

# Campus C-02 AGNI Lab Guide

## UPSK Wireless Policy



This Lab Guide:

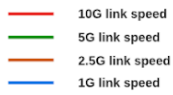
<https://github.com/arista-rockies/Workshops/tree/main/Campus>

# Table of Contents

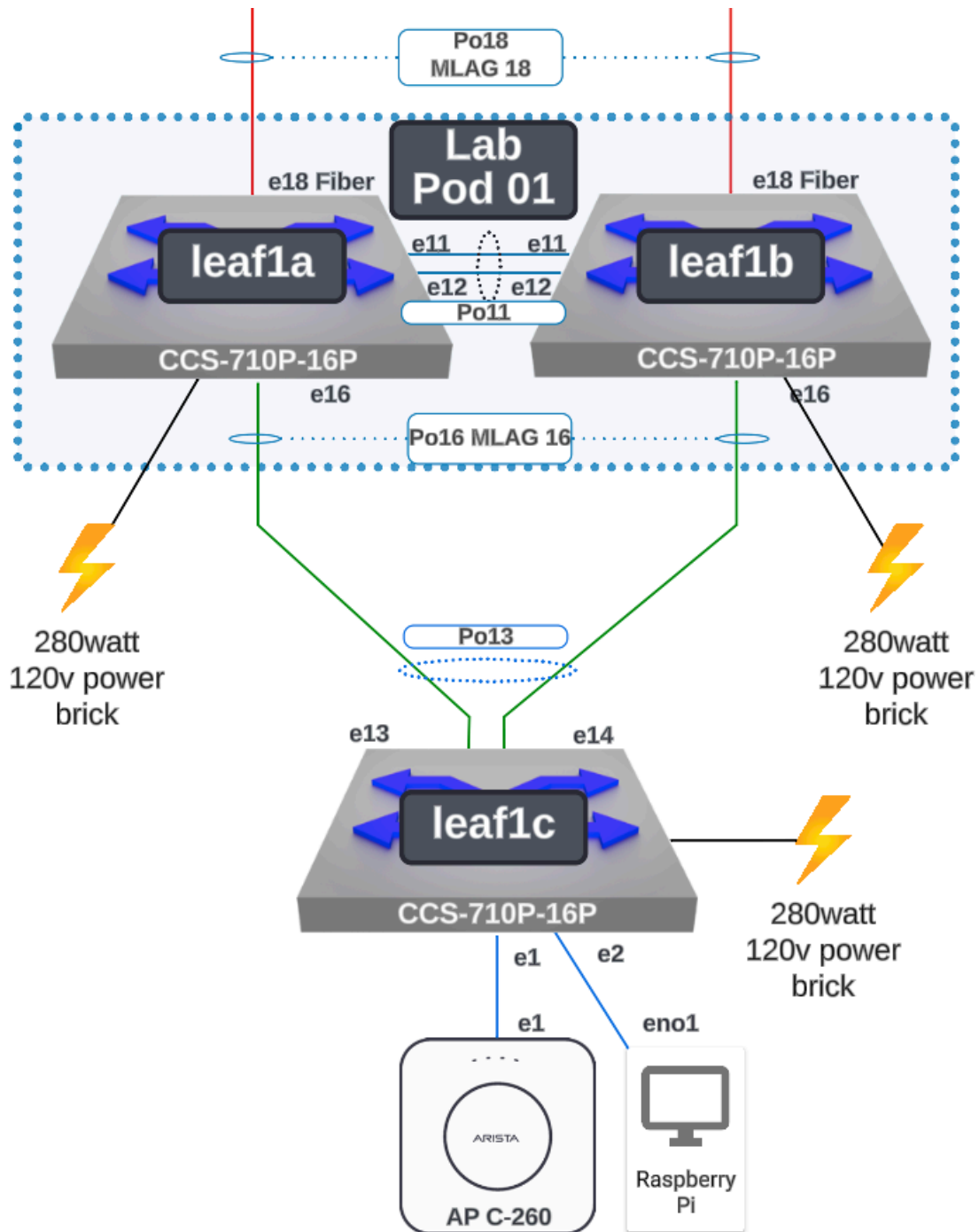
<b>Full Lab Topology.....</b>	<b>2</b>
<b>POD Topology.....</b>	<b>3</b>
<b>NAC Lab #2 - Create UPSK Wireless Policy.....</b>	<b>4</b>
1. Create Identity UPSK SSID:.....	4
2. Create UPSK Network and Segment:.....	10
3. Create an AGNI Local User and Enroll Personal Device.....	15
4. Create an AGNI Client Group.....	19

## Arista Workshop LAB

### Lab Networks Diagram



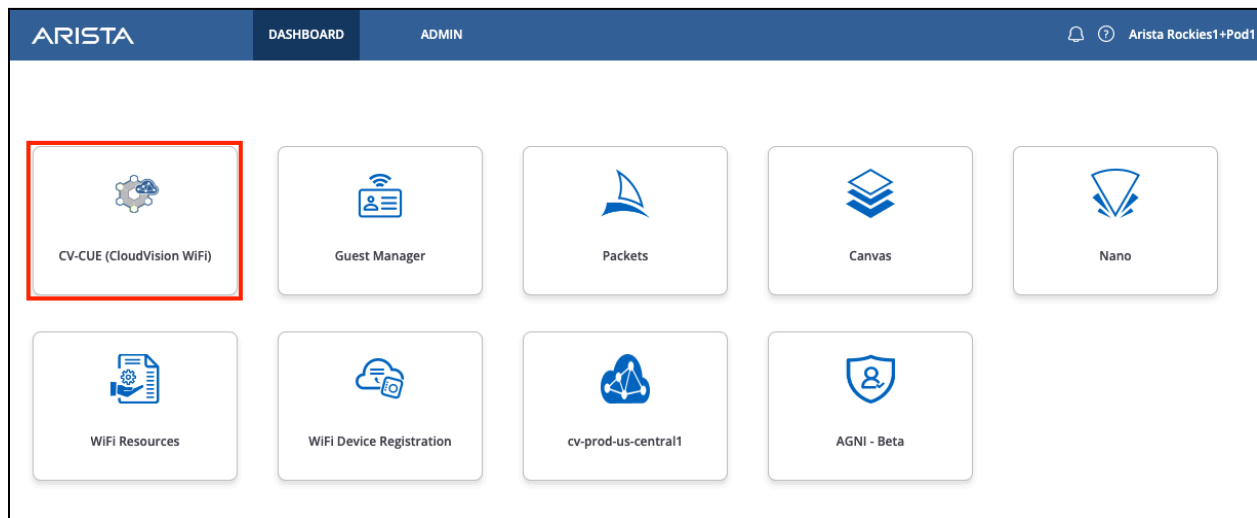
## POD Topology



# NAC Lab #2 - Create UPSK Wireless Policy

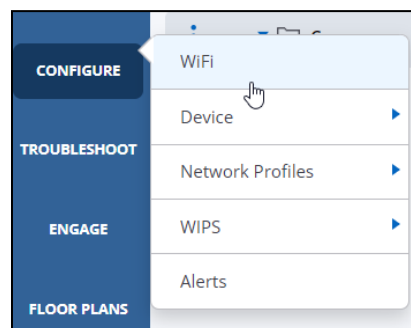
## 1. Create Identity UPSK SSID:

Return to the LaunchPad tab and Log into CV-CUE <https://launchpad.wifi.arista.com/>, or access the CV-CUE tab in your browser.

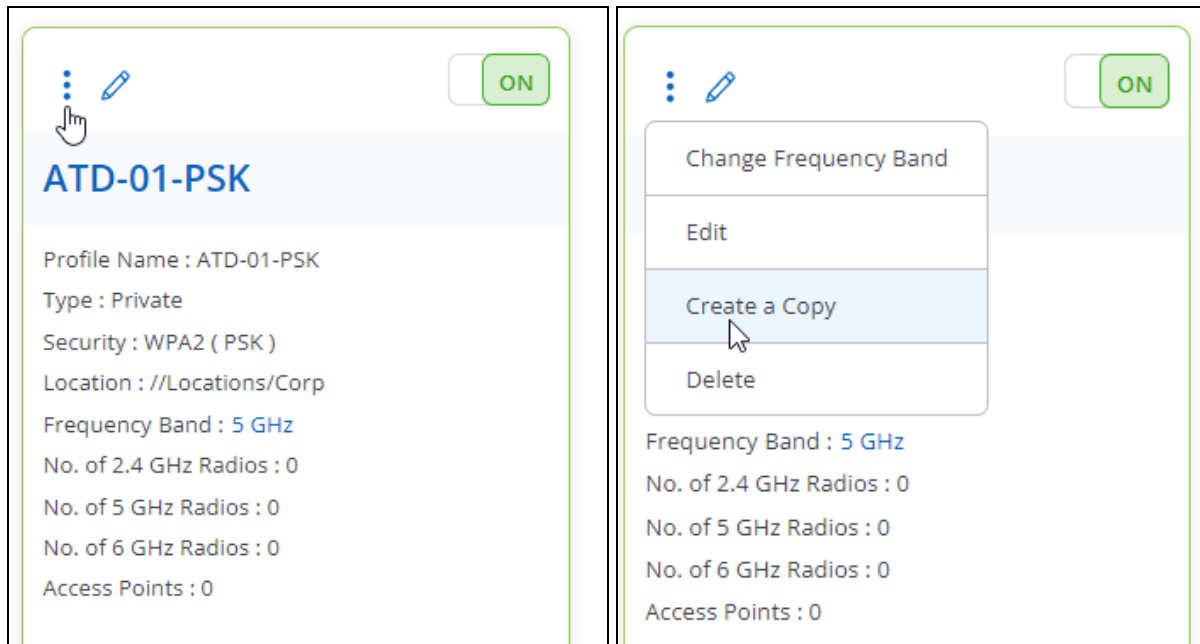


Next, we will modify the PSK SSID we created in the CV-CUE lab.

While on the **Corp** folder, Click on **Configure** and then **WiFi**



Next, click on the 3 Dots and select **Create a Copy** on the SSID **ATD-##-PSK** where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod



Select - **Currently Selected Folders** and then **Continue**.

### Create a Copy of SSID

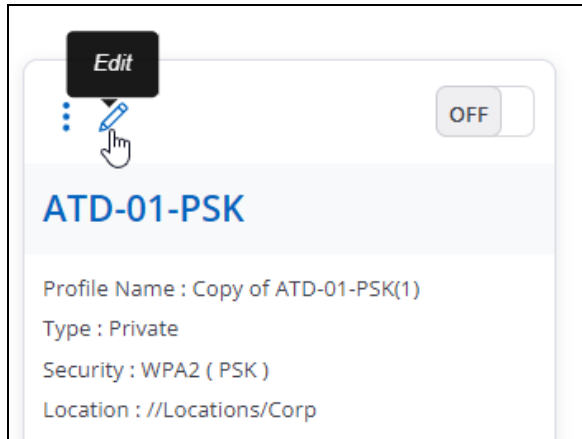
×

Where would you like to create a copy of this SSID Profiles?

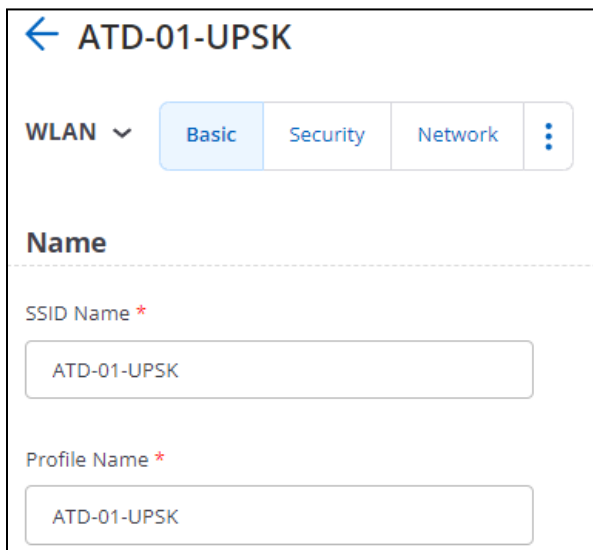
☒ Currently Selected Folder ☐ At a Different Folder

**Continue**

Click on the new SSID and select **Edit**.



On the Basic Tab rename the SSID to **ATD-##-UPSK**, and copy the SSID Name and paste it in the Profile Name field.



Next, click on the Security Tab and change the WPA2 Security from PSK to **UPSK**

←

ATD-01-UPSK

WLAN ▾

Basic

Security

Network

Access Control

⋮

Select Security Level for Associations

*In the 6 GHz band, WiFi 6E does not sup*

WPA2 ▾

☐ PSK

☒ **UPSK**

☐ 802.1X

Next, select **UPSK Identity Lookup**

☐ UPSK User Private Networks

☒ UPSK Identity Lookup

For more information on UPSK click here:

<https://arista.my.site.com/AristaCommunity/s/article/Unique-PSKs>



Next, Click on the **Access Control** tab. Under **RADIUS Settings**, select **RadSec** and then **AGNI** for the Authentication and Accounting Servers, and select **Send DHCP Options and HTTP User Agent**.

[←](#) ATD-01-UPSK

WLAN ▾

BasicSecurityNetworkAccess Control⋮

### RADIUS Settings

☐ RADIUS Pooling

☒ RadSec

PrimarySecondary

Authentication Server\*

AGNI ▾

Add/Edit

Accounting Server

AGNI ▾

Add/Edit

☒ Send DHCP Options and HTTP User Agent

Confirm the Username and Password, Called Station, COA information.

### Username and Password

Username

MAC Address without Delimiter

☐ Password

---

### Called Station/NAS ID

[Location Tag](#)

Called Station ID \*

NAS ID \*

%m-%s

%m-%s

%m - Access Point's Ethernet MAC  
%s - SSID  
%n - Device Name  
%l - Location Tag

☒ **Change of Authorization (CoA)**

Finally, **Save** and turn on the SSID.

**Save**

### Turn SSID On - ATD-01-UPSK

Select the frequency bands for this SSID

☐ 2.4 GHz ☒ 5 GHz ☐ 6 GHz

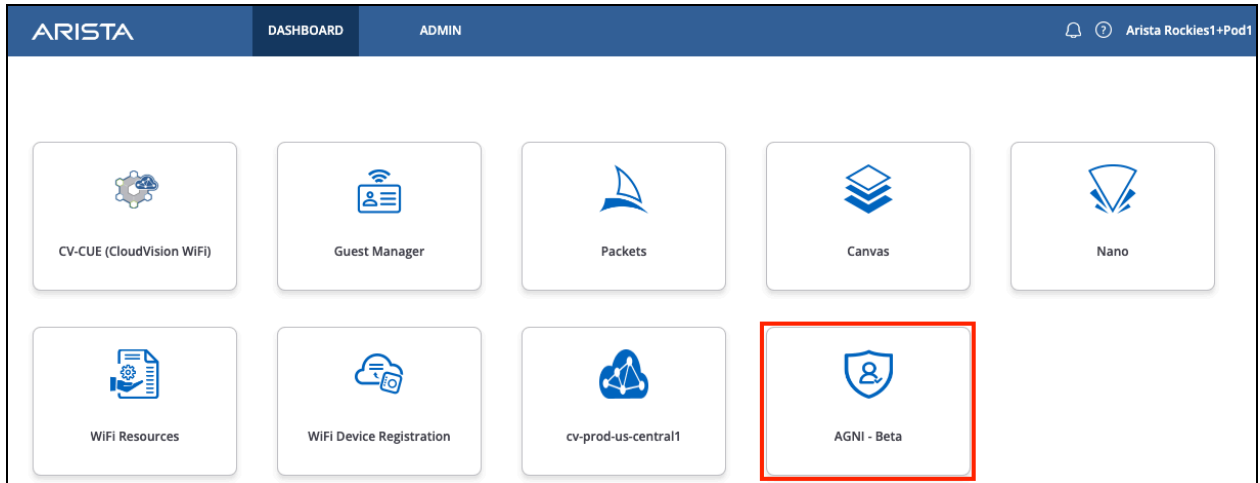
[Cancel](#) **Turn SSID On**

**Please Read!**

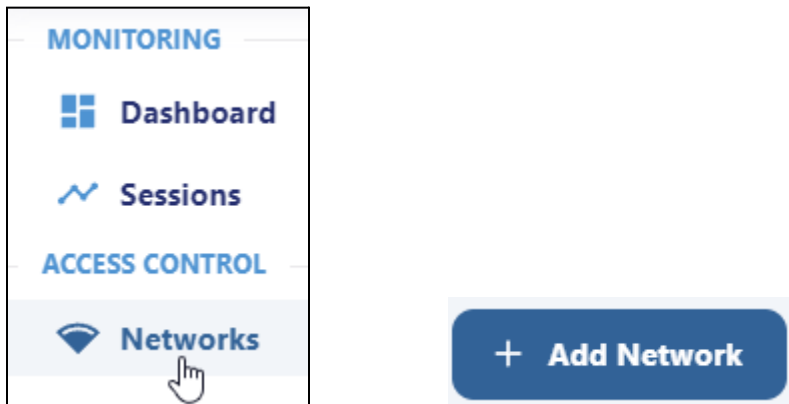
**Only select the “5 GHz” option** on the next screen (**uncheck** the 2.4 GHz box if it's checked), then click **“Turn SSID On”**.

## 2. Create UPSK Network and Segment:

Return to the LaunchPad tab, and select the AGNI tile, or go to your AGNI tab in your browser.



Click on **Networks** and then **+ Add Network**.



Add the following:

Name: **Wireless-UPSK**

Connection Type: **Wireless**

SSID: **ATD-##-UPSK**

Authentication Type: **Unique PSK (UPSK)**

**Add Network**

**Add Network**  
 Provide the following details to add a new Network
 ← Back

Name

Connection Type: ☒ Wireless ☐ Wired

SSID  
 ATD-01-UPSK

Status: Enabled ☒

**Authentication**  
 Authentication Type  
 Unique PSK (UPSK)

Allowed Users: ☒ Organizational users only ☐ Guest users only

**User Private Networks** Disabled ☐  
 ⓘ Enable to prevent clients belonging to different users from communicating with each other.

**Onboarding** Disabled ☐

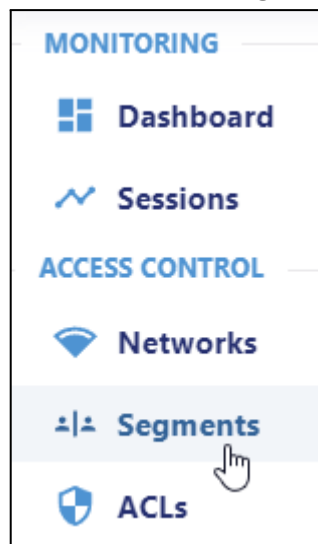
Cancel Add Network

You should now see this listed in your networks.

<b>Wireless-UPSK</b>	Wireless	Unique PSK (UPSK)	ATD-01-UPSK	<span>Enabled</span>
----------------------	----------	-------------------	-------------	----------------------

Next, we will add the Segment.

Under Access Control, click on **Segments** and then **+ Add Segment**



**+ Add Segment**

Name: **Wireless-UPSK**

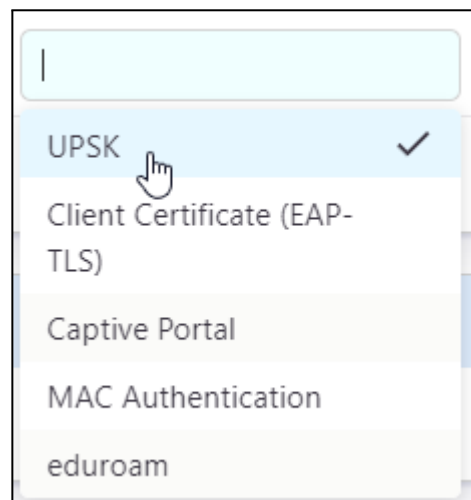
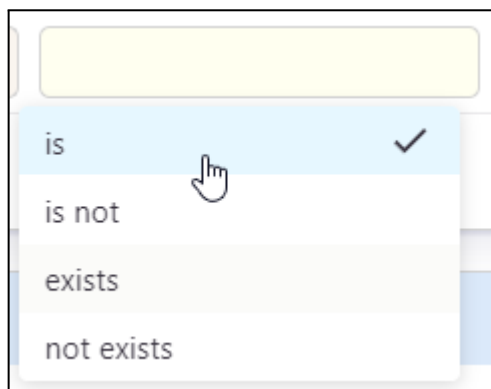
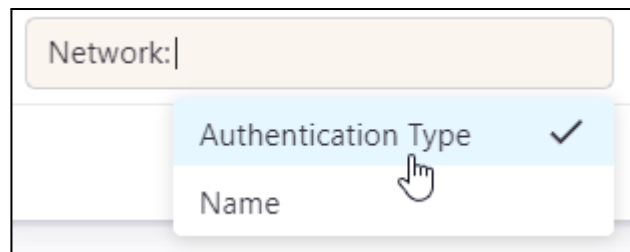
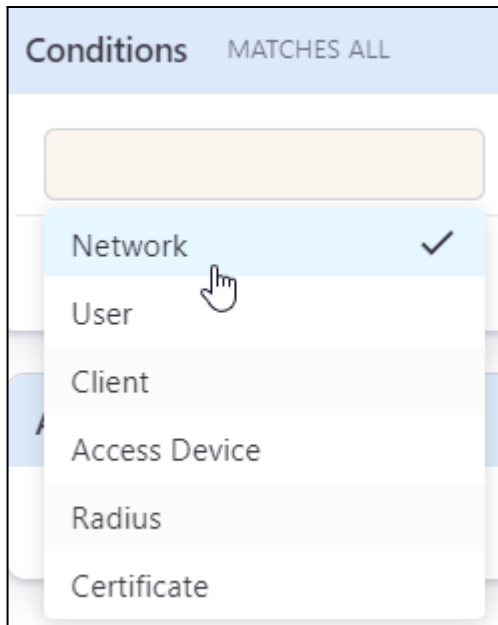
Description: **Wireless-UPSK**

 **Add Condition**

Click on **+ Add Condition**

Conditions: **Network:Authentication Type is UPSK**

**\*Note:** Conditions are always Matches ALL.



Conditions

MATCHES ALL

Network: Authentication Type

is

UPSK

×

⌵+ Add Condition

Click on **+ Add Action**

Actions: **Allow Access**

Actions

Assign VLAN

Apply ACL

Allow Access ✓

Deny Access

Arista-WiFi

Radius

Actions

Allow Access

Allow default access

**Add Segment**  
Provide the following details to add a new segment

← Back to Segments

Name

Wireless-UPSK

Description

Wireless-UPSK

Status: Enabled

Disable | Monitor

Conditions

MATCHES ALL

Network: Authentication Type

is

UPSK

×

⌵ Add Condition

Actions

Allow Access

Allow default access

×

⌵ Add Action

Cancel

Add Segment

Finally, click on **Add Segment**.

You should now see **Wireless-UPSK** in the list of segments.

**Segments**  
Segmentation Policies

🔍 Search by segment name or description

⌵+ Add Segment

⋮

▼

Wireless-UPSK

Wireless-UPSK

✎

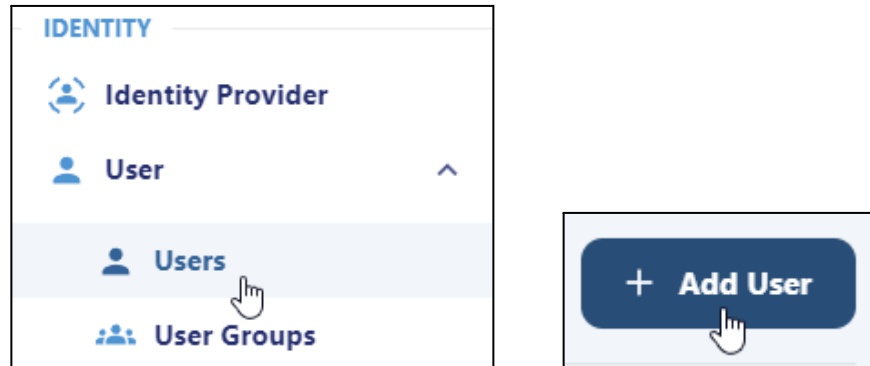
🗑

⋮

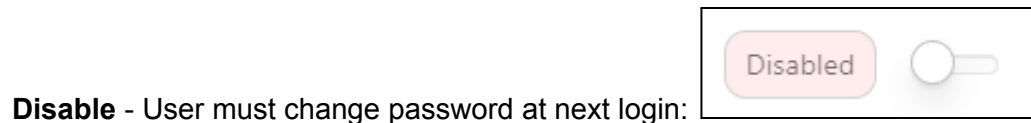
### 3. Create an AGNI Local User and Enroll Personal Device

In this section you will create a local user and enroll the MAC of your device.

In AGNI, under Identity, click on **User** and then **+ Add User**.



Fill out the sections. Use **Arista01!** for the password.

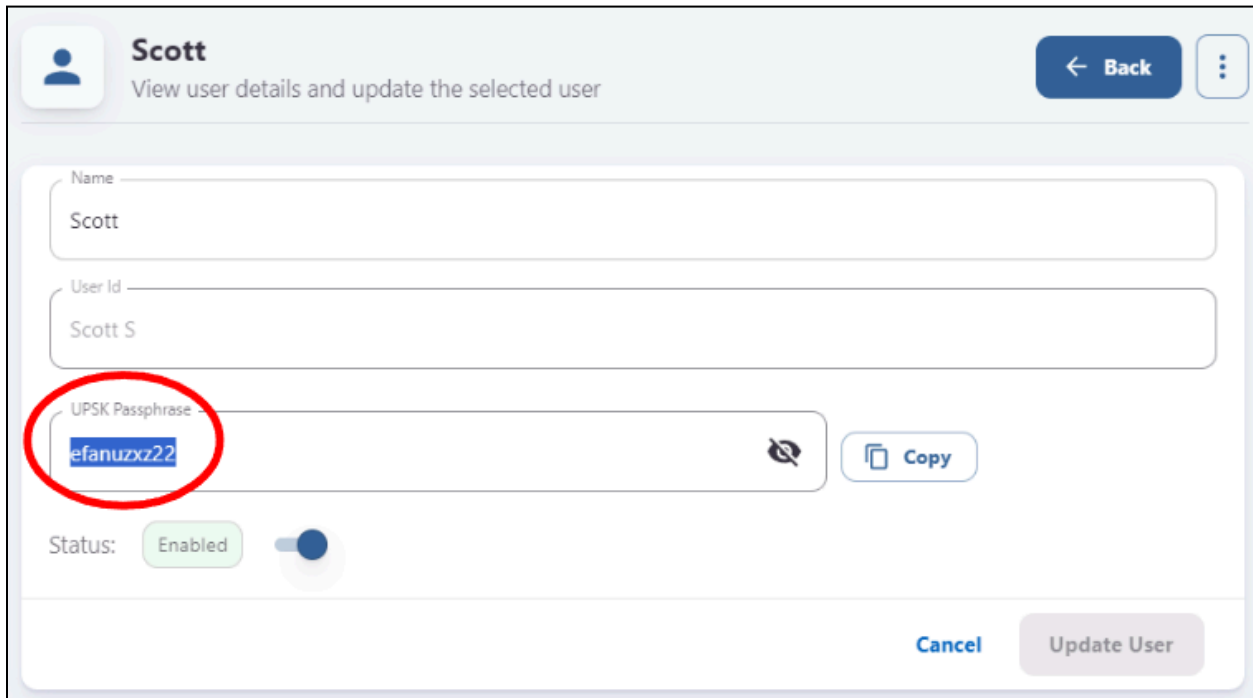
The image shows the 'Add Local User' form in the AGNI interface. The form has a title bar with a user icon, the text 'Add Local User', and a subtitle 'Provide the following details to add a new local User'. There is a 'Back' button in the top right. The form contains several input fields: 'User Id' with the value 'Scott S', 'Name' with the value 'Scott', and 'Password' with the value 'Arista01!'. Below these fields is a 'Status' section with a toggle switch set to 'Enabled'. At the bottom of the form, there is a section labeled 'User must change password at next login:' with a toggle switch set to 'Disabled', which is circled in red. At the very bottom of the form are 'Cancel' and 'Add User' buttons.

Click **Add User**

**NOTE:** You will notice that Password has now changed to UPSK Passphrase



Copy and write down or save to text file the new UPSK Passphrase.



The image shows a user management interface for a user named "Scott". The header includes a user icon, the name "Scott", and the subtitle "View user details and update the selected user". There is a "Back" button and a menu icon. The form contains three input fields: "Name" with the value "Scott", "User Id" with the value "Scott S", and "UPSK Passphrase" with the value "efanuzxz22". The "UPSK Passphrase" field is highlighted with a red circle. To the right of the passphrase field is a "Copy" button. Below the fields is a "Status" section with a toggle switch set to "Enabled". At the bottom right are "Cancel" and "Update User" buttons.

Field	Value
Name	Scott
User Id	Scott S
UPSK Passphrase	efanuzxz22
Status	Enabled

Next, connect your client to **ATD-##-UPSK** using your UPSK Passphrase.

Click on Sessions and validate your device connection.

^	#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
v	1	Scott S	Unique PSK (UPSK)	66:d8:a6:7a:e5:b5	10.11.0.122	Success	4/4/2024 15:17:45.431

**Session Details - Rco7fpm878m8s72ob117g**  
 Details for Session
 Disconnect
Back

**Authentication Request**
Success

Authentication Type	Unique PSK (UPSK)
Segment	Wireless-UPSK
Location	Locations/Corp/1st Floor/1st Floor

**Session Details**
Open

Client IP Address	10.11.0.122
Session Start Time	4/4/2024 15:17:45.431
Session Stop Time	-

**User**
Enabled

**Client**
Enabled

**Actions**

Scott S  
 Scott

66:d8:a6:7a:e5:b5  
 Auto registered with UPSK

Allow Access

**Access Device**
Arista WiFi

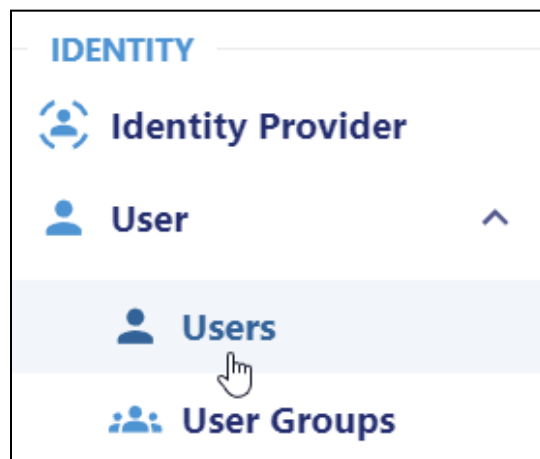
**Network**
Enabled


30:b6:2d:e2:51:8f  
 ATD\_AP01  
 Access Points

Wireless-UPSK-ATD48  
 ATD-48-UPSK  
 Unique PSK (UPSK)

Input Request Attributes
 Output Response Attributes

Next, validate your device by clicking on **User** and then **Users**. Select your user.



**Scott**  
View user details and update the selected user

[< Back](#)

⋮

Name


Scott

User Id

Scott S

UPSK Passphrase


.....



[Copy](#)

Status:


Enabled



[Cancel](#)

[Update User](#)




Reset Password



User clients

[Show Clients](#)

Click on **Show Clients**

User clients				<a href="#">Hide Clients</a>
<div><div> Search by MAC address...</div><div>Status</div><div>Any</div></div>				
#	MAC ADDRESS	DESCRIPTION	STATUS	
1	66:d8:a6:7a:e5:b5	Auto registered with UPSK	Enabled	 

## 4. Create an AGNI Client Group

In this section, you will simulate your device as an IoT device.

Disable and forget previously saved lab networks so your wireless connection on your test device does not auto connect. Under your user client list, delete your device.

User clients

Hide Clients

Search by MAC address...

Status

Any

#	MAC ADDRESS	DESCRIPTION	STATUS	
1	66:d8:a6:7a:e5:b5	Auto registered with UPSK	Enabled	<div><div></div><div>Delete</div></div>

Are you sure you want to delete client with MAC address '66d8a67ae5b5'?

Cancel

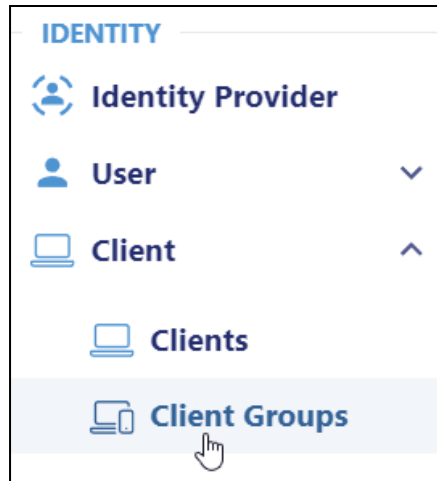
Delete

66d8a67ae5b5 is deleted successfully

Next, you will add your client device as an IoT device in a Client Group.

First, we will need to create the Client Group.

In AGNI, under Identity, click on **Client Groups** and then **+ Add Client Group**.




Name: **Corp Approved Devices**

Description: **Corp Approved Devices**

User Association: **Not user associated**

Enable the Group UPSK. Copy the UPSK Passphrase

Then click on **Add Group**



## Corp Approved Devices

Provide the following details to update the Client Group

+

Add or Import Clients

←

Back

⋮

Name

Corp Approved Devices

Description

User Association

Not user associated

Group UPSK

Enabled

All clients belonging to this group must use the following Group UPSK to connect to the network.

UPS K Passphrase

yw8nsn4iu4

👁

Copy

Allowed Networks

Networks

All Networks

×

Select Networks...

Delegated Management


Disabled

Only AGNI admins can manage members of this group. Enable this to allow specific User Groups to add or remove clients to this group.

Add Group

Next, connect your client to **ATD-##-UPSK** using the Client Group UPSK Passphrase.

Click on Sessions and validate your device connection.

IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS
Corp Approved Devices	Unique PSK (UPSK)	bc:a5:8b:d6:a7:1f	192.168.101.103	Success 

Session Details - Rco7gefpr6phc72s9jimg
Disconnect
Back

**Authentication Request**
Success

Authentication Type: Unique PSK (UPSK)  
 Segment: Wireless-UPSK  
 Location: Locations/Corp/1st Floor/1st Floor

**Session Details**
Open

Client IP Address: 192.168.101.103  
 Session Start Time: 4/4/2024 16:02:07.651  
 Session Stop Time: -

**User**

Not available

**Client**
Enabled

bc:a5:8b:d6:a7:1f  
 -  
 Corp Approved Devices

**Access Device**
Arista WiFi

30:b6:2d:e2:51:8f  
 ATD\_AP01  
 Access Points

**Network**
Enabled

Wireless-UPSK  
 ATD-01-UPSK  
 Unique PSK (UPSK)

**Actions**

Allow Access

**Input Request Attributes**
▼

**Output Response Attributes**
▼

Session logs for request: Rco7gefpr6phc72s9jimg
 Show Logs

Next Click on your Client.

**IDENTITY**

Identity Provider


User

Client

**Clients**

	#	MAC ADDRESS	DESCRIPTION	OWNER (USER)	STATUS	CLIENT GROUP
<input type="checkbox"/>	1	bc:a5:8b:d6:a7:1f	-		Enabled	Corp Approved Devices

Notice your Client Group. Here you have the option to change the Client Group your device belongs to.

**bc:a5:8b:d6:a7:1f**  
View client details and update the selected client

MAC Address

bc:a5:8b:d6:a7:1f


Description


Client Group

Corp Approved Devices

UPSK Passphrase


.....



 Copy

Status:

Enabled





Cancel


Update Client




Next, delete your device from the **Client Group - Corp Approved Devices**.

**Corp Approved Devices**  
Provide the following details to update the Client Group

 Add or Import Clients


 Back




All clients belonging to this group must use the following Group UPSK to connect to the network.

UPSK Passphrase

\*\*\*\*\*





 Copy

Regenerate


**Allowed Networks**

Networks

All Networks  Select Networks...



**Delegated Management**

Disabled 


Only AGNI admins can manage members of this group. Enable this to allow specific User Groups to add or remove clients to this group.

Cancel

Update Group



**Clients in this group**


Hide Clients

 Search by MAC Address or description ...


Status 

Any

#	MAC ADDRESS	DESCRIPTION	STATUS	
1	bca58b:d6:a7:1f		Enabled	<div></div>

 Back

Delete



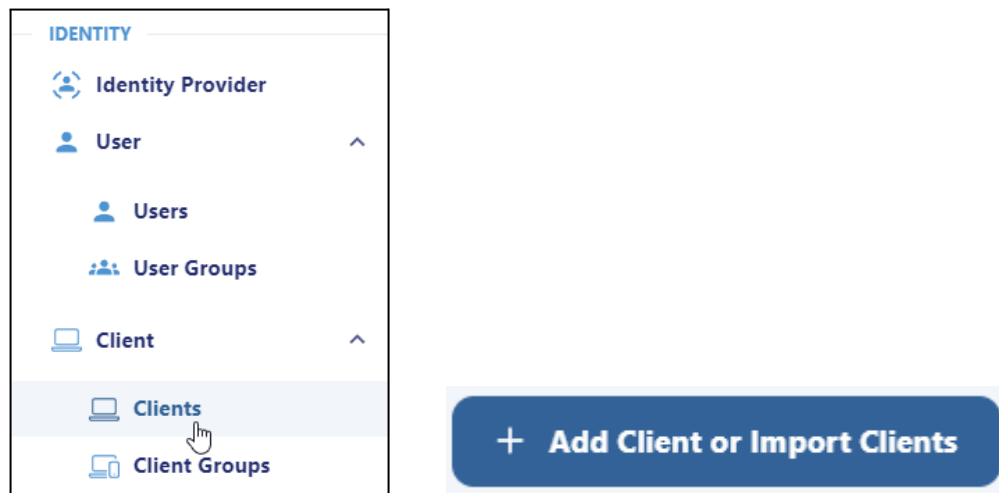
**Are you sure you want to delete Client with  
MAC address 'bca58bd6a71f'?**

Cancel

Delete

24

Next, under Identity, click on **Clients** and then **+ Add Client**.





Select the Client Group: **Corp Approved Devices**

Add in the MAC Address of your test device like your phone that is not randomized.


Then select **Add Client**




The image shows a form titled 'Add or Import Clients' with a laptop icon on the left and a 'Back' button on the right. Below the title is a subtitle: 'Provide the following details to add a new client or upload a file to import clients'. The form contains three main sections: 1. 'Client Group' with a dropdown menu showing 'Corp Approved Devices' and a plus icon. 2. 'Choose Action:' with two radio buttons: 'Add' (selected) and 'Import'. 3. 'MAC Address' with a text input field containing 'bc:a5:8b:d6:a7:1f'. Below this is a 'Description' text input field. At the bottom right are 'Cancel' and 'Add Client' buttons.

You will then see the Client added to the Group.

Clients in this group				Hide Clients
<input type="text" value="Search by MAC Address or description ..."/>				Status Any
#	MAC ADDRESS	DESCRIPTION	STATUS	
1	bc:a5:8b:d6:a7:1f		Enabled	 

Validate and Verify your connection using the Client Group UPSK Passphrase.


**Corp Approved Devices**  
Provide the following details to update the Client Group

 Add or Import Clients  Back 

Name  
Corp Approved Devices



Description


User Association  
Not user associated

**Group UPSK** Enabled 

All clients belonging to this group must use the following Group UPSK to connect to the network.

UPSK Passphrase  
yw8nsn4iu4

  Copy

IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS
Corp Approved Devices	Unique PSK (UPSK)	bc:a5:8b:d6:a7:1f	192.168.101.103	Success 

## NAC LAB #2 COMPLETE