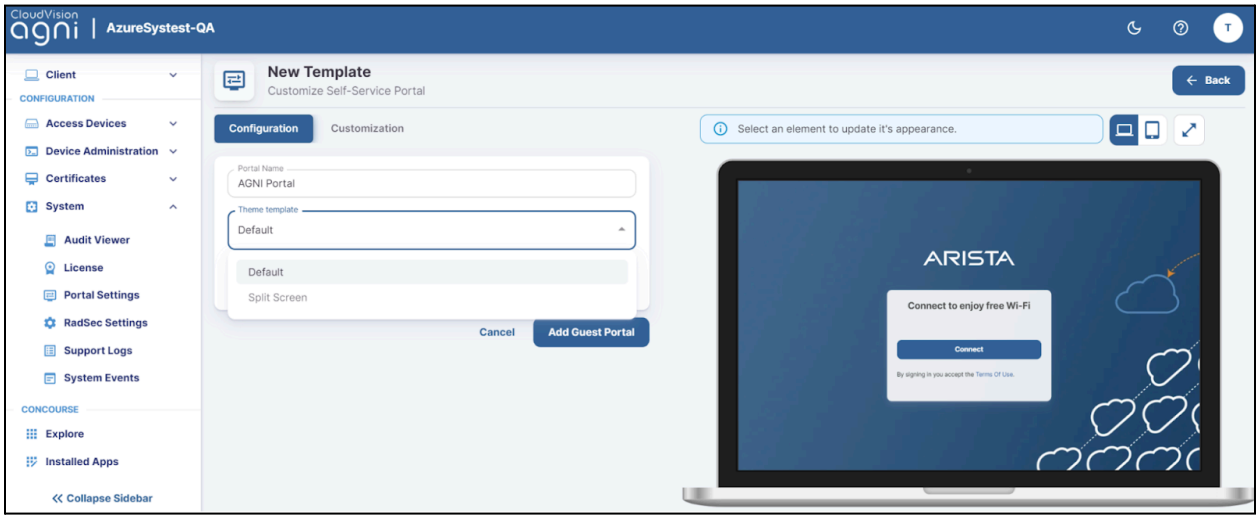


In **Portal Settings**, the **Default** portal is always present, which is non-removable. You can use the same for configuration. Let's create a new guest portal.

Click the **Add Guest Portal** button.



In the **Configuration** tab, provide the portal name (AGNI Portal) and select the theme of the portal. The available theme options are **Default** or **Split Screen.**

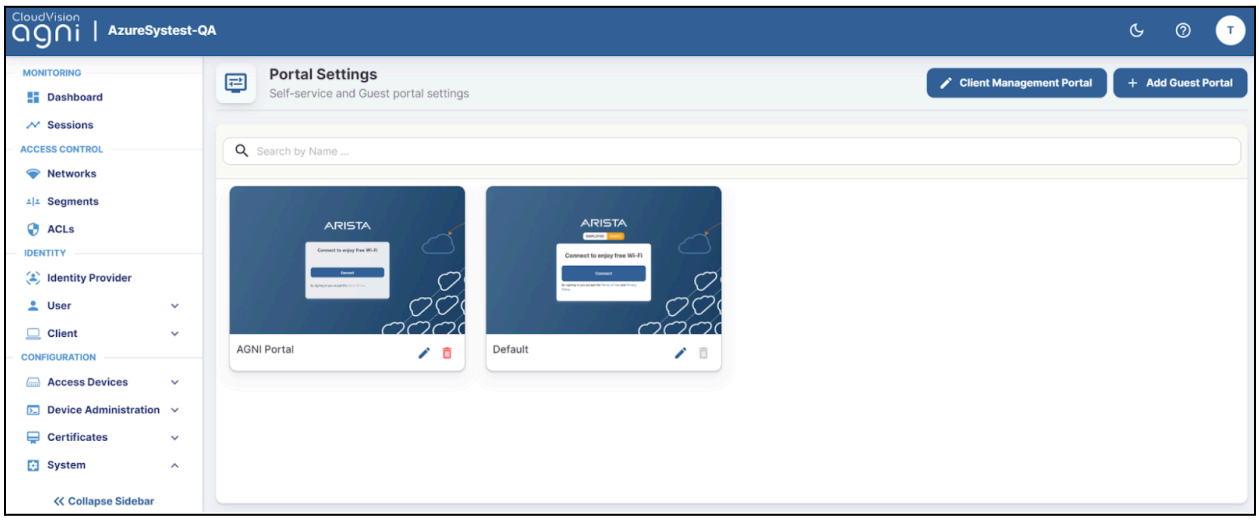


Select the Authentication Type as **Clickthrough.**

Click the **Customization** tab to customize the portal settings, including:

Page
Login Toggle
Terms of Use and Privacy Policy
Logo
Guest Login Submit Button
Etc

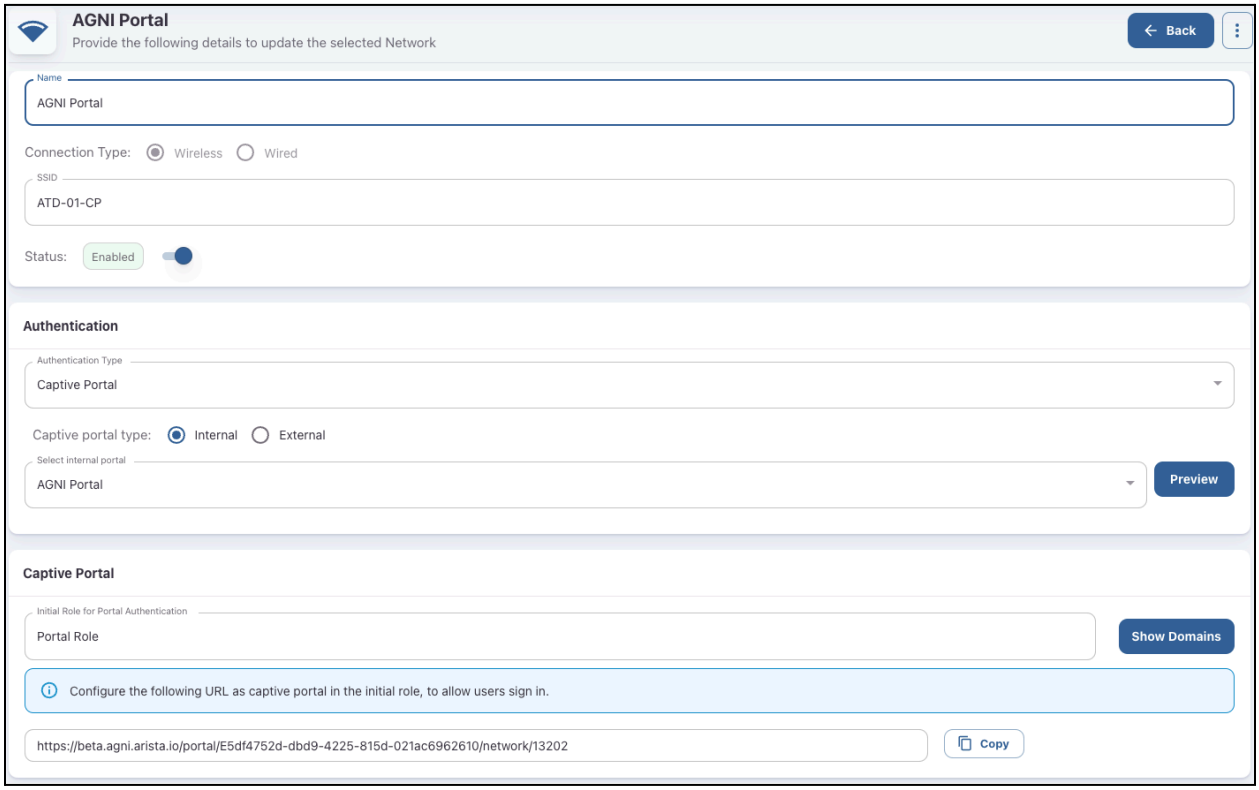
When done, click **Add Guest Portal.** The portal gets listed in the portal listing.



Navigate to the **Access Control > Networks.**

Add a new network with following settings:

Name - **Wireless-Guest-CP**
Connection Type — **Wireless**
SSID - Guest SSID in CV-CUE (**ATD-##-CP**)
Authentication Type - **Captive Portal**
Captive Portal Type - **Internal**
Select Internal Portal - **AGNI Portal**
Internal Role for Portal Authentication - **Portal Role**



Click **Add Network.**

Copy the portal URL at the bottom of the page.

Configuring CV-CUE

In CV-CUE, configure a role profile and the SSID settings. Ensure that the SSID is enabled for the captive portal with redirection to the portal URL.

Configuring Portal and Guest Role Profiles

Portal Role Profile

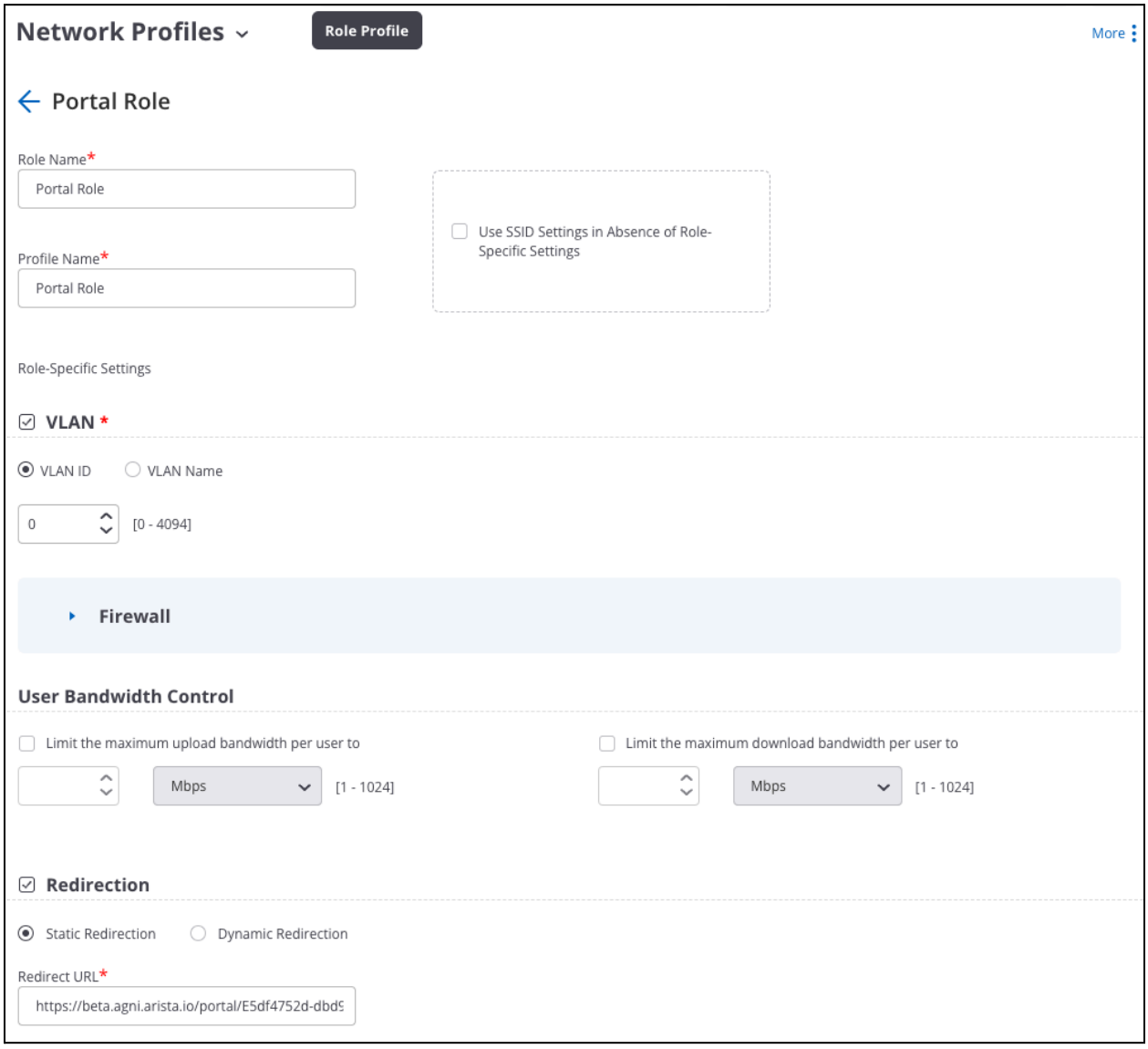
Log in to CV-CUE and navigate to **Configure > Network Profiles > Role Profile**.

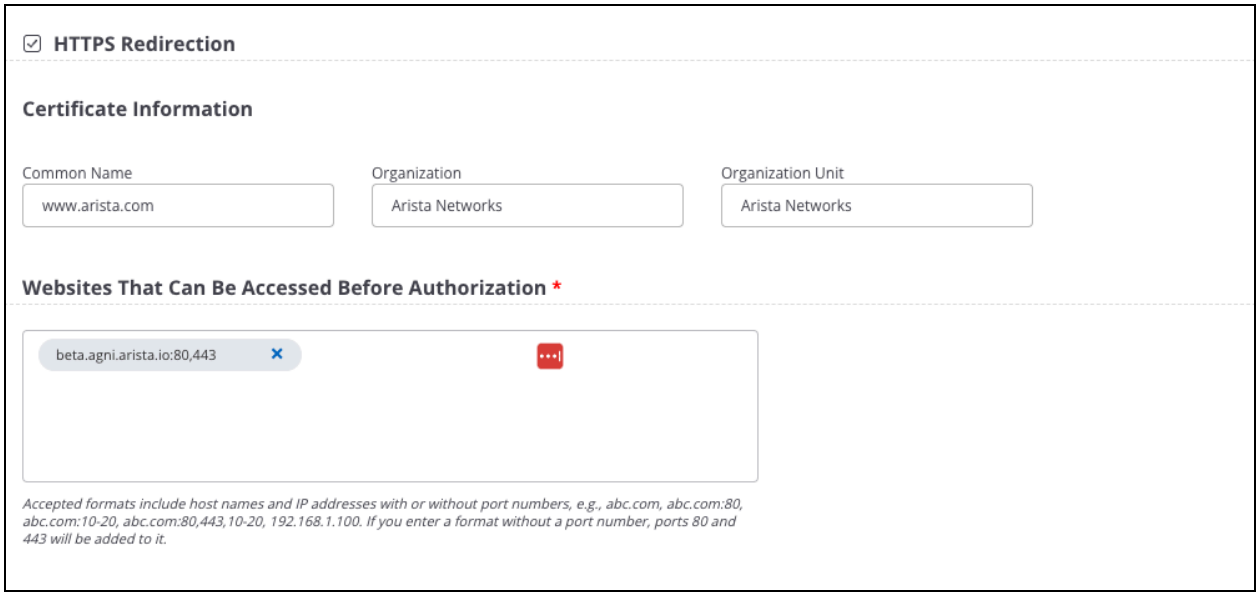
Add Role Profile.

Add the Role Name as **Portal Role**.

Enable the **Redirection** check box and select **Static Redirection**.

In the **Redirect URL** field, add the portal URL that you have copied from AGNI.





Click **SAVE** at the bottom of the page.

***Note:** **The Guest Role and Wireless-Guest-CP Segment are not required for Click Through Guest Access. If users are required to create a guest account or receive approval, then the Guest Role and Wireless-Guest-CP Segment are required.**

The sections below with * preceding the section are not required for Click Through Guest Access.**

****Guest Role Profile**

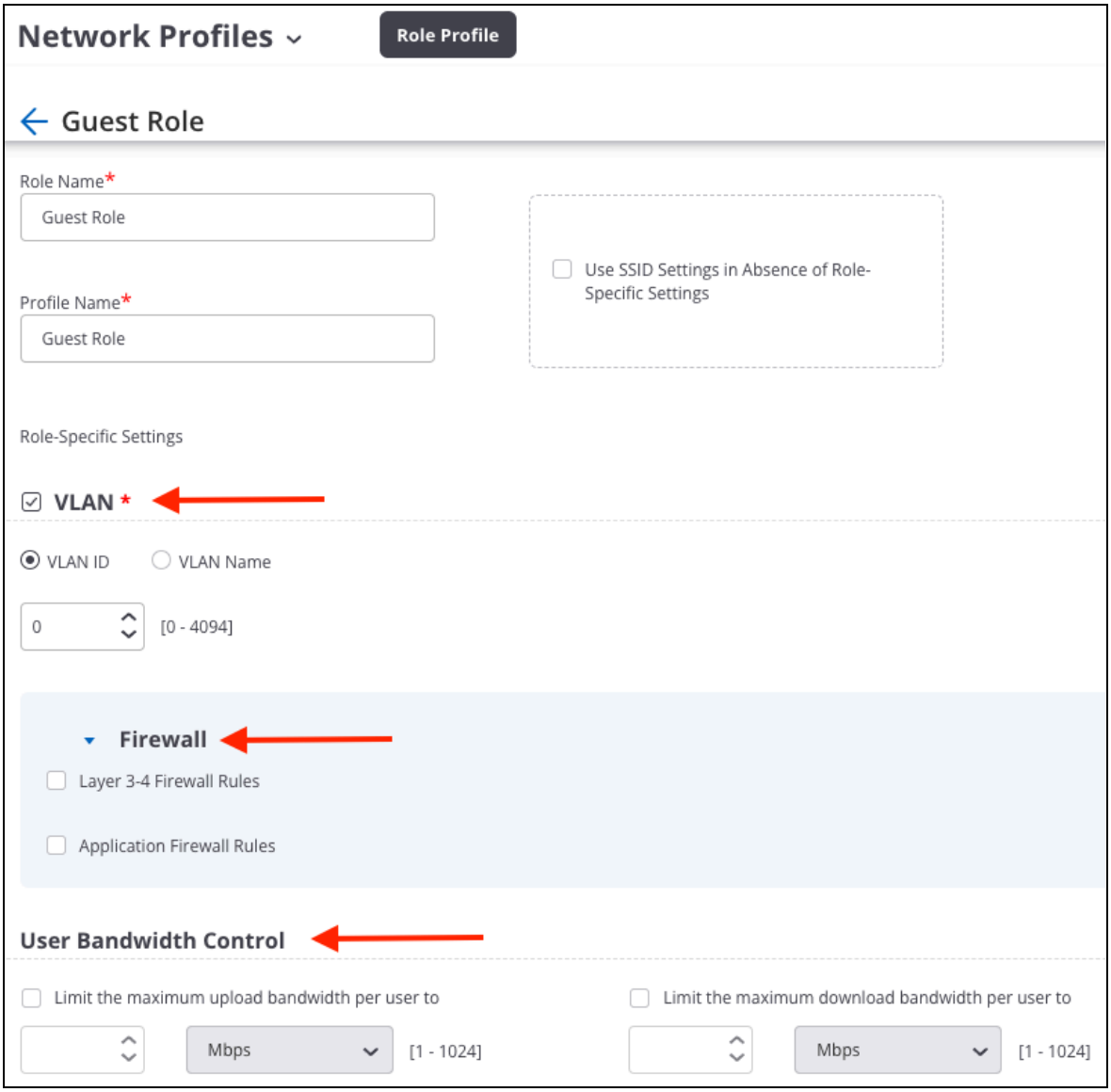
Next, we'll configure a Guest Role in CV-CUE to assign to Guest Users post authentication.

In CV-CUE, navigate to **Configure > Network Profiles > Role Profile**.

Add Role Profile.

Add the Role Name as **Guest Role**.

Select the check box next to **VLAN.**



Additional Information

VLAN

In this lab the VLAN is set to 0. In production networks you would define the Guest VLAN ID or Name that you want to assign to the Guest Users.

Firewall

Layer 3-4 and Application Firewall Rules can be assigned to the Guest User Role.

User Bandwidth Control

Upload and Download Bandwidth Limits can be assigned to the Guest User Role.

Click **SAVE** at the bottom of the page.

*****Configure AGNI Wireless-Guest-CP Segment**

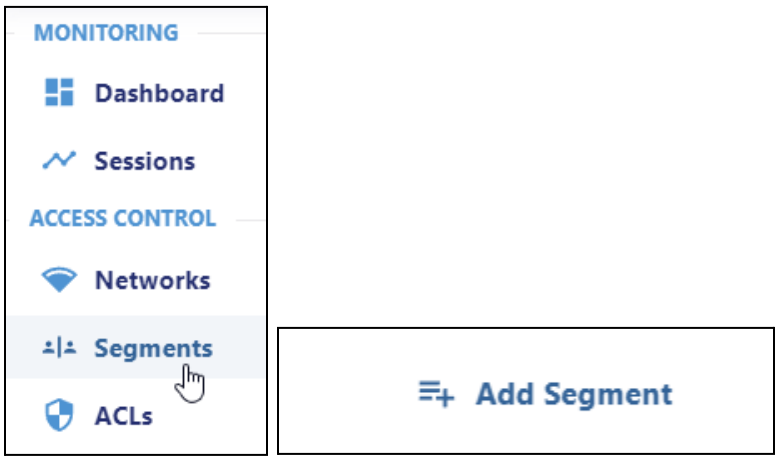
Next, we'll configure a Segment in AGNI to assign the Guest Role Profile post authentication.

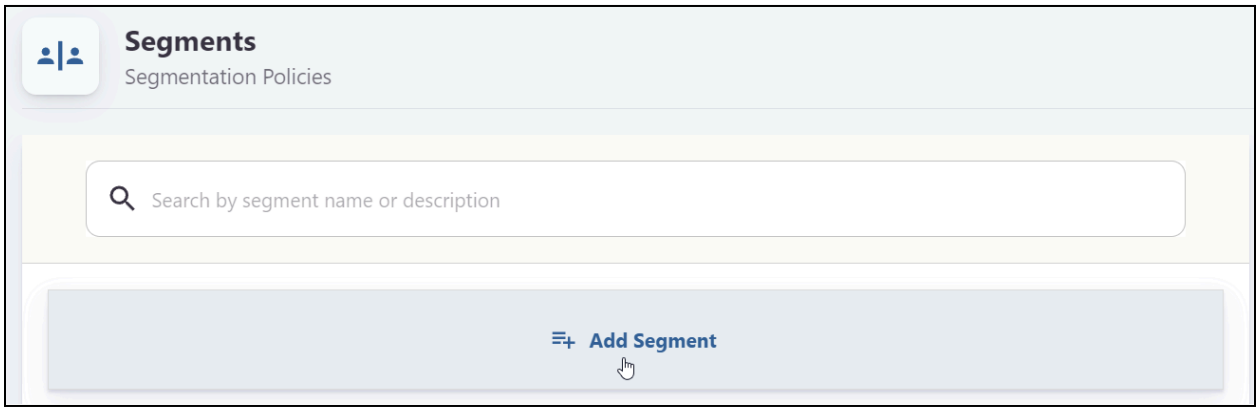
Go back to AGNI and navigate to the **Access Control > Segments.**

Add a new Segment with following settings:

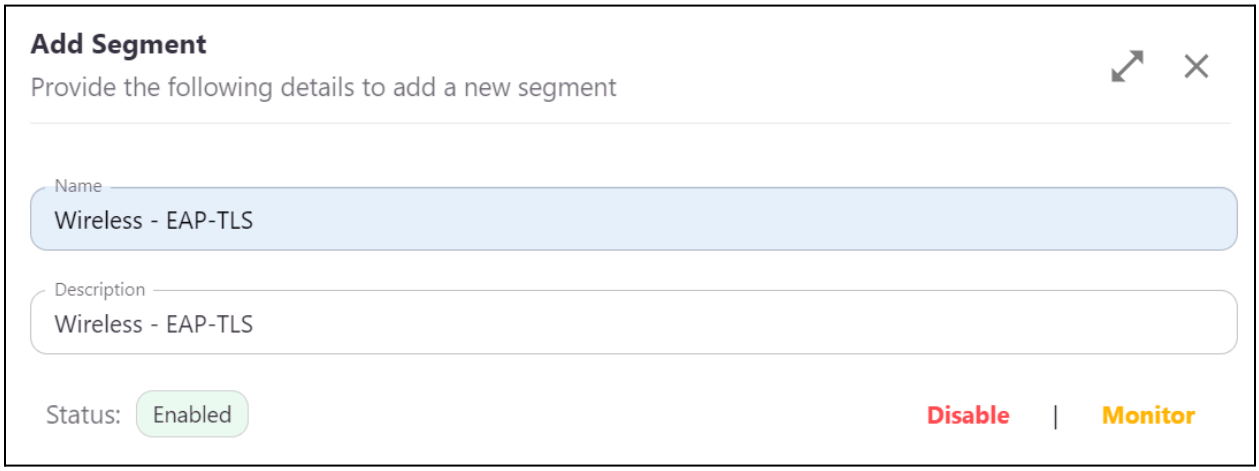
Name - **Wireless-Guest-CP**
Conditions - **Network Name is Wireless-Guest-CP**
Actions - **Arista-WiFi - Role Profile - Guest Role**

Click on **Segments** and then **+ Add Segment**





Next, type in the name: **Wireless-Guest-CP.**

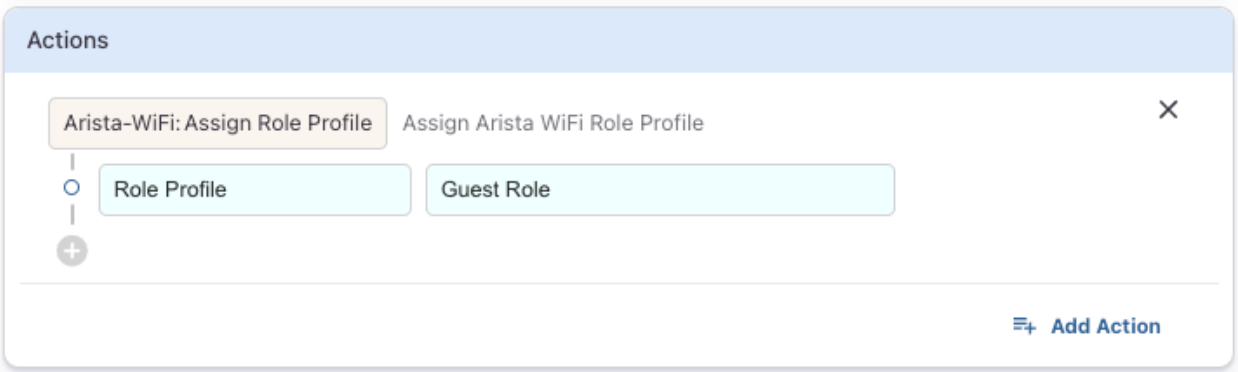


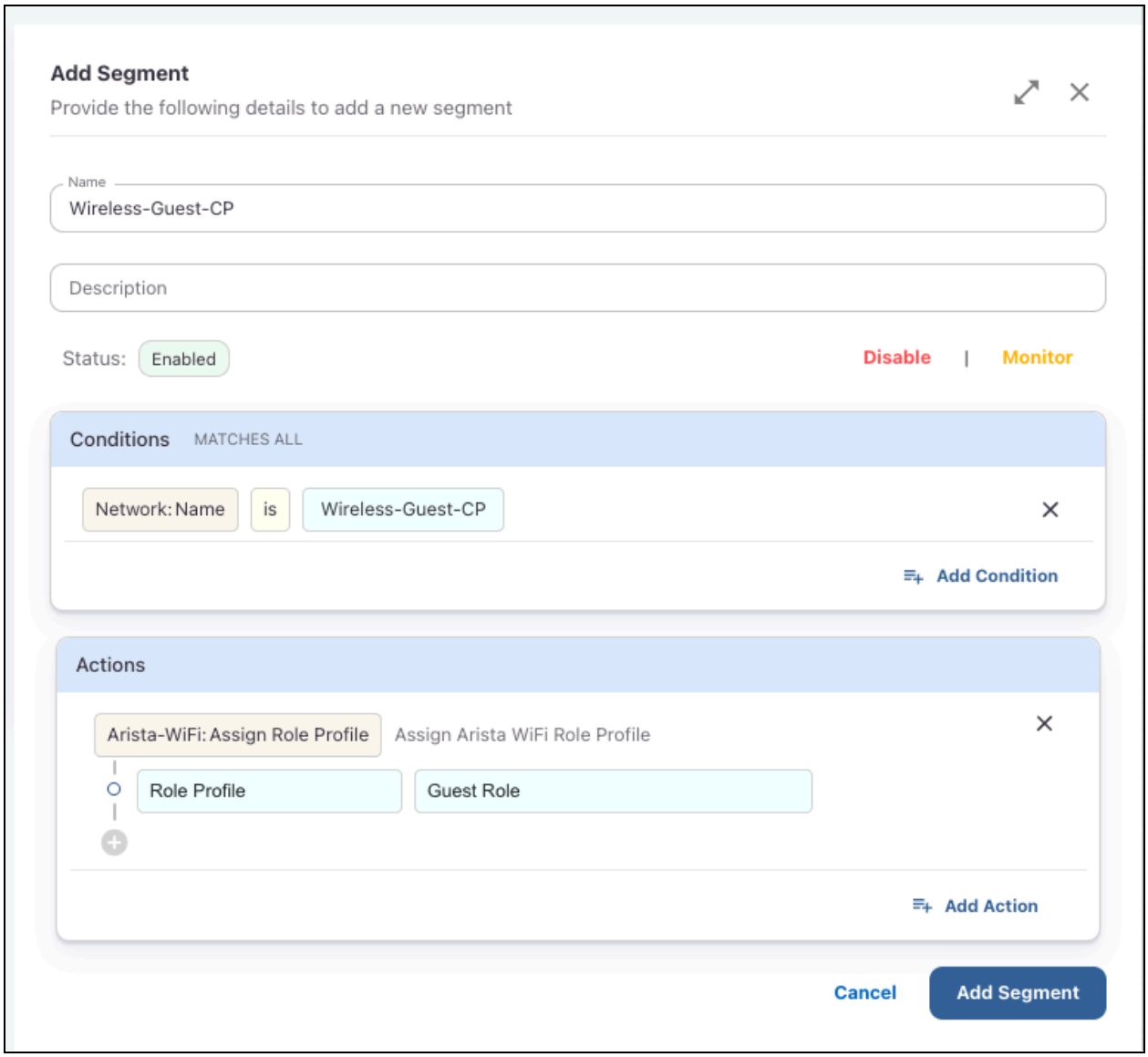
Next, let's **Add Conditions**. ***Note:** Adding more than one condition means MATCH ALL

Select, **Network, Name, Is, Wireless-Guest-CP** from the drop down lists.

Your Conditions should now look like this.

Under Actions select **Add Action**.
Select, **Arista-WiFi - Role Profile - Guest Role**





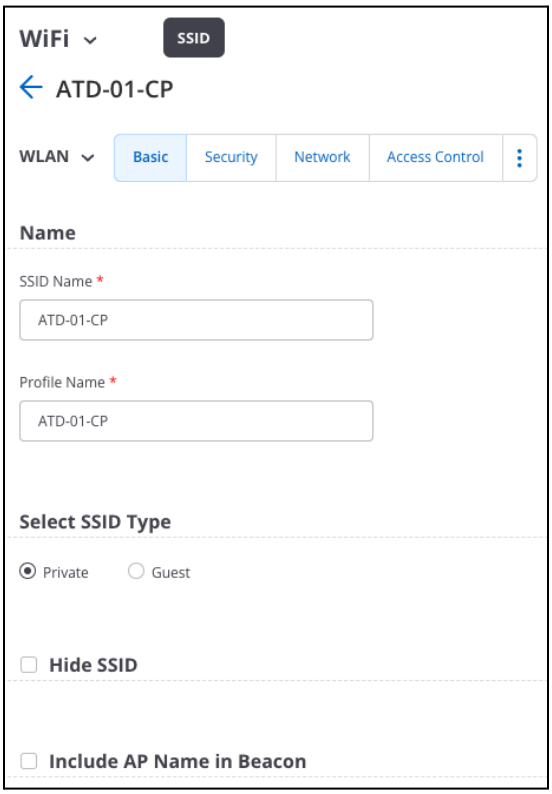
Finally, select **Add Segment** at the bottom of the page.

Configuring the Guest Captive Portal SSID

Next we'll configure the Guest Captive Portal SSID and assign the pre and post authentication roles.

Navigate to **Configure > WiFi**

Add SSID
SSID Name: **ATD-##-CP**
SSID Type: **Private**



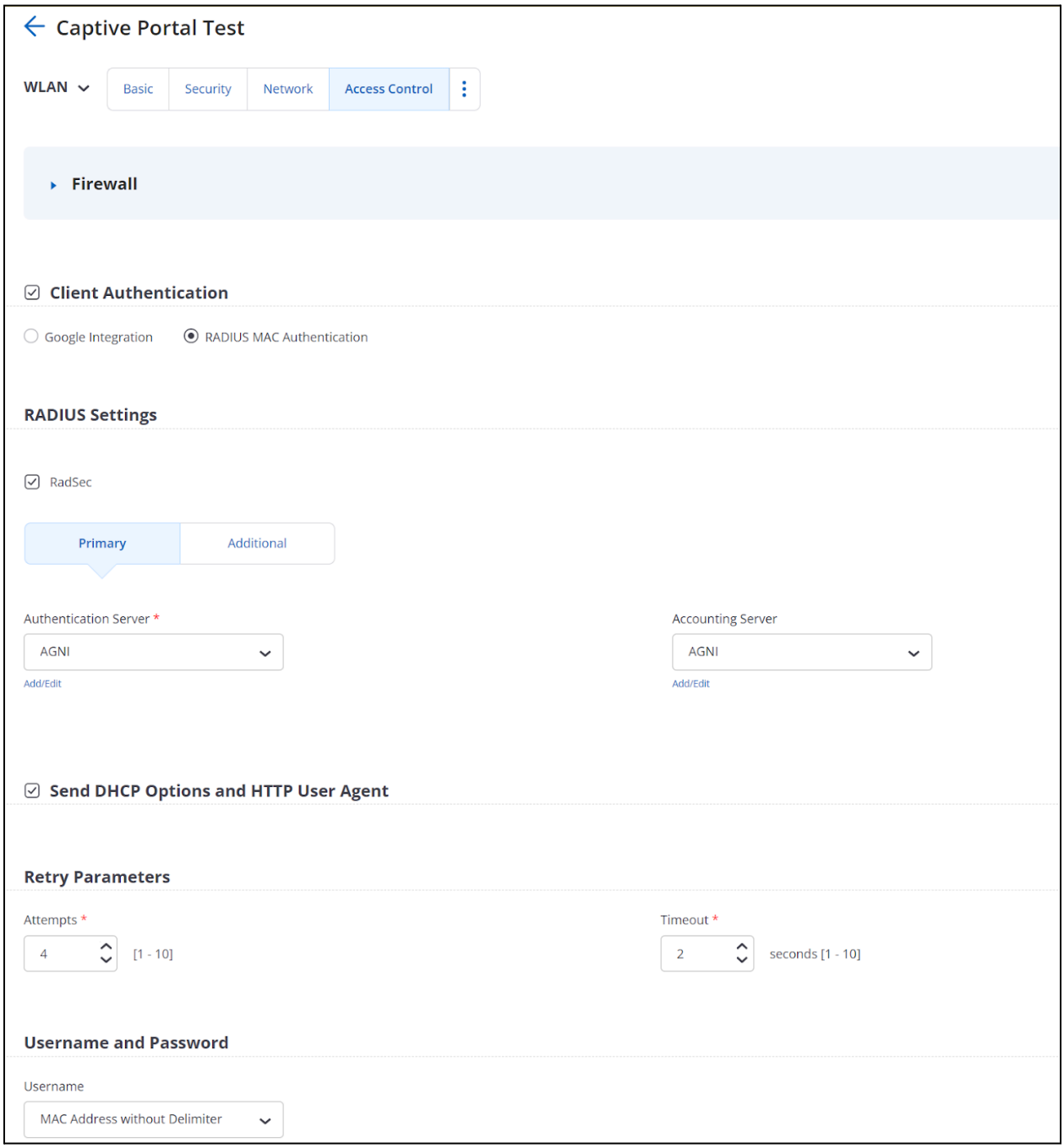
Click the **Access Control** tab.

Enable the **Client Authentication** check box and select **RADIUS MAC Authentication.**

Select **RadSec**

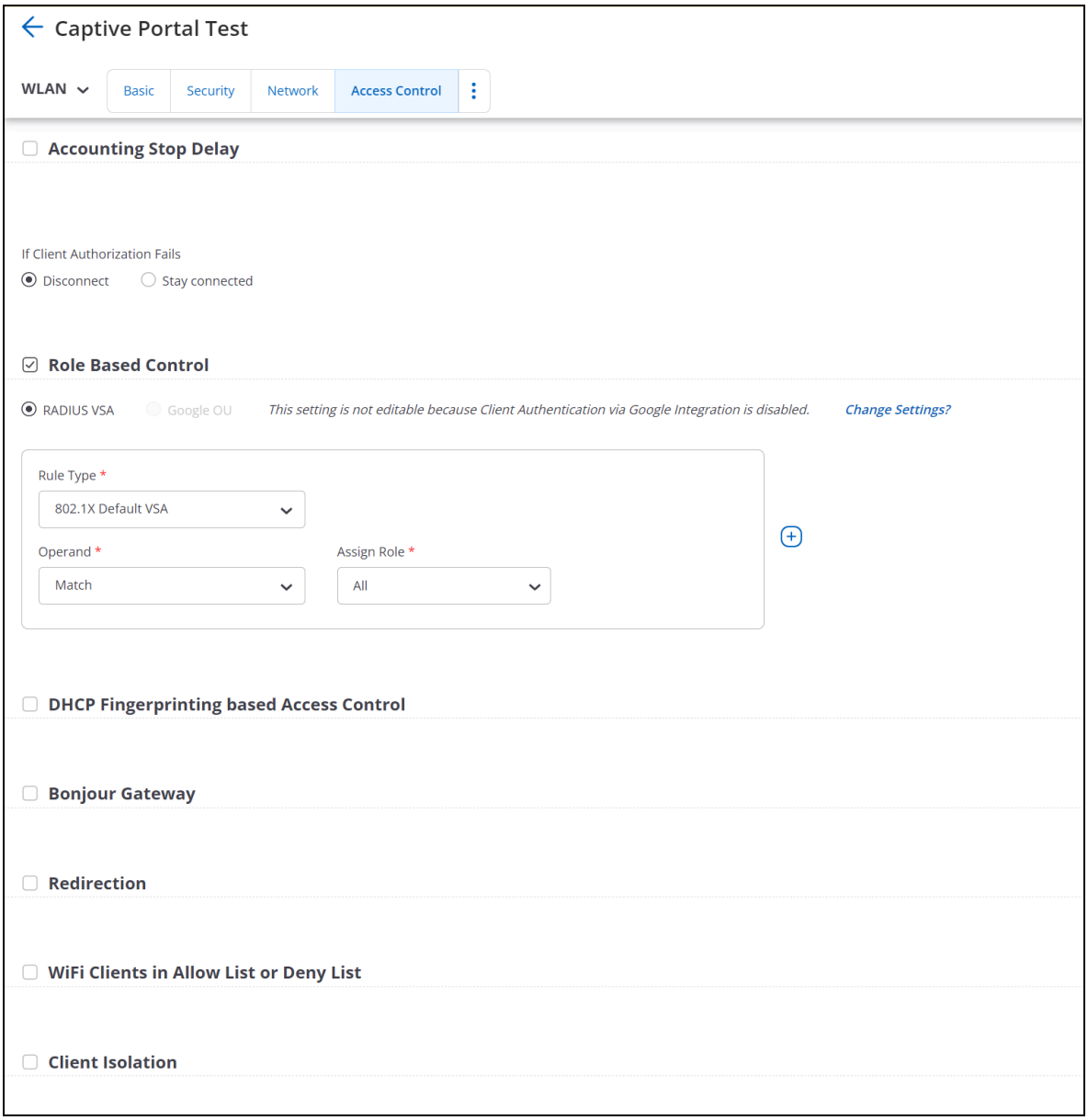
Authentication Server - **AGNI**
Accounting Server - **AGNI**

Select **AGNI** for the **Authentication** and **Accounting** servers, and select the check box next to **Send DHCP Options and HTTP User Agent.**



Select the **Role Based Control** checkbox and configure the following settings:

Rule Type — 802.1X Default VSA
Operand — Match
Assign Role — Select All. You created the Portal and Guest Roles profile in the previous section.



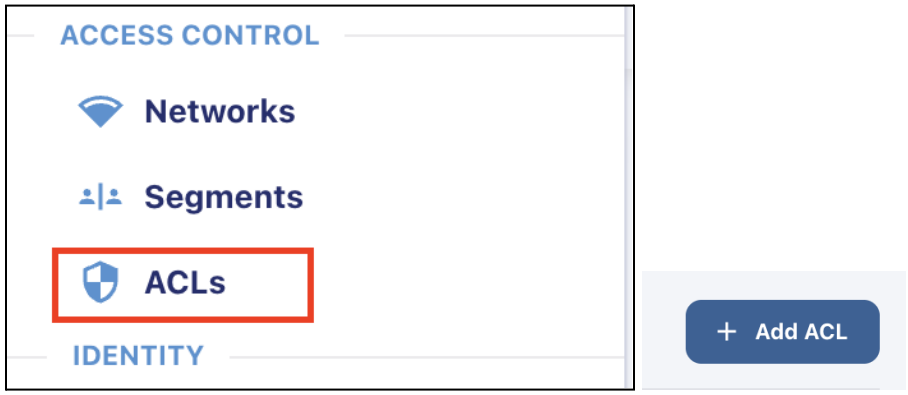
Save & Turn SSID On.

Once you are done, connect your phone to this SSID and select **Connect** from the Captive Portal page. The clients get connected and authenticated via the portal authentication.

D. Adding Access Control Lists

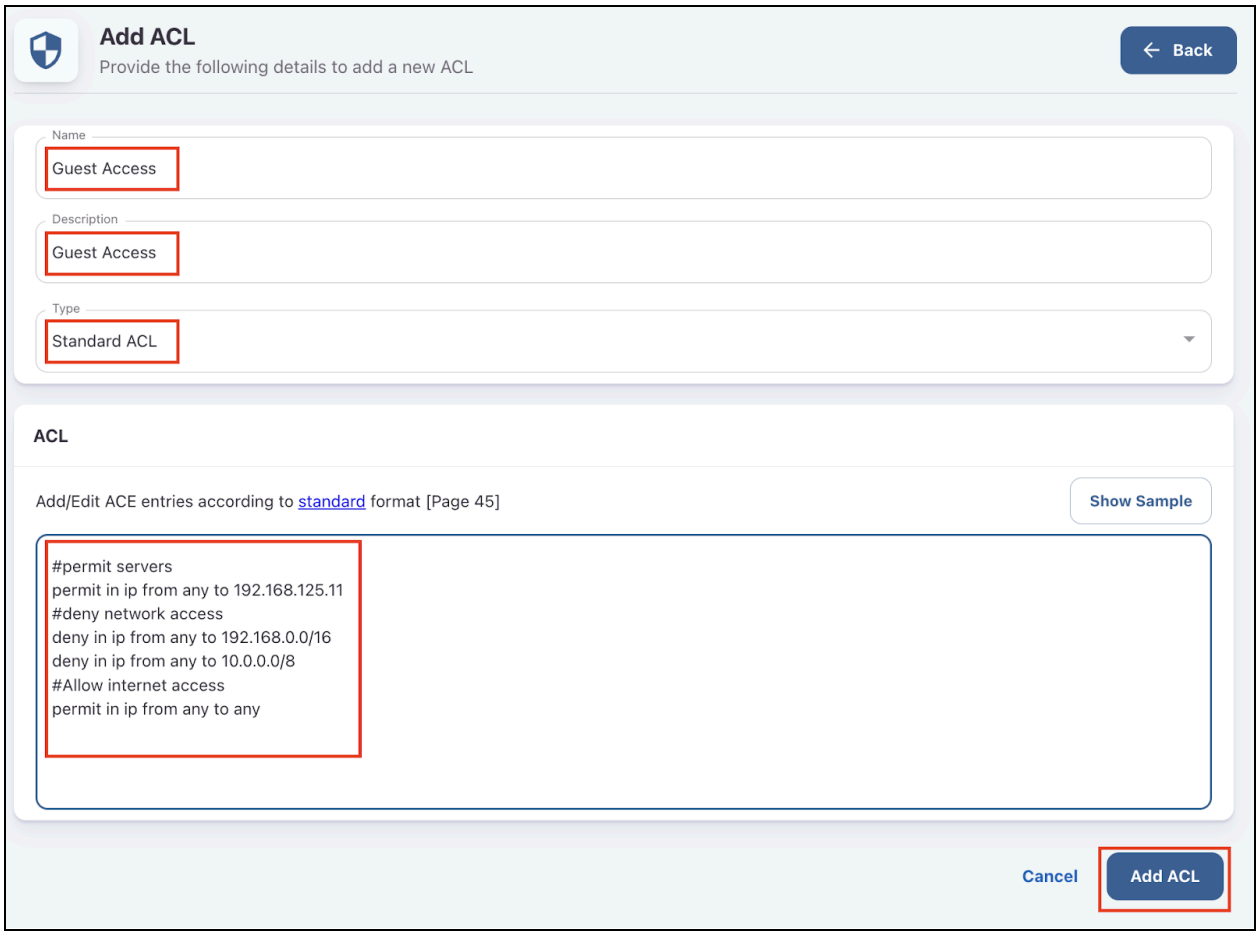
In this section we will add an acl to AGNI which we can push to the switch.

First navigate to **Access Control - > ACLs** and **+ Add ACL** in the upper right corner

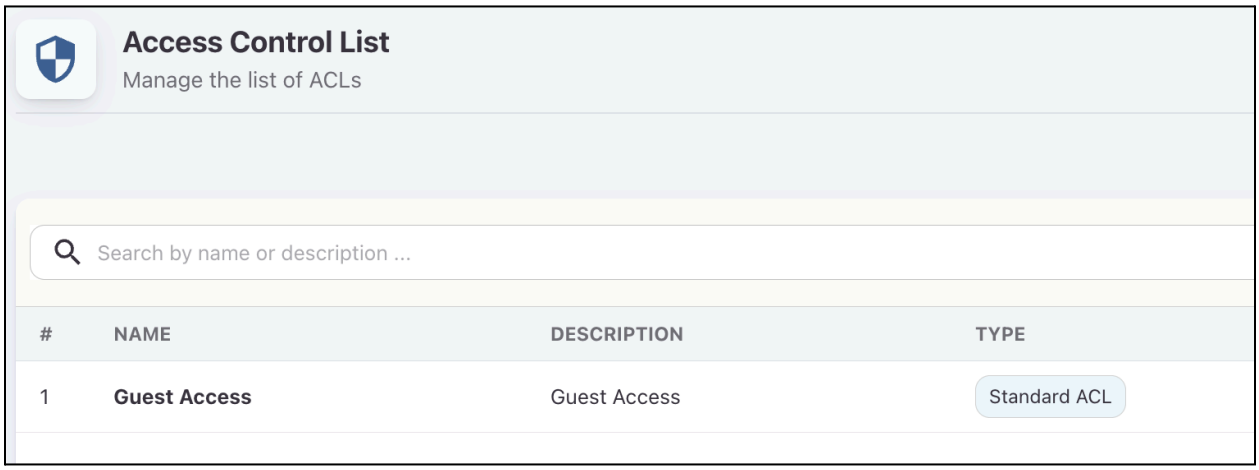


Next fill in the **Name** and **Description** fields with **Guest Access** and ACL Field with the below config then select **Add ACL**

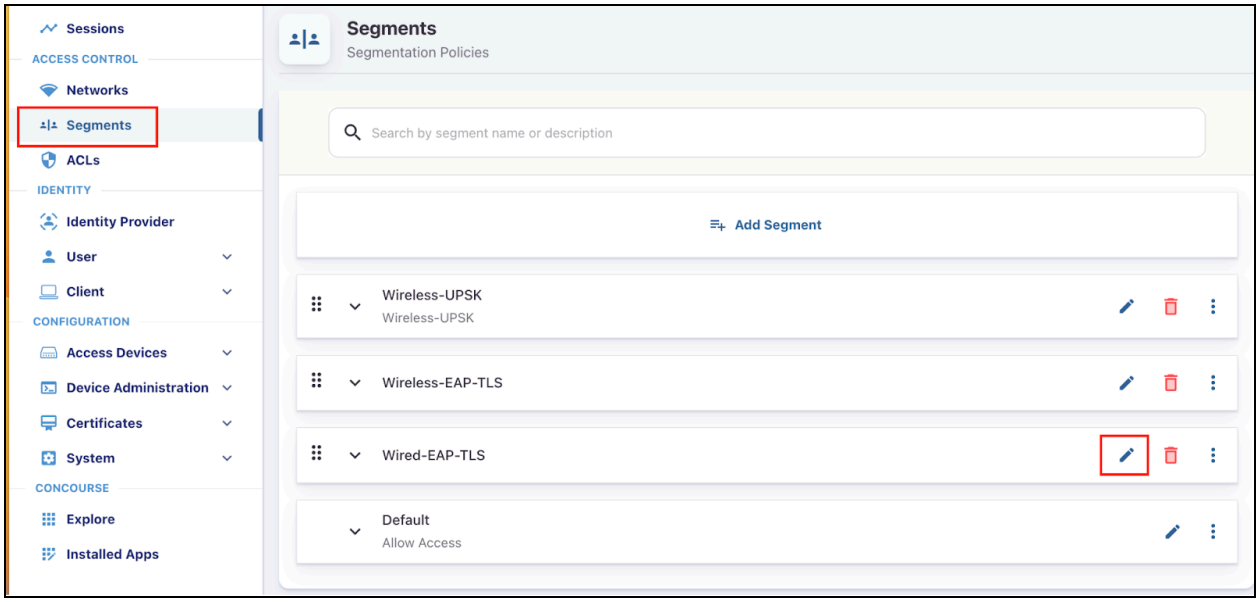
```
#permit servers
permit in ip from any to 192.168.125.11
#deny network access
deny in ip from any to 192.168.0.0/16
deny in ip from any to 10.0.0.0/8
#Allow internet access
permit in ip from any to any
```



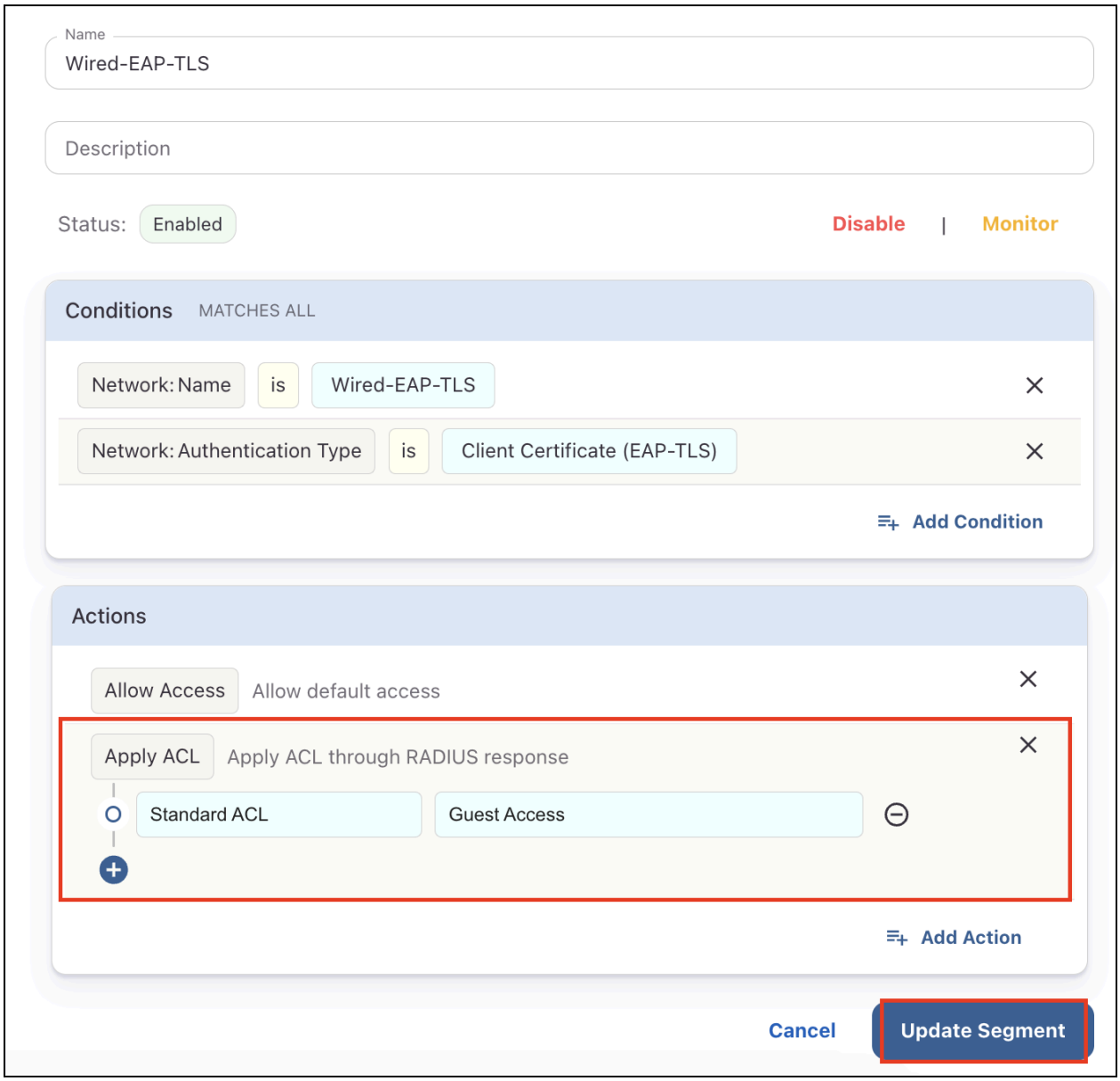
It should now show in the Access Control list



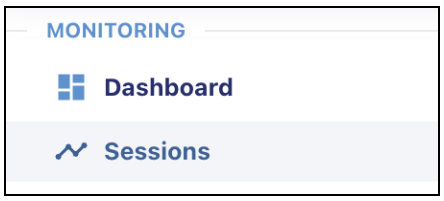
Next we will apply it to a Segment. Navigate to **Segments**, then select edit on the **Wired-EAP-TLS** segment

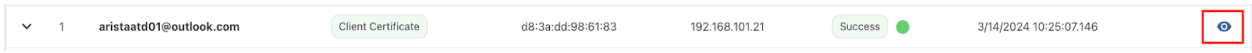


Next under the actions section Select **Add Action** and choose **Apply ACL** from the drop down list then choose **Standard ACL** and **Guest Access** to build out the Action. When Complete it should look as below. You can then select "**Update Segment**"

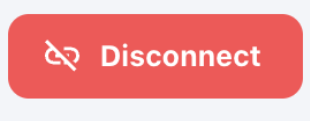


From here navigate back to the **Sessions** screen and find the client session for the raspberry pi select the **eye** on the right hand side to view details.

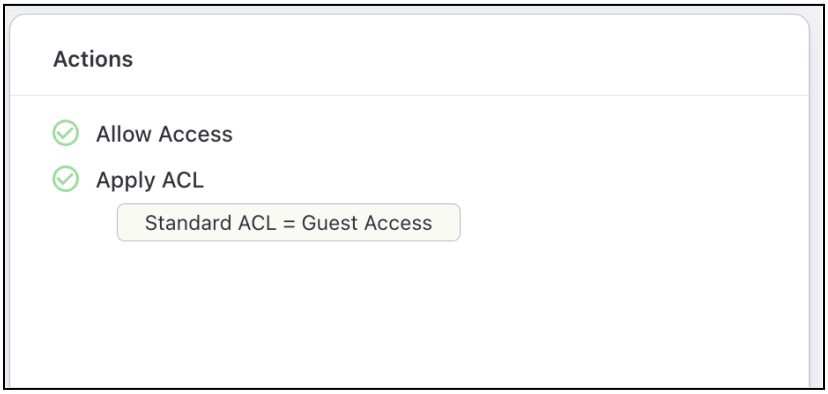




At the top of the session details page select the **Disconnect** button to disconnect and re-authenticate the session.



Next you will then see a new session come up as the client re-authenticates you can validate the acl being applied by selecting the **Eye** next to this new session and viewing the details



Next we can validate on the switch by issuing **Show dot1x host** command

```
710P-16P# sh dot1x host
Port      Supplicant MAC Auth  State                 Fallback              VLAN
--------- -------------- ----- --------------------- --------------------- ----
Et2       d83a.dd98.6183 EAPOL SUCCESS               NONE
```

Take this mac address and issue the command **show dot1x host mac <mac from above> detail** here we will see the Access list applied in the Nas-Filter-Rule

```
710P-16P# sh dot1x host mac  d83a.dd98.6183 detail
Operational:
Supplicant MAC: d83a.dd98.6183
User name: aristaatd01@outlook.com
Interface: Ethernet2
Authentication method: EAPOL
Supplicant state: SUCCESS
Fallback applied: NONE
Calling-Station-Id: D8-3A-DD-98-61-83
Reauthentication behaviour: DO-NOT-RE-AUTH
Reauthentication interval: 0 seconds
VLAN ID:
Accounting-Session-Id: 1x00000007
Captive portal:

AAA Server Returned:
Arista-WebAuth:
Class: Rcnpghgo78m8s712rvjbg|C4151a596-baab-444b-a4fd-ad40946d8b5f
Filter-Id:
Framed-IP-Address: 192.168.101.21 sourceArp
NAS-Filter-Rule: permit in ip from any to 192.168.2.1
                 deny in ip from any to 192.168.0.0/19
                 permit in ip from any to any
Service-Type: None
Session-Timeout: 86400 seconds
Termination-Action: RADIUS-REQUEST
Tunnel-Private-GroupId:
Arista-PeriodicIdentity:
```

Lastly issue the **show ip access-lists** command to view the dynamic access list applied

```
710P-16P#sh ip access-lists
IP Access List 802.1x-5877942182543360 [dynamic]
        10 permit ip any host 192.168.2.1
        20 deny ip any 192.168.0.0/19 [match 312 bytes in 4 packets, 0:00:22 ago]
        30 permit ip any any
```

You can try pinging the device ip from your laptop to confirm acl functionality.

This completes the Access Control List lab.