

Campus C-01 AGNI Lab Guide

EAP-TLS Wireless Policy



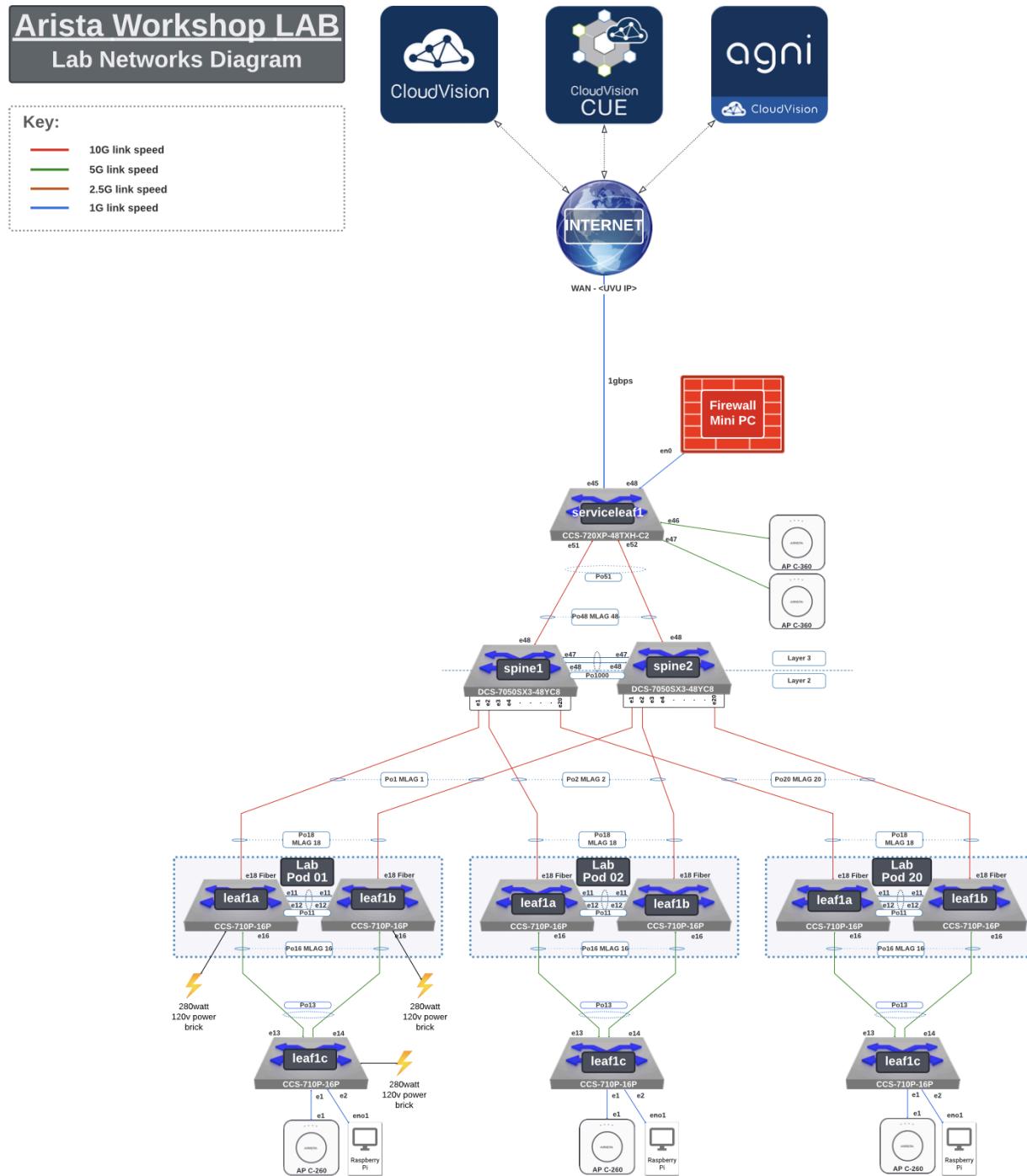
This Lab Guide:

<https://github.com/arista-rockies/Workshops/tree/main/Campus>

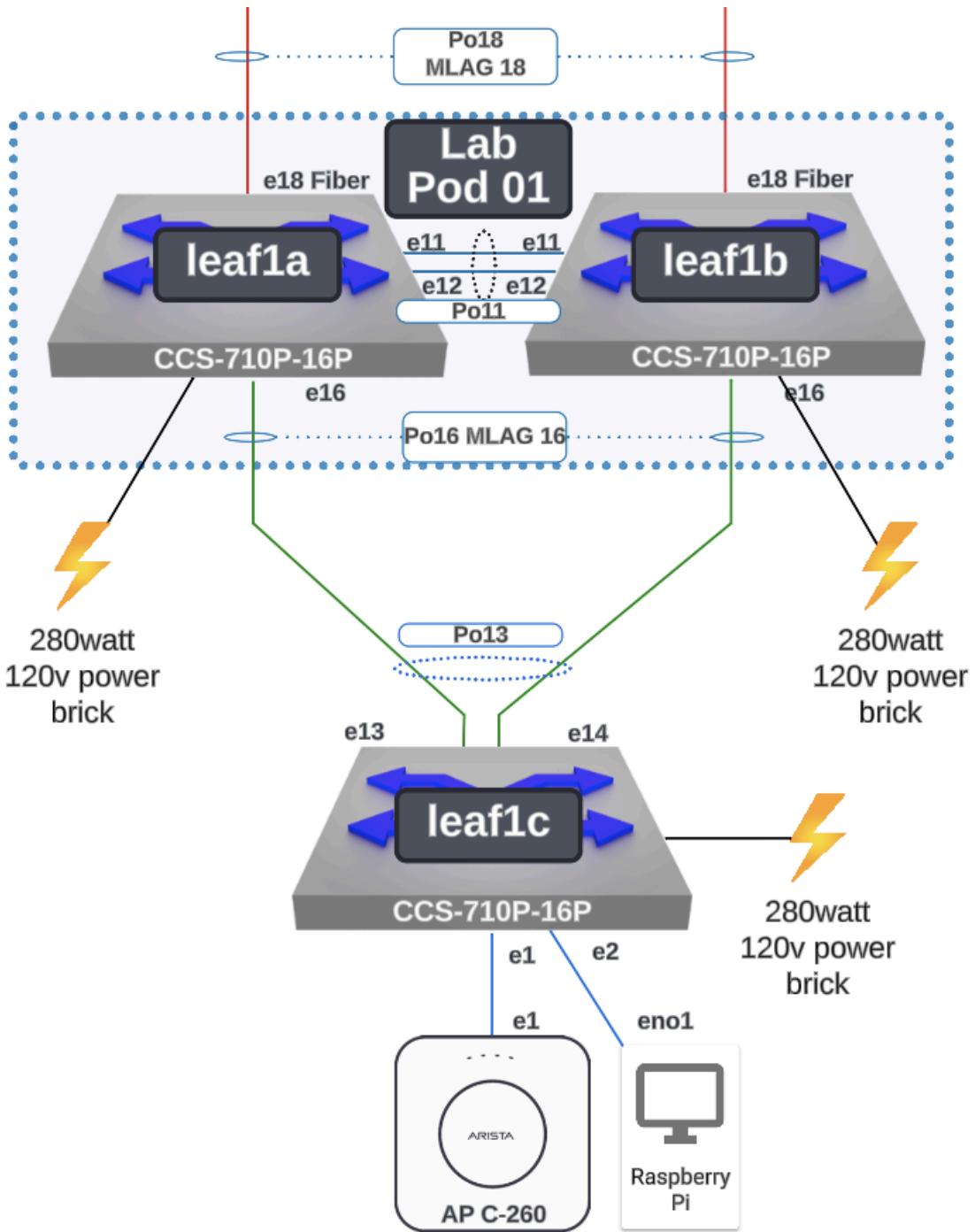
Table of Contents

Full Lab Topology.....	2
POD Topology.....	3
NAC Lab #1 - Create EAP-TLS Wireless Policy.....	4
1. CloudVision Cognitive Unified Edge CV-CUE Access.....	4
2. Create an EAP-TLS SSID.....	6
3. CloudVision AGNI Access.....	11
4. Create AGNI Networks & Segments for the EAP-TLS Wireless Policy.....	12
Additional Information.....	19
A. Setting up RadSec with a TPM AP Certificate.....	19
B. Setting up RadSec with a Custom AP Certificate.....	23
C. Create an AGNI Guest Captive Portal.....	28

Full Lab Topology



POD Topology



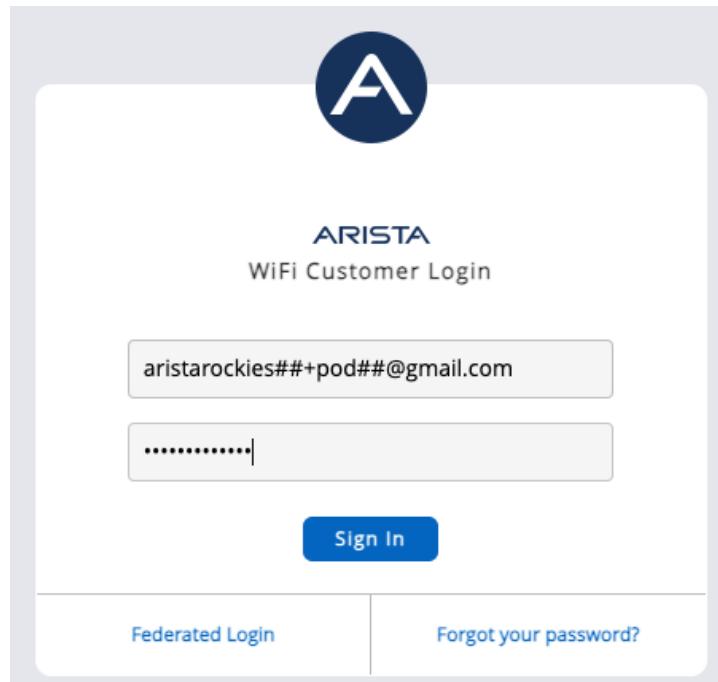
NAC Lab #1 - Create EAP-TLS Wireless Policy

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]*

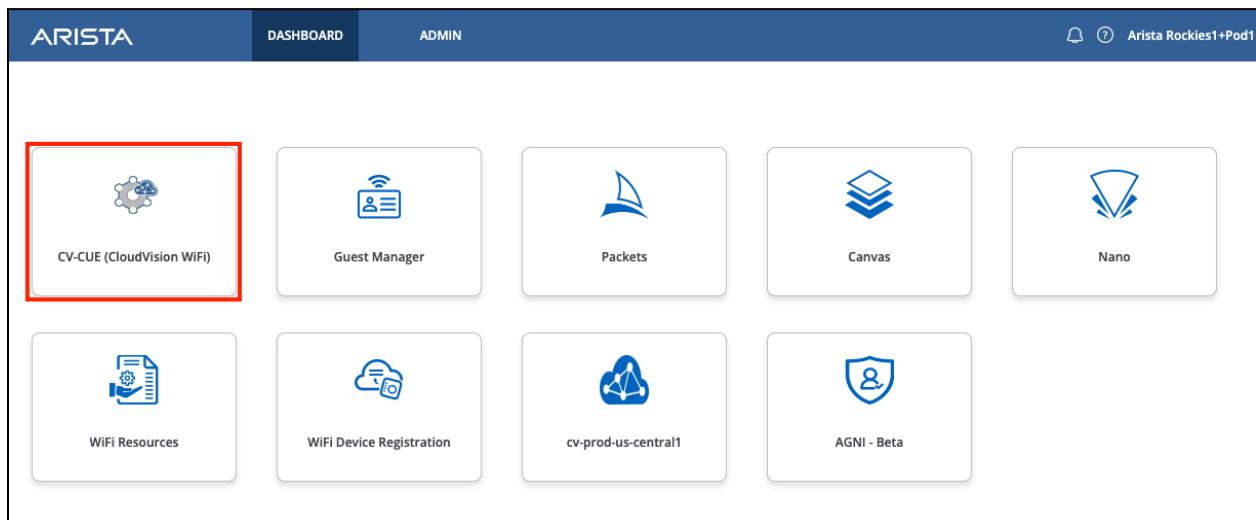


Click **Sign In**

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”.

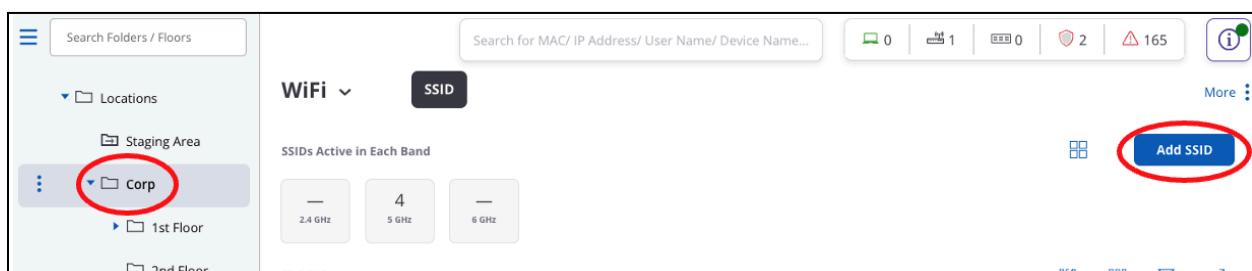


At the top of the screen, you will see where you are in the location hierarchy. If you aren't on “Corp”, click on the three lines (hamburger icon) next to “Locations” to expand the hierarchy and choose/highlight the “Corp” folder. Now click the “Add SSID” button on the right hand side of the screen.

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.).

SSID Name

WLAN Basic Security Network :

Name

SSID Name *

Enter SSID Name

Profile Name *

Enter Profile Name

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.

Name

SSID Name *

ATD-01-EAP

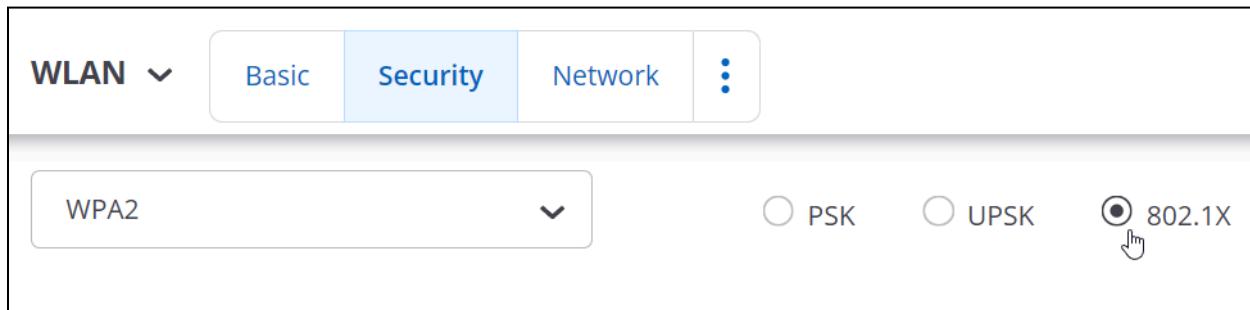
Profile Name *

ATD-01-EAP

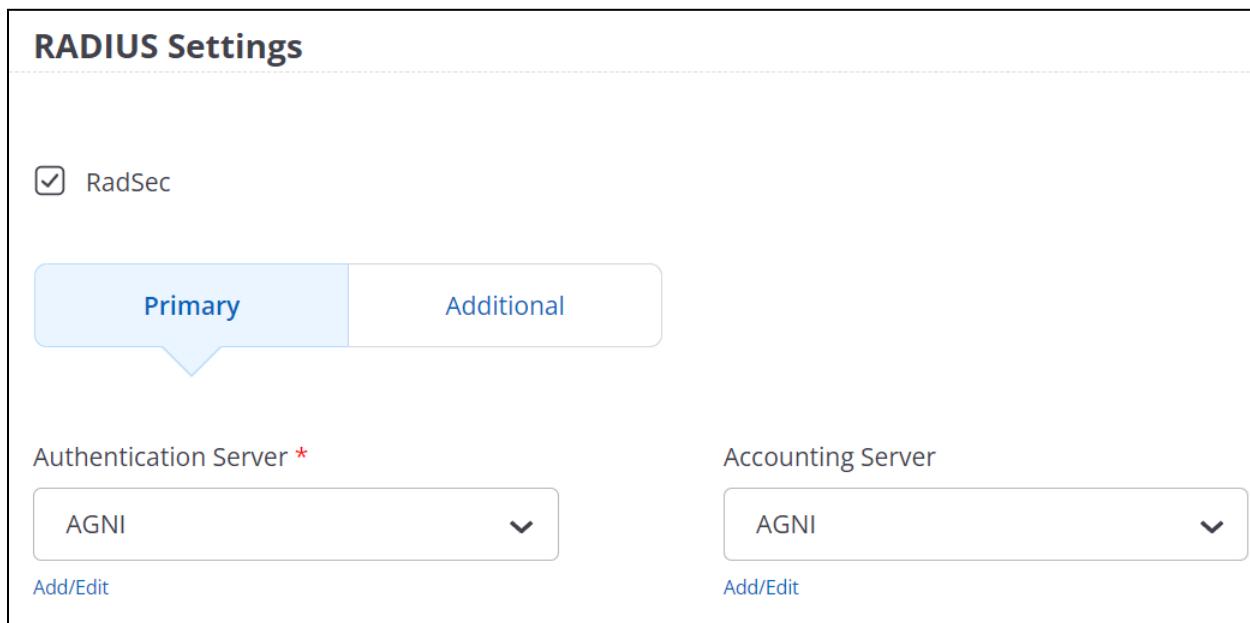
Since this is our corporate SSID, leave the “**Select SSID Type**” set to “**Private**”, but note this is where you would change it to “**Guest**” if needed. Select **Next** at the bottom.



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 A](#) 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.

← ATD-01-EAP



VLAN *

VLAN ID VLAN Name

0 [0 - 4094]

Network Mode

Bridged NAT L2 Tunnel L3 Tunnel

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).

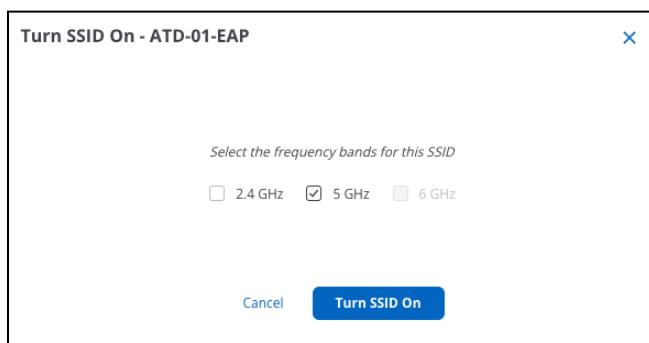
The rest of the settings can be left at the default values.

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

Save & Turn SSID On

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.

A screenshot of the WiFi Radios page. At the top, there are tabs for WiFi (selected), Clients, Access Points, Radios (which is highlighted in black), Active SSIDs, Application Visibility, and Tunnels. Below this, it says "2 Radios" and shows a "Radio Explorer" button. The main table lists two access points: "POD-01-FL1" (Status: up) and "POD-01-FL1" (Status: down). The columns in the table are: Status, Access Point Name, AP MAC Address, IP Address, Channel, Client Count, Tx. Power (dBm), and Frequency. The 5 GHz radio is listed as "up" and the 2.4 GHz radio is listed as "down".

Status	Access Point Name	AP MAC Address	IP Address	Channel	Client Count	Tx. Power (dBm)	Frequency
up	POD-01-FL1	30:86:2D:30:4...	10.0.101.109	44	0	--	5 GHz
down	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?

A screenshot of the WiFi Active SSIDs page. At the top, there are tabs for WiFi (selected), Clients, Access Points, Radios, Active SSIDs (which is highlighted in black), Application Visibility, and Tunnels. Below this, it says "1 Active SSIDs" and shows a "Search for MAC/ IP Address/ User" input field. The main table lists the active SSID: "ATD-01-EAP". The columns in the table are: SSID, Security, Authentication, and 5 GHz Radios. The table shows WPA2 security, EAP authentication, and 1 5 GHz radio.

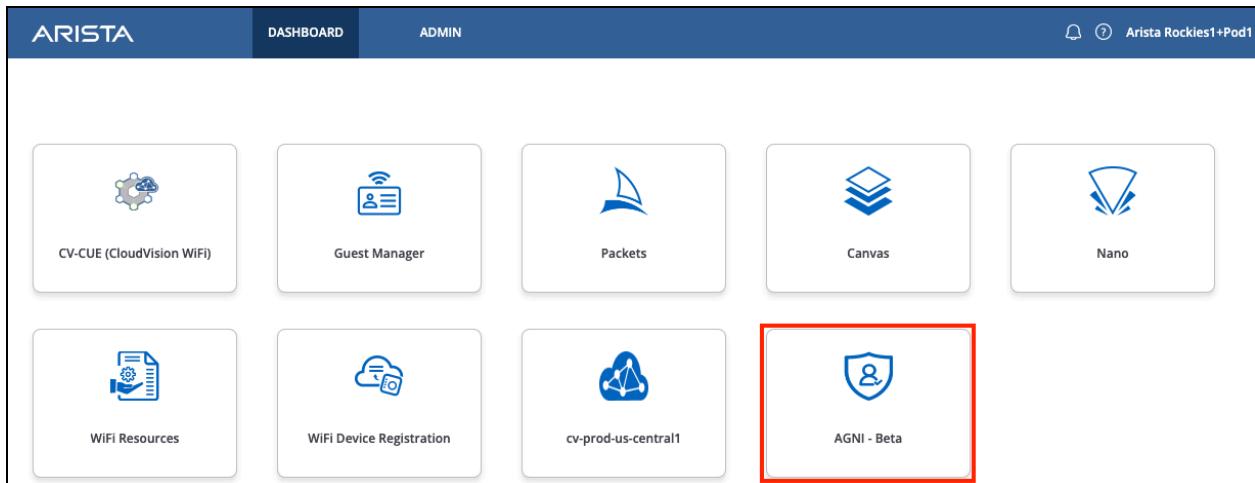
SSID	Security	Authentication	5 GHz Radios
ATD-01-EAP	WPA2	EAP	1

3. CloudVision AGNI Access

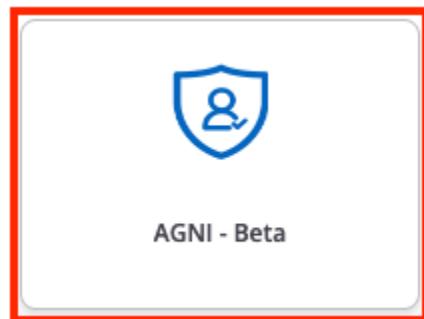
Launchpad

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

Dashboard tab:

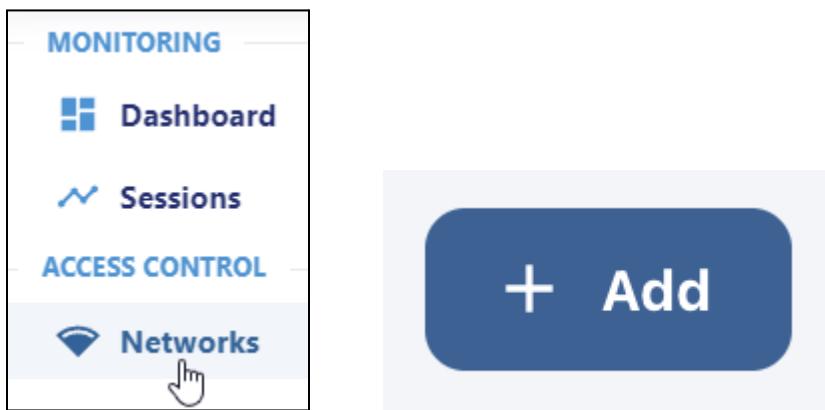


Select AGNI - Beta.



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

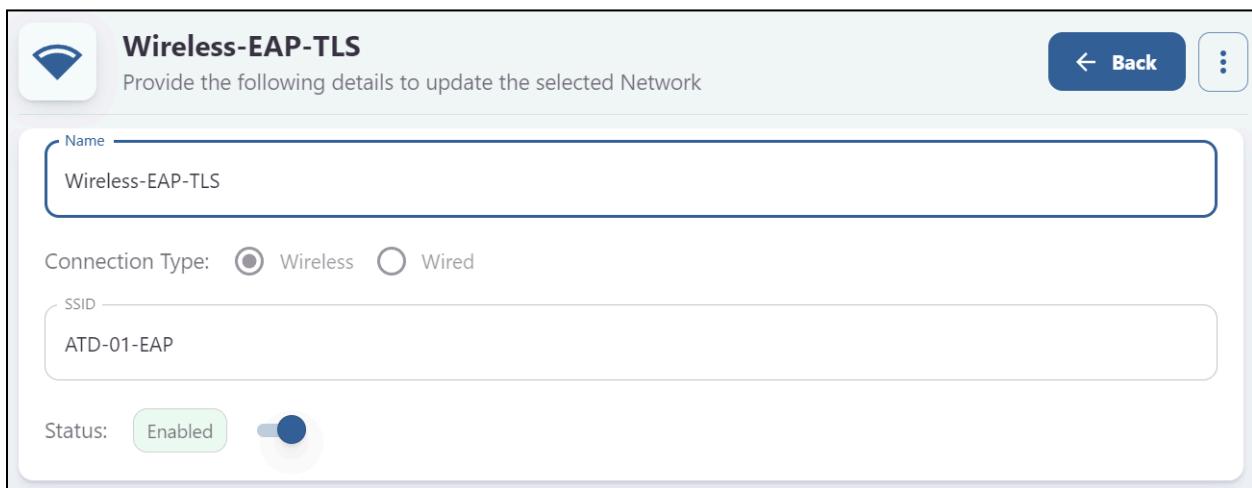
Click on **Networks** and select **+ Add**



Type in the name **Wireless-EAP-TLS**

Select Connection Type: **Wireless**

SSID needs to match what you created in CV-CUE type **ATD-##-EAP**



Wireless-EAP-TLS
Provide the following details to update the selected Network

Name: Wireless-EAP-TLS

Connection Type: Wireless Wired

SSID: ATD-01-EAP

Status: Enabled

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

Authentication

Authentication Type: Client Certificate (EAP-TLS)

Domain Machine Authentication: Disabled

i Enable to allow machine authentication with domain machine certificates.

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



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

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

 - Networks
 - Segments (selected)
 - ACLs

Segments
Segmentation Policies

■ Search by segment name or description

■ **+ Add Segment**

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

Add Segment

Provide the following details to add a new segment

Name: Wireless - EAP-TLS

Description: Wireless - EAP-TLS

Status: Enabled | **Disable** | **Monitor**

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

=+ Add Condition

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

Network: Name: **Wireless-EAP-TLS**

Let's add one more condition.

=+ Add Condition

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

Network: Authentication Type: **Client Certificate (EAP-TLS)**

Your Conditions should now look like this.

Conditions MATCHES ALL

Network: Name is Wireless-EAP-TLS X

Network: Authentication Type is Client Certificate (EAP-TLS) X

≡+ Add Condition

Under Actions select **Add Action**.

Actions

≡+ Add Action

Select Allow Access.

Actions

- Assign VLAN
- Apply ACL
- Allow Access** ✓
- Deny Access
- Arista-WiFi
- Radius

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

Add Segment

Provide the following details to add a new segment



Name

Wireless - EAP-TLS

Description

Wireless - EAP-TLS

Status: Enabled

Disable

Monitor

Conditions MATCHES ALL

Network: Name

is

Wireless-EAP-TLS



Network: Authentication Type

is

Client Certificate (EAP-TLS)



Add Condition

Actions

Allow Access

Allow default access



Add Action

Cancel

Add Segment



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

Segments
Segmentation Policies

Search by segment name or description

Add Segment

Wireless-EAP-TLS

Conditions

Network:Name is Wireless-EAP-TLS

Network:AuthType is Client Certificate (EAP-TLS)

Actions

Allow Access

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.

The screenshot displays a NAC interface with the following sections:

- Authentication Request:** Shows "Success" status. Fields include:
 - Authentication Type: Client Certificate (EAP-TLS) (highlighted by a red arrow)
 - Segment: Wireless-EAP-TLS (highlighted by a red arrow)
 - Location: Locations/AGNI
- User:** Aristaatd01@outlook.com, Arista, Enabled
- Client:** d8:3a:dd:9d:4c:e4, Arista's Mac OS X Wireless, Enabled
- Access Device:** 30:86:2d:4e:36:ff, C230_AP01, Arista WiFi, Enabled
- Network:** Wireless-EAP-TLS, ATD-01-EAP (highlighted by a red arrow), Client Certificate (EAP-TLS)
- Session Details:** Client IP Address, Session Start Time, Session Stop Time
- Actions:** Allow Access (checkbox checked, highlighted by a red arrow)

NAC LAB #1 COMPLETE

Additional Information

A. Setting up RadSec with a TPM AP Certificate

NOTE: The following example is for TPM Based AP's. The Arista's C-2xx (except the C-250/C-260), C-3xx, and C-4xx Series APs include a TPM chip.

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 CV-CUE and AGNI Tiles from the LaunchPad and they will open in a new Tab.



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

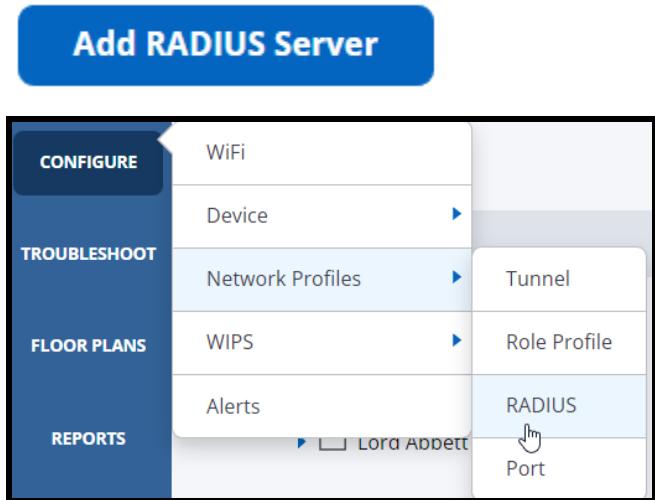
The screenshot shows the AGNI configuration interface. On the left, a sidebar lists various configuration sections: Access Devices, Certificates, System (selected), Audit Viewer, License, Portal Settings, RadSec Settings (selected), Support Logs, and System Events. The main panel is titled "RadSec Settings". It contains two main sections: "RadSec Server" and "RadSec CA Certificate". In the "RadSec Server" section, the "RadSec Server Hostname" is set to "radsec.beta.agni.arista.io". A note below it says, "Use the above server as RadSec(TLS) RADIUS server in your Network Access Devices." In the "RadSec CA Certificate" section, the "Subject DN" is listed as "CN=ISRG Root X1, O=Internet Security Research Group, C=US" and the "Issuer DN" is also "CN=ISRG Root X1, O=Internet Security Research Group, C=US". A note below it says, "Use this CA certificate to validate the RadSec(TLS) server certificate." At the bottom right of the main panel, there is a download icon.

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

This screenshot shows the detailed view of the RadSec CA Certificate. It displays the FQDN "radsec.beta.agni.arista.io" with a red arrow pointing to it. Below the FQDN, there is a note: "Use the above server as RadSec(TLS) RADIUS server in your Network Access Devices." The certificate details show it expires on "6/4/2035" and has a subject and issuer DN of "CN=ISRG Root X1, O=Internet Security Research Group, C=US". A note below states, "Use this CA certificate to validate the RadSec(TLS) server certificate." At the bottom, there is a download icon followed by the file name "certificate.pem" with another red arrow pointing to it.

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

Configure → Network Profiles → RADIUS → Add RADIUS Server



RADIUS Server Name*
Demo AGNI

IP Address/FQDN*
radsec.beta.agni.arista.io

RADSEC
 ON OFF

RADSEC Port*
2083 [1-65535]

certificate.pem

Certificate Tag*
DEFAULT_RSA

Save

Note: Once the Radius Profile is assigned to a SSID, the RadSec Connection will come up.

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		Green dot	7/5/2023 15:50:47

If the AP does not connect, issue a reboot.

For more information see the video below.

[RadSec Tunnel with TPM chip APs](#)



B. Setting up RadSec with a Custom AP Certificate

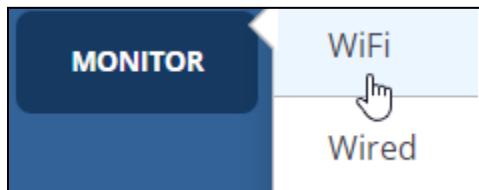
NOTE: The following example is for non-TPM Based AP's. The Arista C-250 and C-260 APs are non-TPM Based APs.

Click on the CV-CUE and AGNI Tiles from the LaunchPad and they will open in a new Tab.

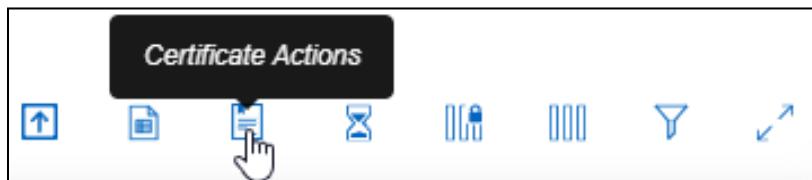


*Note: When applying the Certificate to the AP it is recommended to have both the CV-CUE and AGNI windows opened side by side.

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



On Right hand side on top and click on Certificate Actions



Generate CSR

The generate CSR will override any existing CSR for all access points under this location/group for the selected tag. Are you sure you want to continue?

Add New Certificate Tag Select Certificate Tag

AGNI1L2P

[Cancel](#) [Generate](#)

CSR generation initiated.

Generate CSR

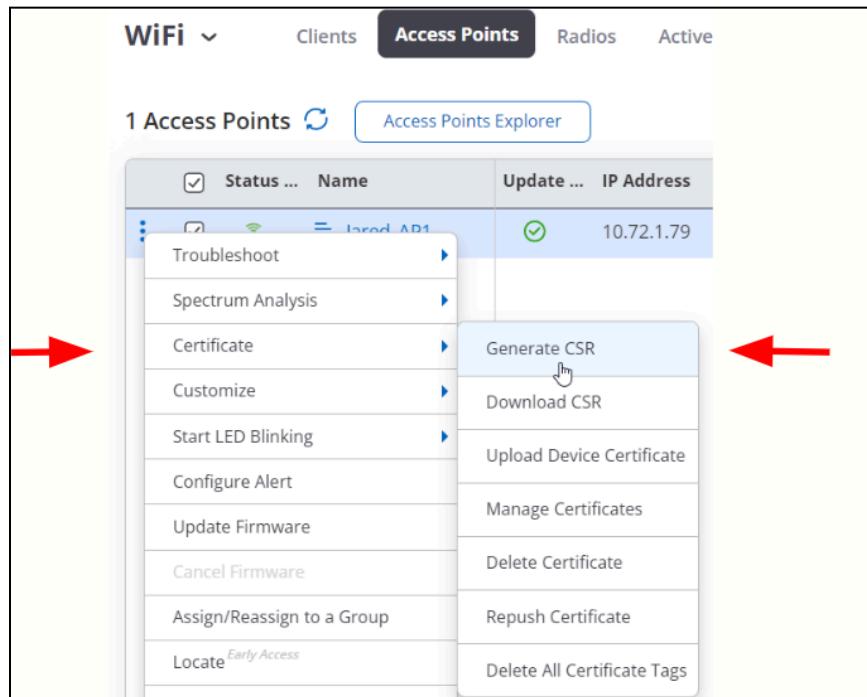
The generated CSR will override any existing CSR for the selected tag. Are you sure you want to continue?

AGNI1L2P

[Cancel](#) [Generate](#)

CSR generation initiated.

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.

The first screenshot shows a context menu for a selected AP (10.72.1.79) with options: Troubleshoot, Spectrum Analysis, Certificate, Customize, and Start LED Blinking. The 'Download CSR' option is highlighted with a mouse cursor. The second screenshot is a confirmation dialog titled 'Download CSR' asking 'Are you sure you want to download the CSR for the selected access points?' with a dropdown menu showing 'AGNI1L2P'. The third screenshot shows an 'Ongoing Activity' window with the message 'CSR is available for download.' and a blue 'Download' button.

Unzip the CSR File



AGNI - Click on Access Devices and Select the AP.

Access Devices → Devices → Select AP → Get Client Certificate

CONFIGURATION

- Access Devices**
- Devices** (Selected)
- Device Groups**

0235E_AGNI
Fill in the fields below to update the selected Device

Name: 0235E_AGNI

MAC Address: 30:86:2d:e0:8c:0f

Vendor: Arista WiFi

Access Device Group: Access Points

Optional

Location:

Optional, example: Global/America/California/Site-1

RadSec Connection Status: Connected

You can generate a RadSec client certificate for this Access Device.

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.

Get Client Certificate

Generate RadSec Client Certificate
Fill in the details to generate RadSec client certificate for the Access Device

Generate Certificate: Generate Use CSR (Single Device) Upload Zip with multiple CSRs

Access Device: W-318-AGNI

Select Action: Upload CSR File Paste CSR ←

Upload CSR File: E4.D1.24.10.EE.4F.csr

The file must be a PEM encoded PKCS10 certificate request.

←

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.

WiFi Clients Access Points Radios Active

1 Access Points ↻ Access Points Explorer

Status ...	Name	Update ...	IP Address
<input type="checkbox"/>	Lared AP1	<input type="checkbox"/>	10.72.1.79

Troubleshoot ►

Spectrum Analysis ►

Certificate ► ←

Customize ►

Start LED Blinking ►

Configure Alert

Update Firmware

Generate CSR

Download CSR

Upload Device Certificate ► ←

Manage Certificates

Upload Device Certificate

X

The upload device certificate will override any existing certificate for the selected tag. Are you sure you want to continue?

AGNI1L2P

Select File

0235E_AGNI.pem

Supported Formats: .crt, .pem, .zip

Cancel

Upload

Note: Once the Radius Profile is assigned to a SSID, the RadSec Connection will come up.

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.

For more details see the video below.

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

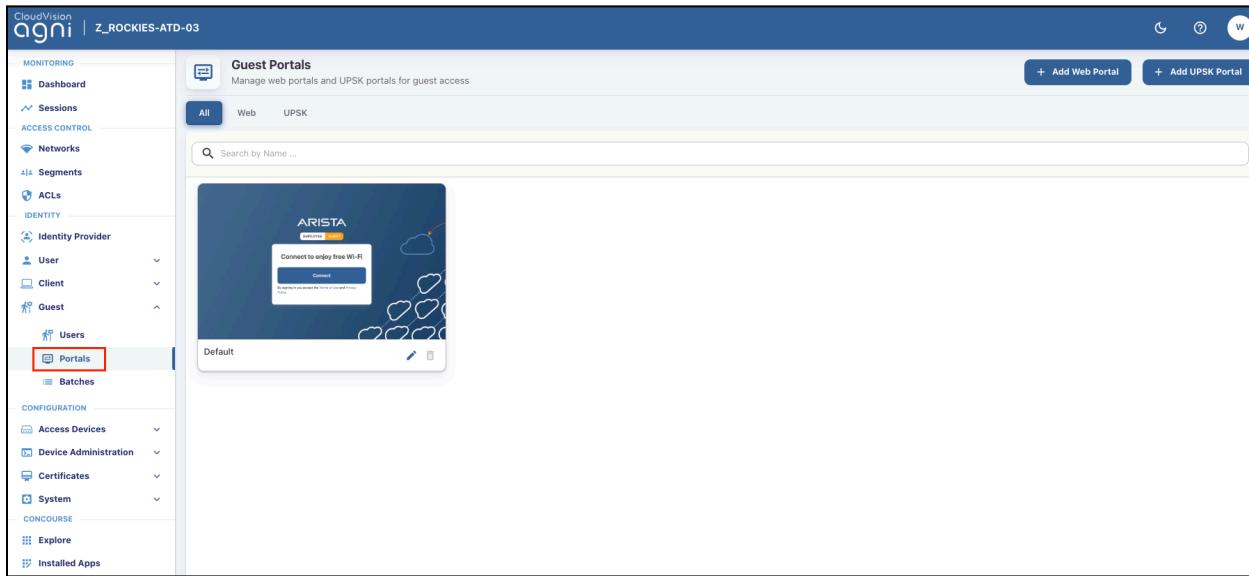


C. Create an AGNI Guest Captive Portal

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.

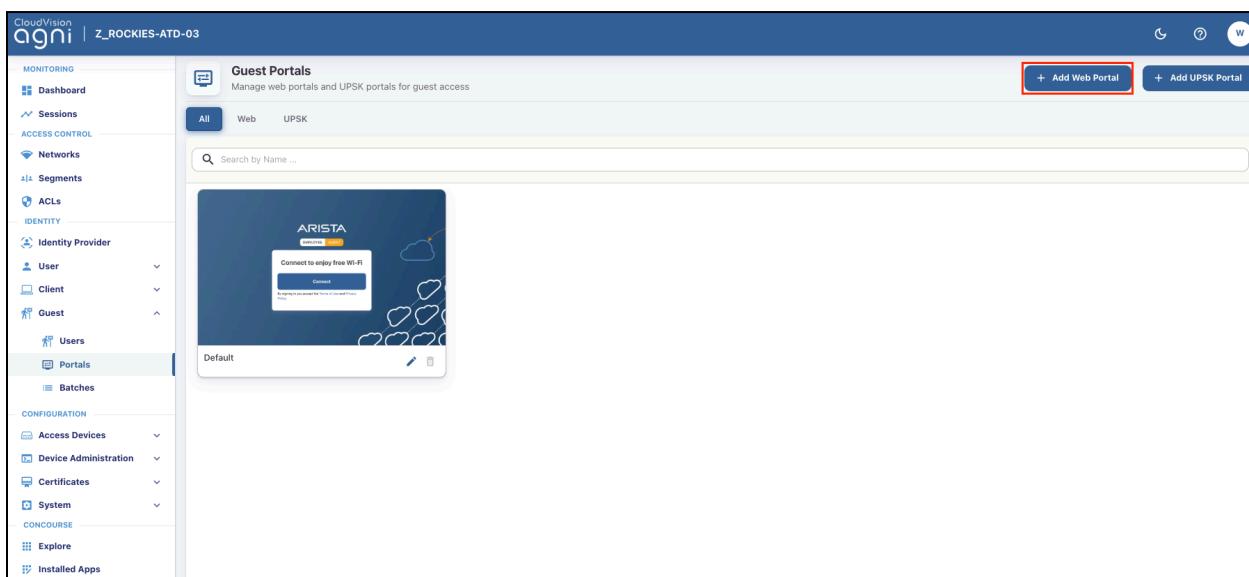
Configuring AGNI

Log in to AGNI and navigate to **Identity > Guests > Portals**.

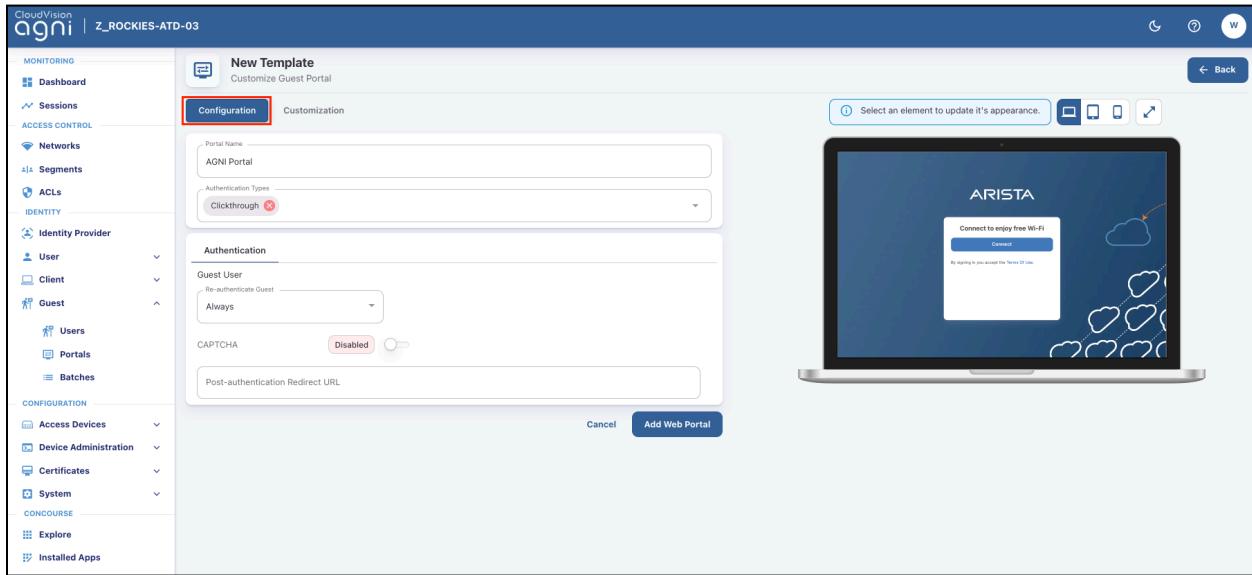


In **Guest Portals**, the **Default** portal is always present, which is non-removable. You can use the same for configuration. Let's create a new guest portal.

Click the **Add Web Portal** button.

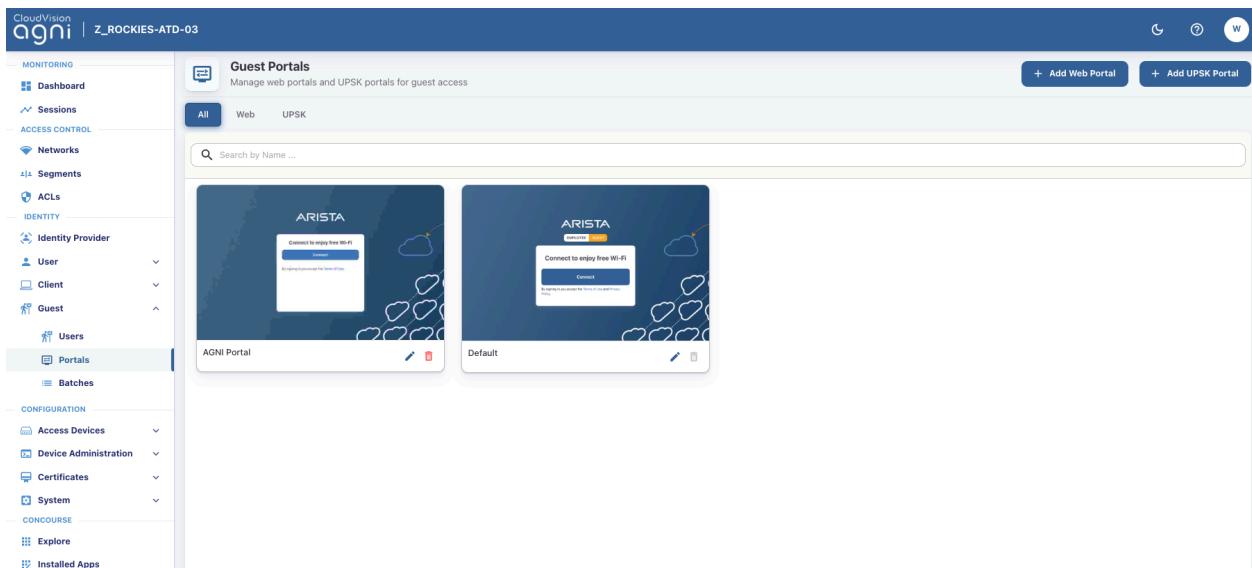


In the **Configuration** tab, provide the portal name (AGNI Portal) and select the Authentication Type as **Clickthrough**.



Click the **Customization** tab to customize the portal settings. Select the theme of the portal. The available theme options are **Default** or **Split Screen**. Next, click the dropdown for the **Select elements** to customize the portal options, 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.

The screenshot shows the CloudVision AGNI interface with the title "CloudVision AGNI | Z_ROCKIES-ATD-03". The left sidebar contains navigation links for MONITORING, ACCESS CONTROL, IDENTITY, and CONFIGURATION. Under CONFIGURATION, "Portals" is selected. The main content area is titled "Guest Portals" with the subtitle "Manage web portals and UPSK portals for guest access". It shows two entries: "AGNI Portal" and "Default". Each entry has a preview image of a Wi-Fi connection screen, a "Connect" button, and edit/delete icons. A search bar at the top says "Search by Name ...". Buttons for "+ Add Web Portal" and "+ Add UPSK Portal" are at the top right.

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**

Initial Role for Portal Authentication - **Portal Role**

The screenshot shows the 'AGNI Portal' configuration page. At the top, it says 'Provide the following details to update the selected Network'. The 'Name' field contains 'AGNI Portal'. The 'Connection Type' section has 'Wireless' selected. The 'SSID' field contains 'ATD-01-CP'. The 'Status' is set to 'Enabled'. In the 'Authentication' section, 'Captive Portal' is selected as the authentication type, and 'Internal' is selected as the captive portal type. The 'Select internal portal' dropdown shows 'AGNI Portal'. In the 'Captive Portal' section, 'Portal Role' is selected as the initial role for portal authentication. A note says 'Configure the following URL as captive portal in the initial role, to allow users sign in.' Below this is a text input field containing 'https://beta.agni.arista.io/portal/E5df4752d-db9-4225-815d-021ac6962610/network/13202' with a 'Copy' button next to it.

Click **Add Network**.

Copy the portal URL at the bottom of the page.

Configuring CV-CUE

In CV-CUE, select the Corp Location folder and 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.

NOTE: Role Names are case sensitive.

The screenshot shows the 'Network Profiles' section of the CV-CUE interface. A 'Role Profile' card is open, titled 'Portal Role'. The 'Role Name*' field contains 'Portal Role'. The 'Profile Name*' field also contains 'Portal Role'. A checkbox labeled 'Use SSID Settings in Absence of Role-Specific Settings' is unchecked. Under 'Role-Specific Settings', the 'VLAN' section is expanded, showing 'VLAN *' checked, 'VLAN ID' selected, and a dropdown menu set to '0'. A 'Firewall' section is partially visible. In the 'User Bandwidth Control' section, two checkboxes are present: 'Limit the maximum upload bandwidth per user to' and 'Limit the maximum download bandwidth per user to', both of which are unchecked. Under 'Redirection', 'Redirection' is checked, 'Static Redirection' is selected, and the 'Redirect URL*' field contains 'https://beta.agni.arista.io/portal/E5df4752d-dbdc'. A 'More' button is located in the top right corner of the card.

HTTPS Redirection

Certificate Information

Common Name www.arista.com	Organization Arista Networks	Organization Unit Arista Networks
-------------------------------	---------------------------------	--------------------------------------

Websites That Can Be Accessed Before Authorization *

X
...

Accepted formats include host names and IP addresses with or without port numbers, e.g., abc.com, abc.com:80, abc.com:10-20, abc.com:80,443,10-20, 192.168.1.100. If you enter a format without a port number, ports 80 and 443 will be added to it.

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**.

Network Profiles ▾ **Role Profile**

[Guest Role](#)

Role Name*
Guest Role

Profile Name*
Guest Role

Use SSID Settings in Absence of Role-Specific Settings

Role-Specific Settings

VLAN * ←

(VLAN ID) (VLAN Name)

0 [0 - 4094]

Firewall ←

Layer 3-4 Firewall Rules

Application Firewall Rules

User Bandwidth Control ←

Limit the maximum upload bandwidth per user to
Mbps [1 - 1024]

Limit the maximum download bandwidth per user to
Mbps [1 - 1024]

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**.

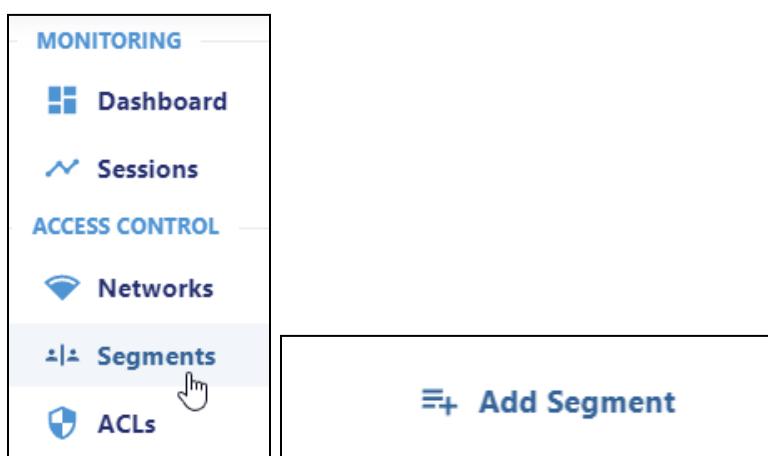
Add a new Segment with following settings:

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**



The screenshot shows the AGNI Segments page. At the top left is a user icon and the title 'Segments'. Below the title is a subtitle 'Segmentation Policies'. In the center is a search bar with the placeholder 'Search by segment name or description'. At the bottom of the page is a large button with a plus sign and the text 'Add Segment', with a mouse cursor icon pointing to it.

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

Add Segment

Provide the following details to add a new segment

Name: Wireless - EAP-TLS

Description: Wireless - EAP-TLS

Status: Enabled | **Disable** | **Monitor**

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

=+ Add Condition

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

Your Conditions should now look like this.

Conditions MATCHES ALL

Network: Name is Wireless-Guest-CP X

=+ Add Condition

Under Actions select **Add Action**.

Select, **Arista-WiFi - Role Profile - Guest Role**

Actions

Arista-WiFi: Assign Role Profile Assign Arista WiFi Role Profile X

Role Profile Guest Role

=+ Add Action

Add Segment

Provide the following details to add a new segment

Name: Wireless-Guest-CP

Description:

Status: Enabled | Disable | Monitor

Conditions MATCHES ALL

Network: Name is Wireless-Guest-CP

[Add Condition](#)

Actions

Arista-WiFi: Assign Role Profile Assign Arista WiFi Role Profile

Role Profile Guest Role

[Add Action](#)

[Cancel](#) [Add Segment](#)

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**

The screenshot shows the WiFi configuration interface. At the top, there's a navigation bar with 'WiFi' and 'SSID' tabs. Below that, a breadcrumb trail shows '← ATD-01-CP'. Underneath, there's a 'WLAN' dropdown and tabs for 'Basic', 'Security', 'Network', and 'Access Control'.

The main area is titled 'Name' and contains fields for 'SSID Name *' (with 'ATD-01-CP' entered) and 'Profile Name *' (also 'ATD-01-CP').

A section titled 'Select SSID Type' has a radio button for 'Private' (which is selected) and one for 'Guest'.

At the bottom, there are two checkboxes: one for 'Hide SSID' and another for 'Include AP Name in Beacon'.

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**.

The screenshot shows the 'Captive Portal Test' configuration page under the 'Access Control' tab. The 'RADIUS Settings' section is highlighted, showing 'RadSec' selected and 'Primary' chosen for the RADIUS server. The 'Authentication Server' dropdown is set to 'AGNI'. The 'Send DHCP Options and HTTP User Agent' checkbox is checked. The 'Retry Parameters' section shows attempts set to 4 and timeout to 2 seconds. The 'Username and Password' section shows 'MAC Address without Delimiter' as the username.

WLAN ▼ Basic Security Network Access Control :

▶ Firewall

Client Authentication

Google Integration RADIUS MAC Authentication

RADIUS Settings

RadSec

Primary Additional

Authentication Server *

AGNI

Add/Edit

Accounting Server

AGNI

Add/Edit

Send DHCP Options and HTTP User Agent

Retry Parameters

Attempts *

4 [1 - 10]

Timeout *

2 seconds [1 - 10]

Username and Password

Username

MAC Address without Delimiter

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.

Select **Client Isolation** (optional) to disable client-to-client communications.

[Captive Portal Test](#)

WLAN ▼ Basic Security Network Access Control ⋮

Accounting Stop Delay

If Client Authorization Fails
 Disconnect Stay connected

Role Based Control

RADIUS VSA Google OU This setting is not editable because Client Authentication via Google Integration is disabled. [Change Settings?](#)

Rule Type *
802.1X Default VSA

Operand * Match Assign Role * All

DHCP Fingerprinting based Access Control

Bonjour Gateway

Redirection

WiFi Clients in Allow List or Deny List

Client Isolation

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”.

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.