

Campus C-03 AGNI Lab Guide

EAP-TLS Wired Policy



This Lab Guide:

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

Table of Contents

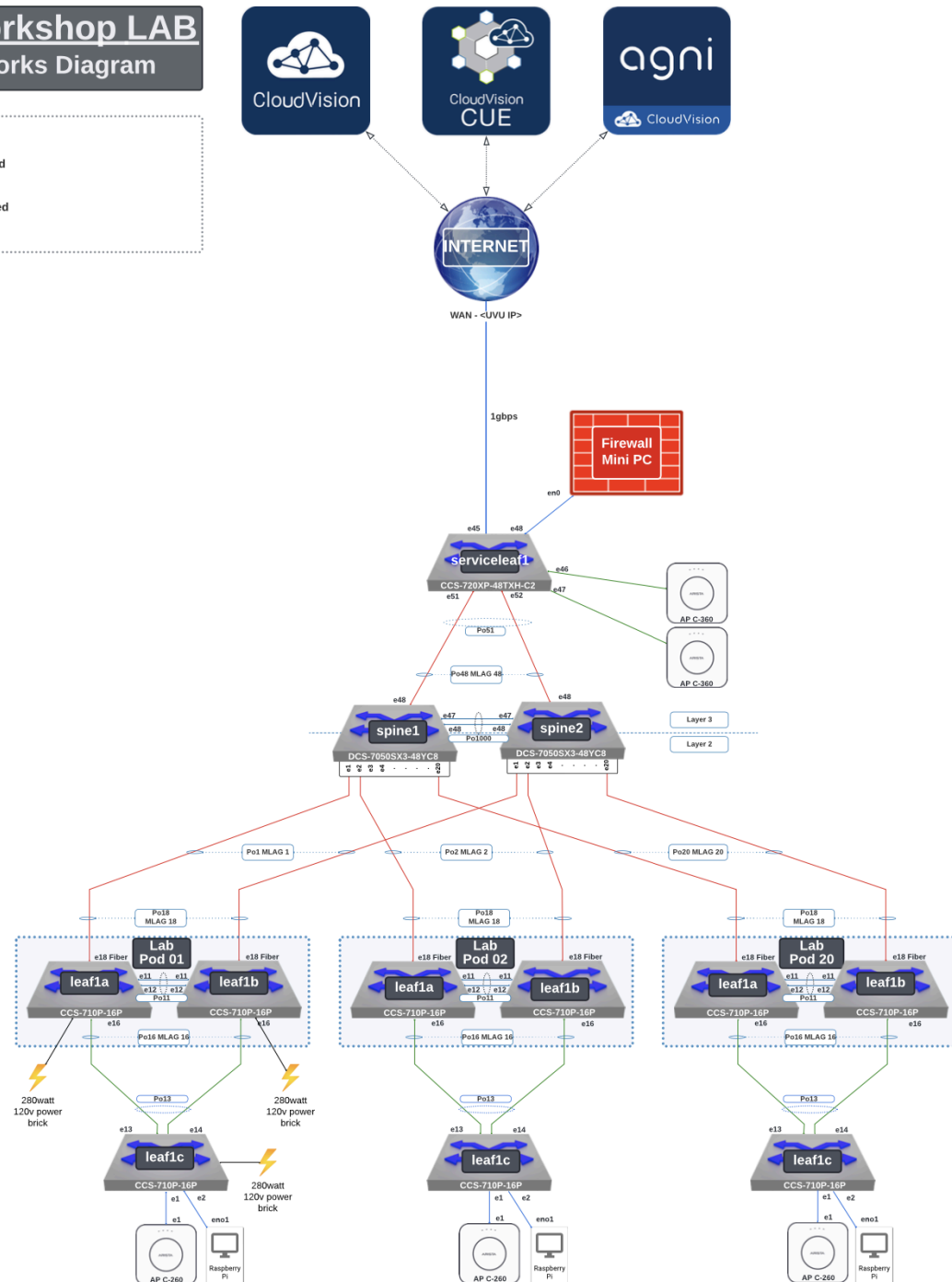
Full Lab Topology.....	2
POD Topology.....	3
NAC Lab #3 - Create EAP-TLS Wired Policy.....	4
1. Access CloudVision as a Service.....	4
2. Enable RadSec on campus-pod<xx>-leaf1c.....	6
3. Access AGNI from the LaunchPad.....	11
4. Create Wired EAP-TLS Network and Segment.....	12
5. Validate and Verify Wired EAP-TLS Device.....	18
Additional Information.....	20
A. 802.1x High-Level Overview.....	20
B. Configuring RadSec profile in EOS.....	21
C. Adding Access Control Lists for Wired Users.....	22

Full Lab Topology

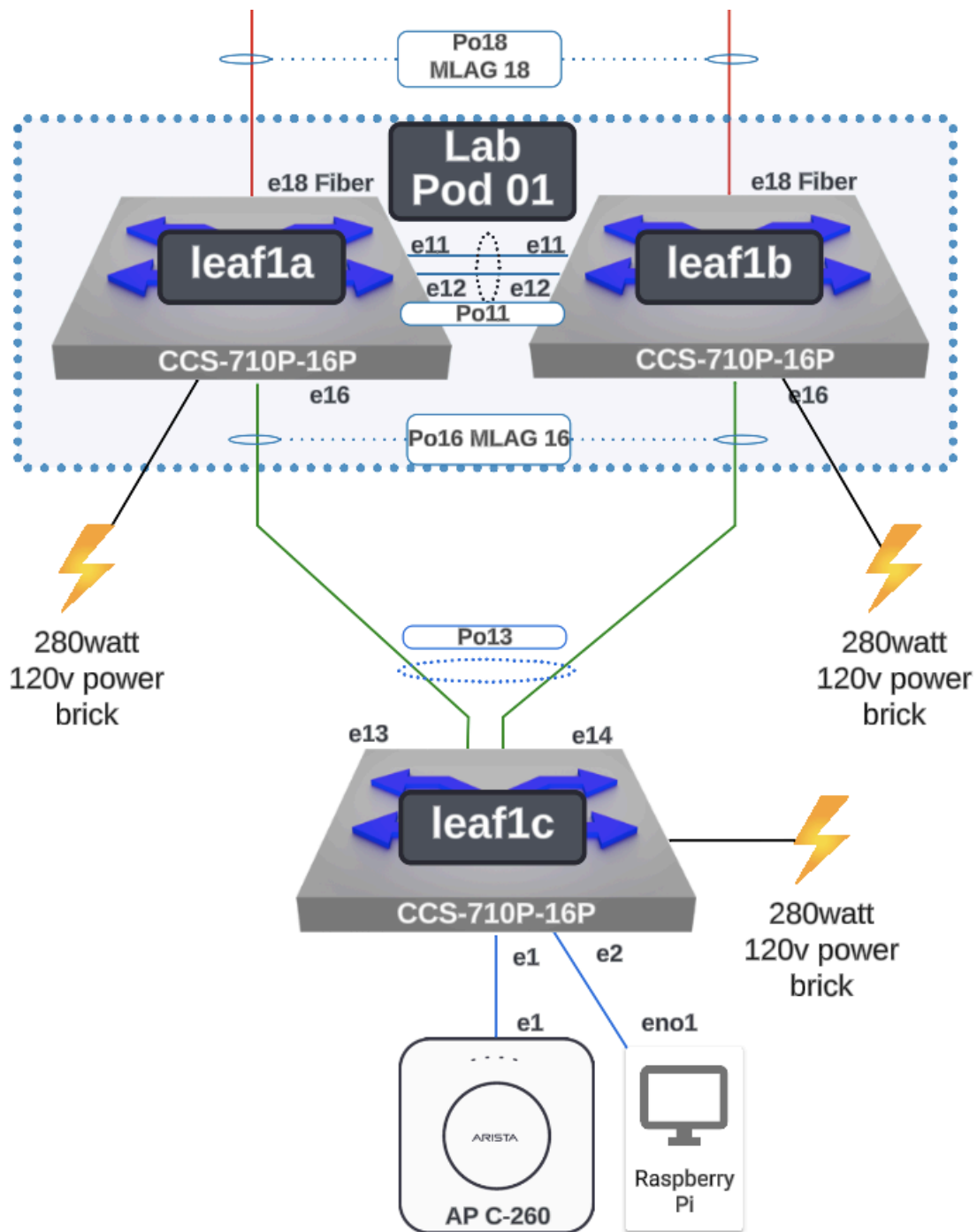
Arista Workshop LAB Lab Networks Diagram

Key:

- 10G link speed
- 5G link speed
- 2.5G link speed
- 1G link speed



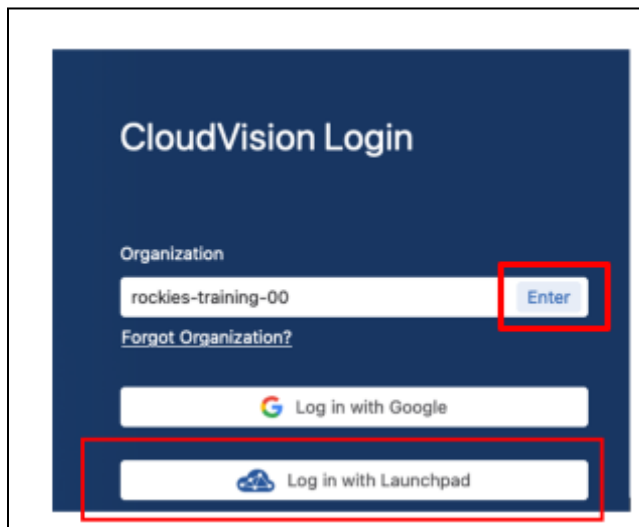
POD Topology



NAC Lab #3 - Create EAP-TLS Wired Policy

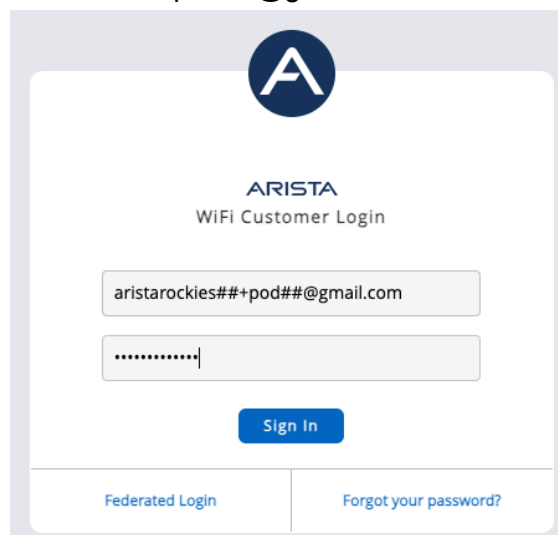
1. Access CloudVision as a Service

1. In your browser, enter the following URL: <https://www.arista.io/> to access CloudVision as a Service (CVaaS).
2. Enter the Organization name <rockies-training-##> in the “**Organization**” box, then click “**Enter**” (where ## is a 2 digit character between 01-20 that was assigned to your lab/Pod).

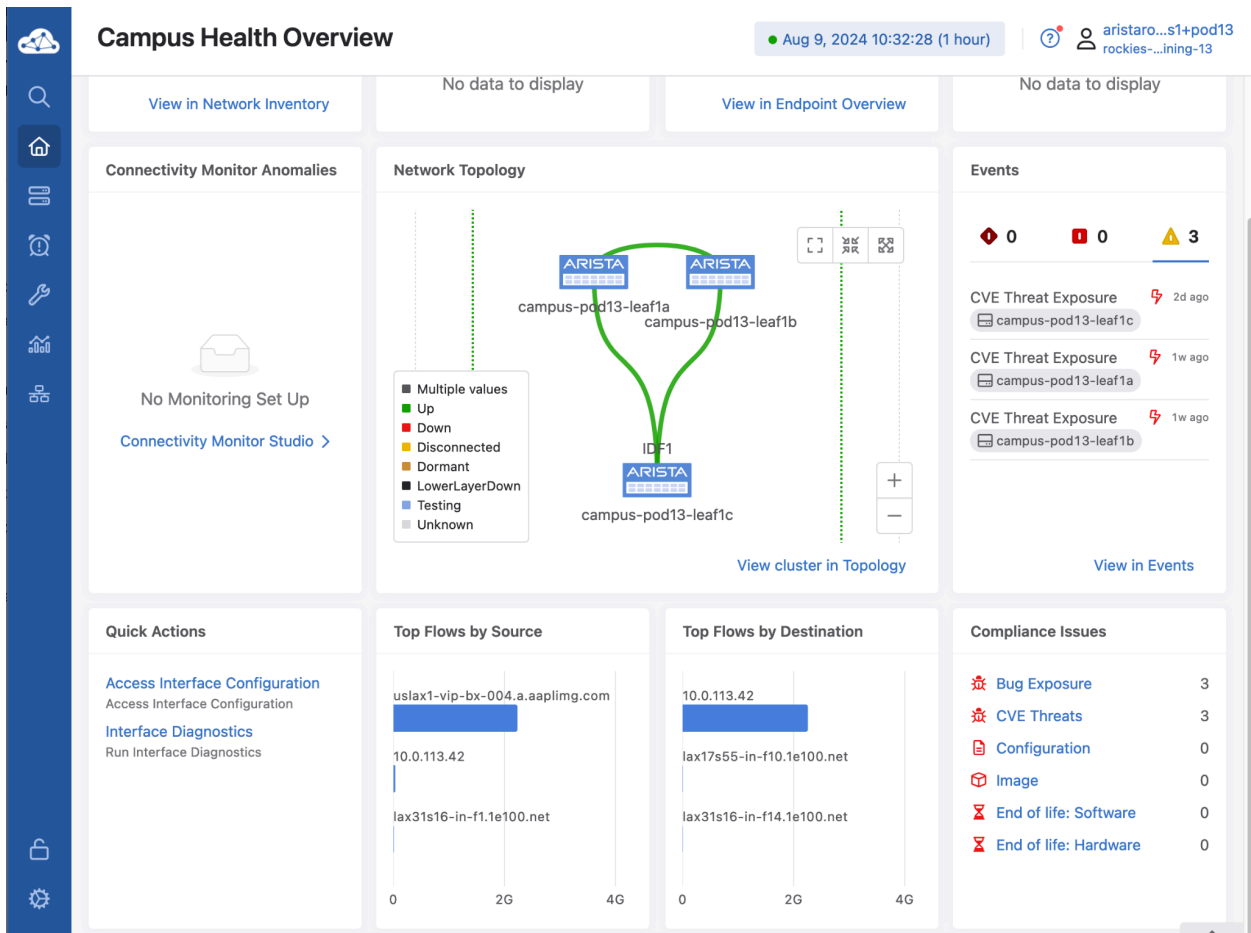
The image shows the CloudVision Login interface. It has a dark blue header with the text "CloudVision Login". Below this is a form with a label "Organization" and a text input field containing "rockies-training-00". To the right of the input field is a blue button labeled "Enter". Below the input field is a link "Forgot Organization?". At the bottom of the form are two buttons: "Log in with Google" and "Log in with Launchpad". The "Log in with Launchpad" button is highlighted with a red rectangle.

3. Click the Log in with Launchpad button and provide your assigned lab email address and password:

Email address format: aristarockies##+pod##@gmail.com

The image shows the ARISTA WiFi Customer Login screen. It has a light gray background with a white central box. At the top of the box is the ARISTA logo (a blue circle with a white 'A'). Below the logo is the text "ARISTA" and "WiFi Customer Login". There are two text input fields: the first contains the email address "aristarockies##+pod##@gmail.com" and the second contains a masked password ".....". Below the input fields is a blue button labeled "Sign In". At the bottom of the box are two links: "Federated Login" and "Forgot your password?".

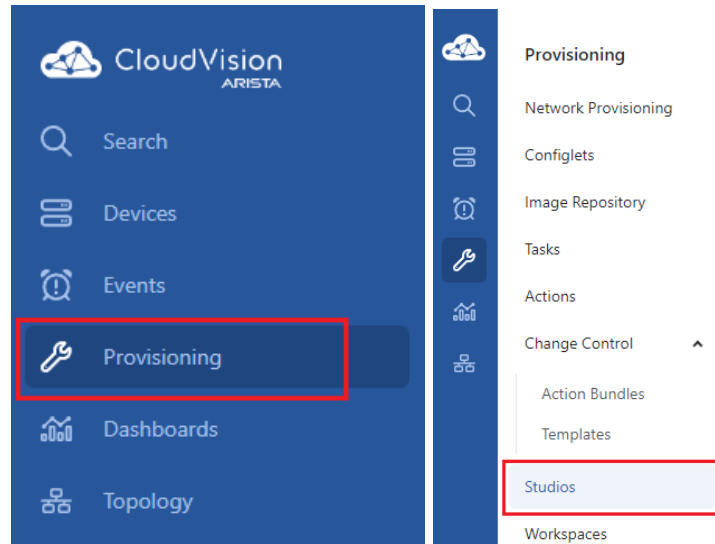
You will now be logged into CloudVision.



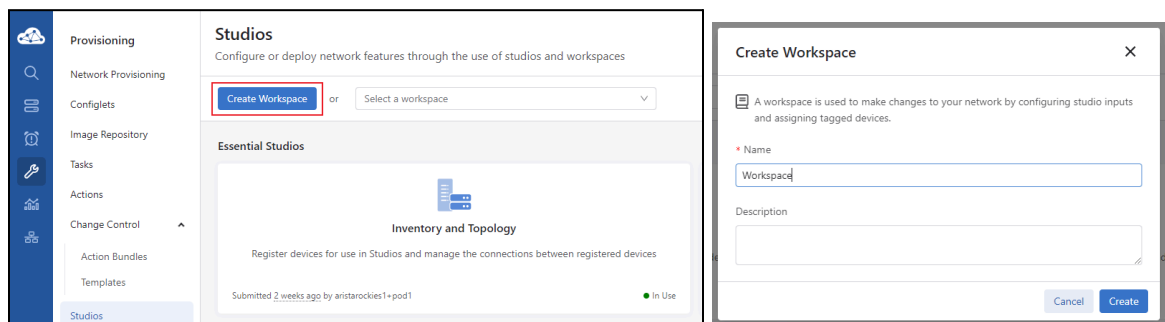
2. Enable RadSec on campus-pod<xx>-leaf1c

In this lab you will be configuring RadSec on the campus-podXX-leaf1c switches by adding the RadSec configuration to the leaf1c switches via the Static Configuration Studio.

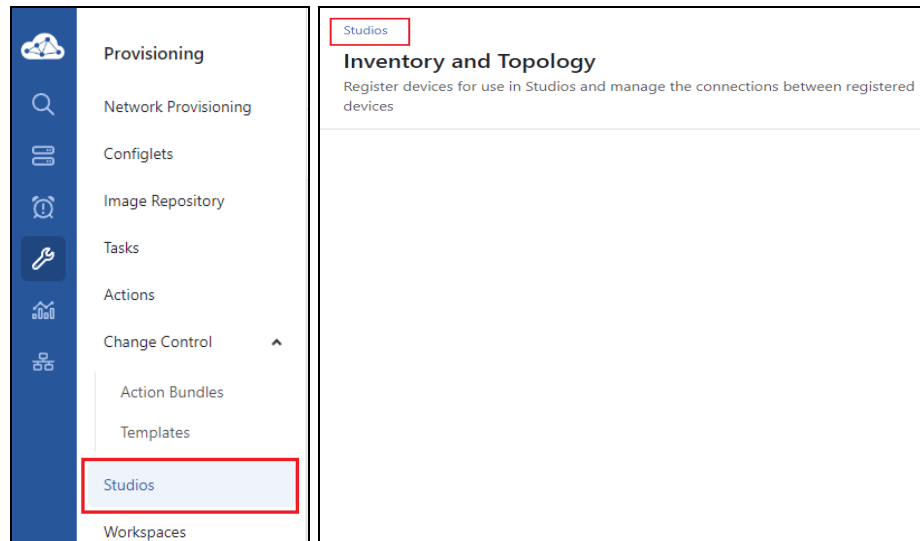
1. Login to CloudVision, then click on the “**Provisioning**” menu option, then choose “**Studios**”.



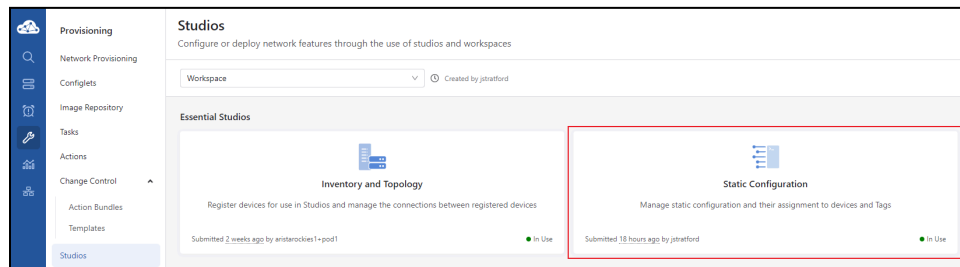
2. Create a workspace to propose changes to the Network Infrastructure. A workspace acts as a sandbox where you can stage your configuration changes before deploying them. Click “**Create a Workspace**”, give it any name you would like and click “**Create**”.



3. Apply the static configuration to the campus-podXX-leaf1c switch using Static Configuration Studio
Click on **Studios** at the Top OR Left side navigation pane



Launch the Static Configuration Studios



Expand the Device Container Tree and select the **“Three Dots”** and select **“Add Device”**.

Container Tree ⓘ

Manage the container hierarchy and the device tags and configlets assigned to containers.



Static Configuration

+ Add

▼ Device




campus-pod03-leaf1a

campus-pod03-leaf1b

 Rename

 Add Sub Container

 Add Device

 Delete

Select the radial button next to “**campus-pod<xx>-leaf1c**” and select “**Add**”

Add Devices device:*

Devices

Add devices to the tag assigned to the selected container.

Device

Device ID

campus-pod03-leaf1a

Tagged

WTW23490505

campus-pod03-leaf1b

Tagged

WTW22200349

campus-pod03-leaf1c

Tagged

WTW22210161

Container Hierarchy

Add the devices to tags of parent containers to support the hierarchy of inheritance.

device:*

Tag matches all devices

Summary of Changes

Tags:

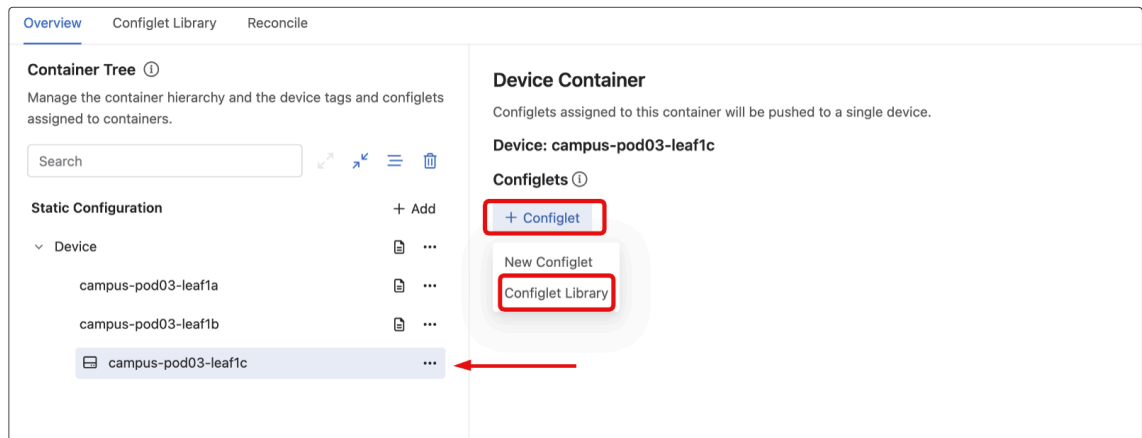
Will be added to 1 device

A new container will be created for each device, which allows you

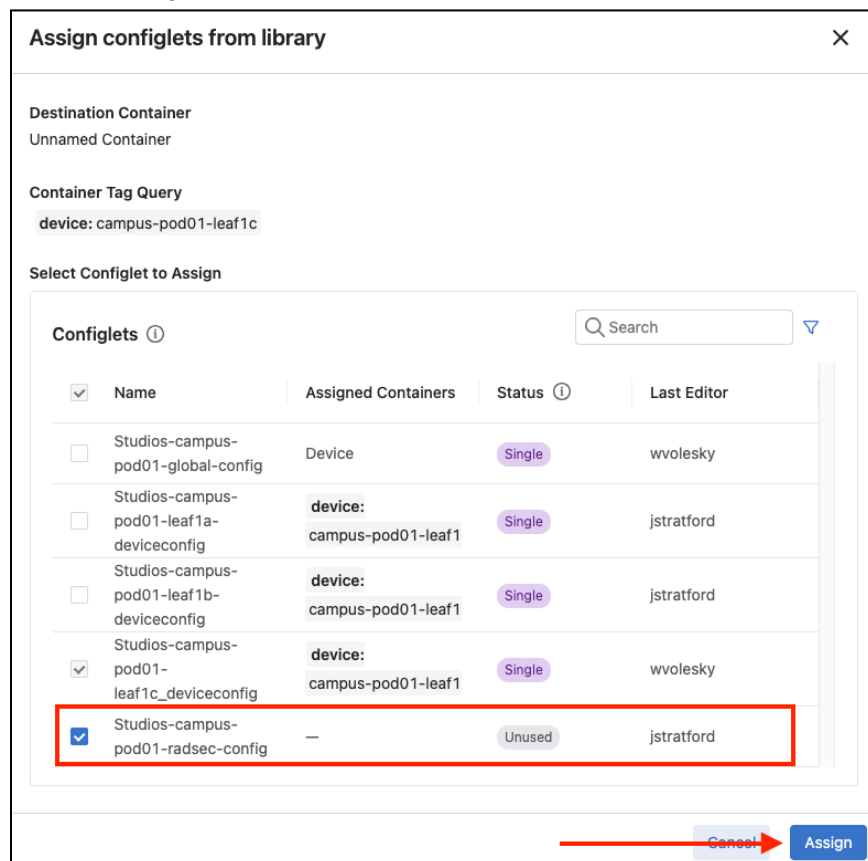
Cancel

Add

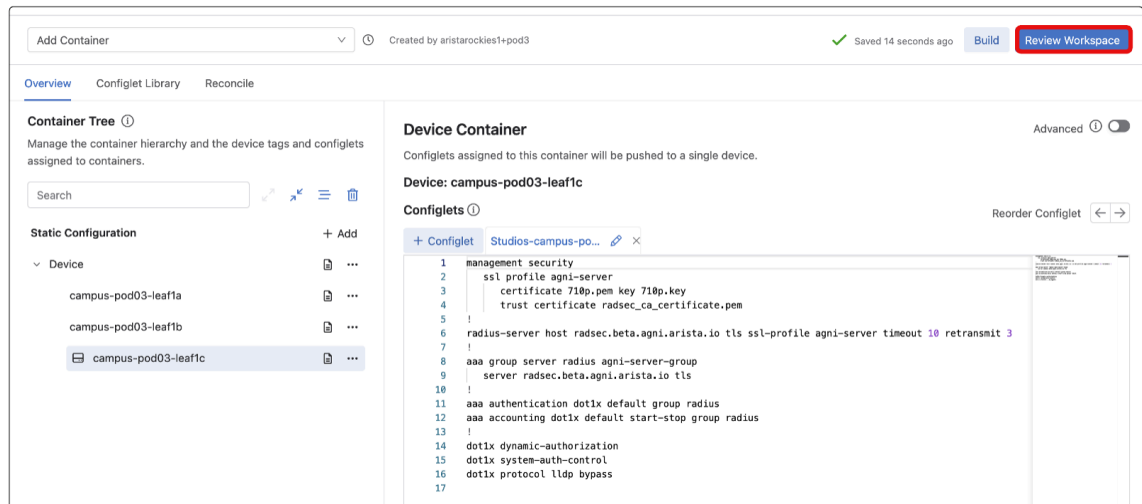
In the Device Container window, click on “+ Configlet” followed by “Configlet Library”.



Select the Configlet named “Studios-campus-pod<xx>-radsec-config” and click Assign to add the configlet to the “campus-pod<xx>-leaf1c” switch.



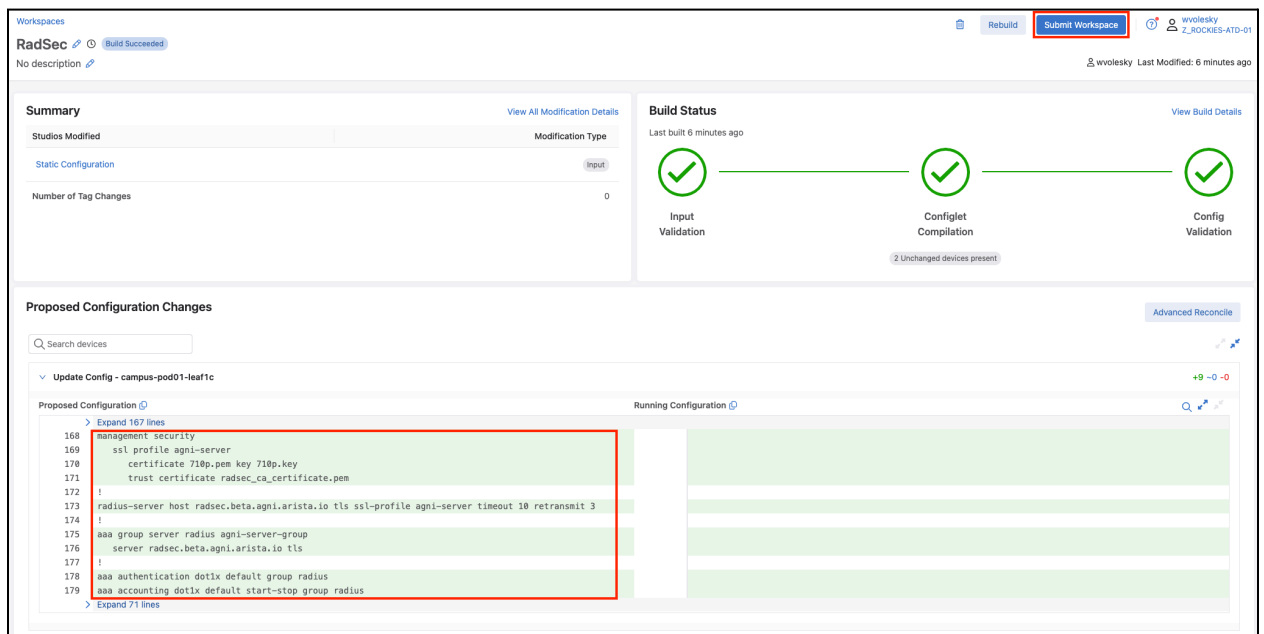
Click **Review Workspace** to review all the changes proposed to the CloudVision Studio



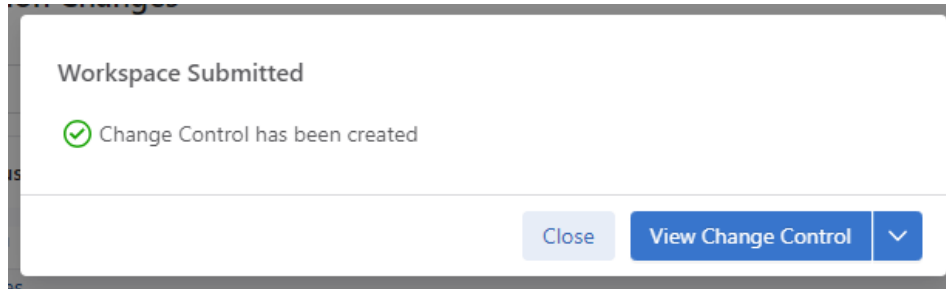
4. Review and Submit the Workspace

Review the workspace details showing the summary of modified studios, the build status, and the proposed configuration changes for each device.

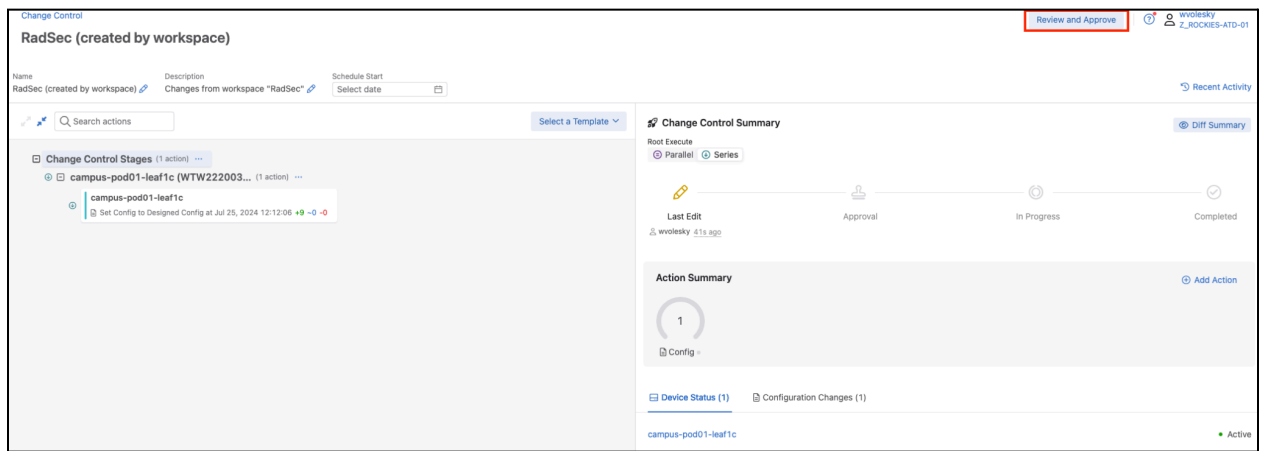
Click **“Submit Workspace”**



Click **“View Change Control”**



- Review, Approve and Execute the Change Control to apply the configuration changes
Click “Review and Approve”



Select “Execute immediately” and click “Approve and Execute”



- The change control will execute and apply all the RadSec configuration changes to the device. This will enable RadSec connectivity between the campus-pod<xx>-leaf1c switch and AGNI.

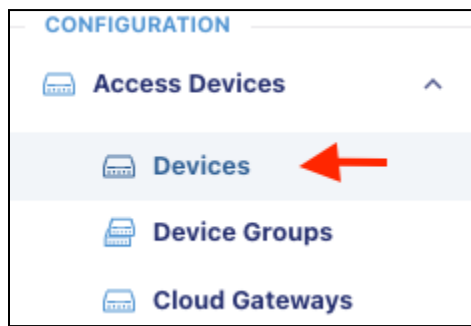
***Note:** The switch device certificate and the AGNI RadSec root certificate have already been provisioned on the switch.

See Section B. Configuring RadSec profile in EOS for additional information.

3. Access AGNI from the LaunchPad.



Click on **Access Devices - Devices** to confirm the RadSec connection is up.

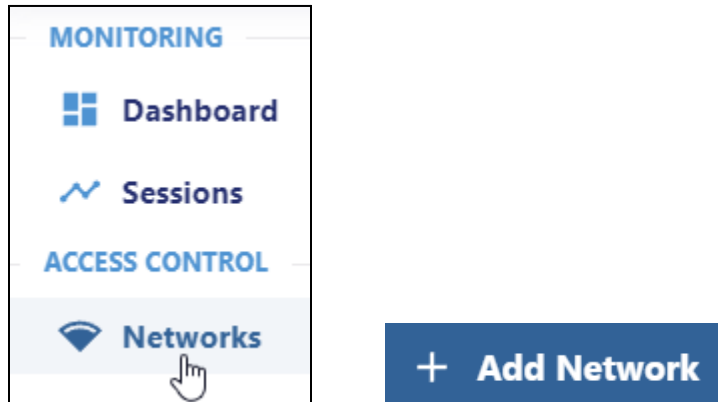


<input type="checkbox"/>	#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS
<input type="checkbox"/>	1	campus-pod01-leaf1c.cam...	2c:dd:e9:fd:84:90	Arista Switch	Arista CloudVision/Tenant/Undefined	●
<input type="checkbox"/>	2	POD-01-FL1	30:86:2d:30:42:2f	Arista WiFi	Locations/Corp/1st Floor	●

4. Create Wired EAP-TLS Network and Segment

In this section we will create a Network and Segment in Cloudvision AGNI to utilize a certificate based TLS authentication method on a wired connection with a Raspberry Pi.

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



Fill in and select the Following fields on the “Add Network” page.

Name: **Wired-EAP-TLS**

Connection Type: **Wired**

Access Device Group: **Switches**

Status: **enabled**


Authentication type: **Client Certificate (Eap-TLS)**

Fallback to mac Authentication: **Enabled**

MAC Authentication Type: **Allow Registered Clients Only**

Onboarding: **Enabled**

Authorized User Groups: **Employees**



Add Network

Provide the following details to add a new Network

[< Back](#)

Name

Wired-EAP-TLS

Connection Type:

☐ Wireless

☒ Wired

Access Device Group

Switches

✕

+

Select an Access Device Group to make this Network only applicable to a subset of Access Devices. Multiple Networks can't be linked to the same Access Device Group.

Status:

Enabled

☒

Authentication


Authentication Type

Client Certificate (EAP-TLS)

Domain Machine Authentication:

Disabled

☐




Enable to allow machine authentication with domain machine certificates.

Trust External Certificates

Disabled

☐



Enable this setting to accept client certificates issued by external CAs.

Fallback To MAC Authentication

Enabled

☒


MAC Authentication Type

Allow Registered Clients Only

Disallow user associated clients:

Disabled

☐



Enable to disallow user associated clients on this network.

Onboarding

Enabled

☒

Authorized User Groups

Employees ✕ Select Authorized User Groups...

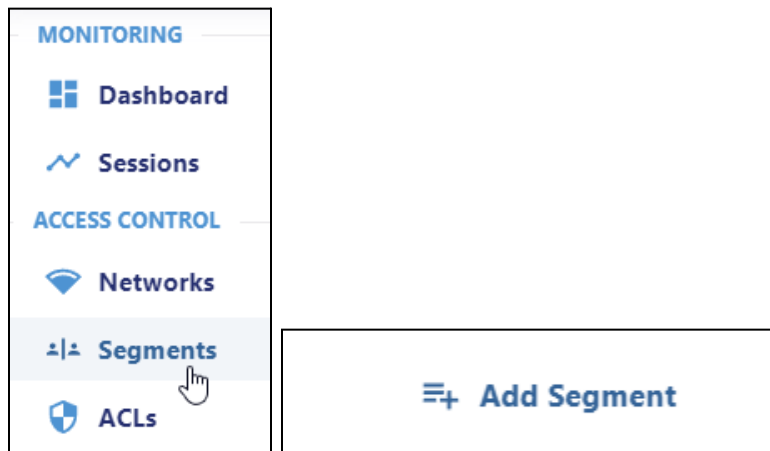
Cancel

Add Network

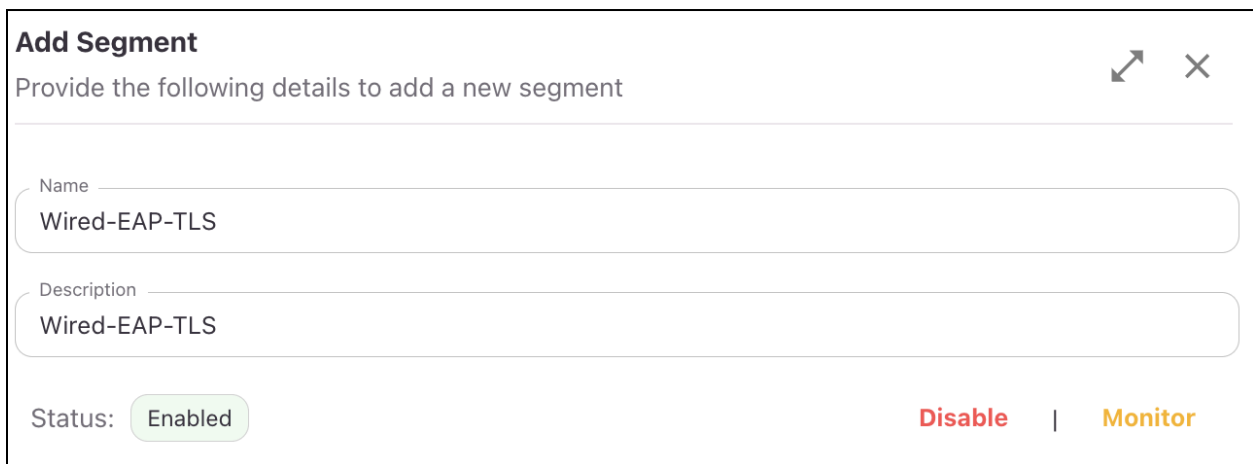
A dark blue rounded rectangular button with the text "Add Network" in white. A hand cursor is pointing at the bottom right corner of the button.

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

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



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

A form titled "Add Segment" with a subtitle "Provide the following details to add a new segment". It has two input fields: "Name" and "Description", both containing the text "Wired-EAP-TLS". At the bottom, there is a "Status:" label followed by a green "Enabled" button, and two links: "Disable" in red and "Monitor" in orange.

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

Add Condition

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

Network: Name

is

Wired-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

is

Client Certificate (EAP-TLS)

Your Conditions should now look like this.

Conditions MATCHES ALL

Network: Name

is

Wired-EAP-TLS

×

Network: Authentication Type

is


Client Certificate (EAP-TLS)

×

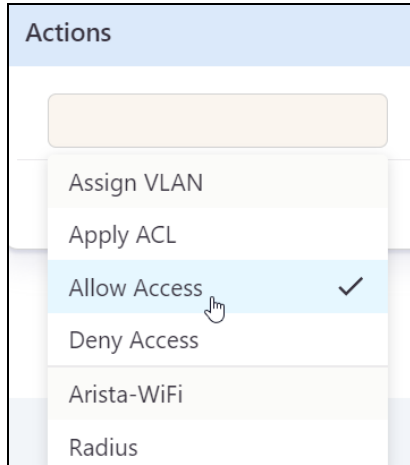
 Add Condition

Under Actions select **Add Action**.

Actions

 Add Action

Select Allow Access.



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

A screenshot of the 'Add Segment' form. The form has a title 'Add Segment' and a subtitle 'Provide the following details to add a new segment'. It contains several input fields: 'Name' with the value 'Wired-EAP-TLS' and 'Description' with the value 'Wired-EAP-TLS'. Below these is a 'Status' section with a green 'Enabled' button and red 'Disable' and 'Monitor' buttons. The 'Conditions' section is titled 'MATCHES ALL' and contains two conditions: 'Network: Name is Wired-EAP-TLS' and 'Network: Authentication Type is Client Certificate (EAP-TLS)'. Below the conditions is an 'Add Condition' button. The 'Actions' section is titled 'Actions' and contains one action: 'Allow Access Allow default access'. Below the actions is an 'Add Action' button. At the bottom of the form are 'Cancel' and 'Add Segment' buttons. The 'Add Segment' button is highlighted with a red border.

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

Wired-EAP-TLS

Conditions

Network:Name is Wired-EAP-TLS

Network:AuthType is Client Certificate (EAP-TLS)

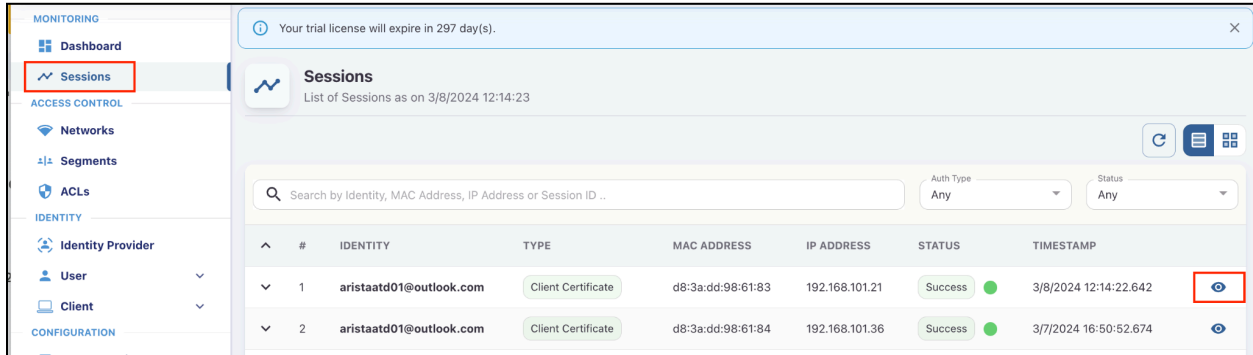
Actions

Allow Access

Next, unplug and plug your raspberry Pi into port 2 on the switch and click on **Sessions** to see if your ATD Raspberry Pi has a connection via the Wired connection. ***Note:** The Client Certificate has already been applied to the Raspberry Pi.

5. Validate and Verify Wired EAP-TLS Device

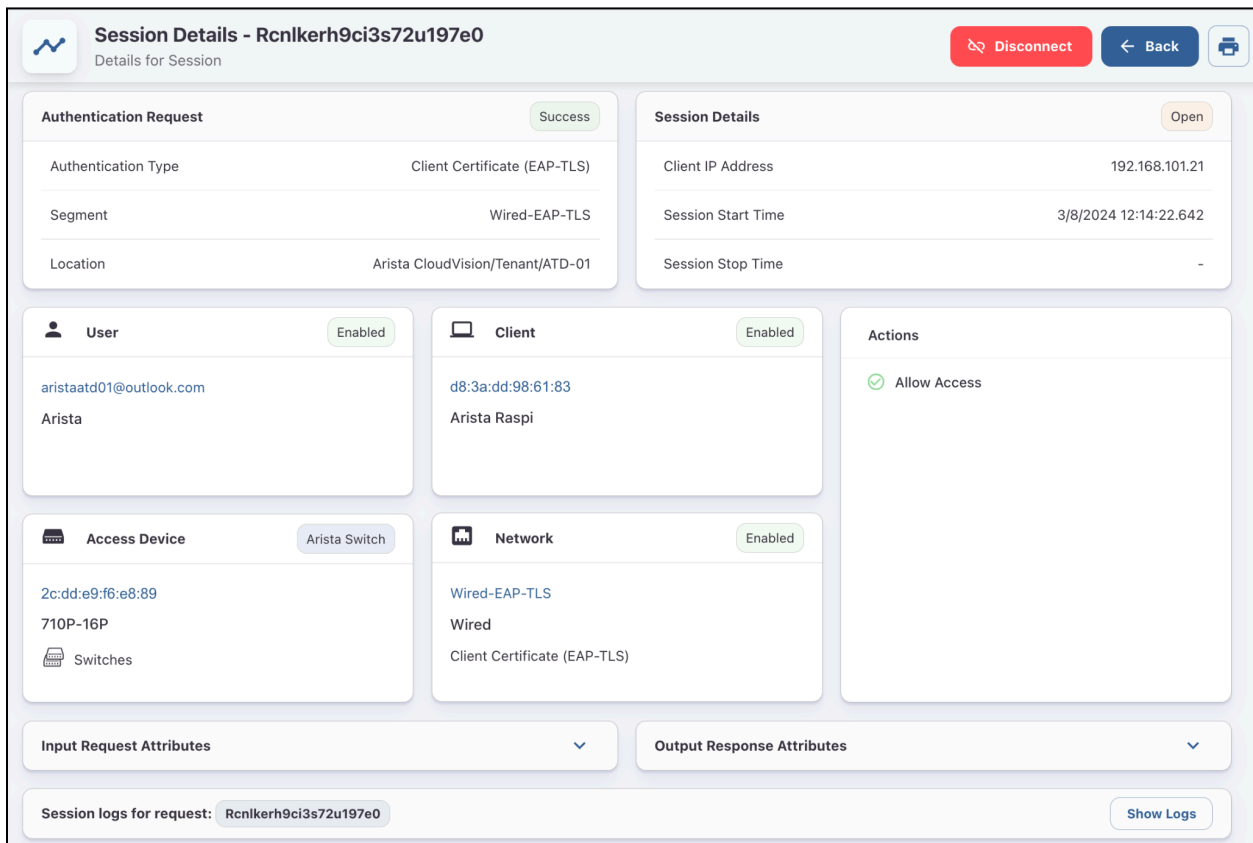
Once the device is connected you will be able to view the status of the connection and additional session details if you click on the Eye to the right of the device.



The screenshot shows the AGNI interface with the 'Sessions' tab selected in the left sidebar. The main area displays a table of sessions. The first session is highlighted, and an eye icon is visible in the rightmost column, indicating that session details can be viewed.

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	aristaatd01@outlook.com	Client Certificate	d8:3a:dd:98:61:83	192.168.101.21	Success	3/8/2024 12:14:22.642
2	aristaatd01@outlook.com	Client Certificate	d8:3a:dd:98:61:84	192.168.101.36	Success	3/7/2024 16:50:52.674

AGNI will then display more in depth session information regarding the device and connection.



The screenshot shows the 'Session Details' page for a specific session. The page is divided into several sections providing detailed information about the session, including authentication request details, session details, user and client information, access device, network, and actions.

Session Details - Rcnlkerh9ci3s72u197e0

Details for Session

Authentication Request (Success)

- Authentication Type: Client Certificate (EAP-TLS)
- Segment: Wired-EAP-TLS
- Location: Arista CloudVision/Tenant/ATD-01

Session Details (Open)

- Client IP Address: 192.168.101.21
- Session Start Time: 3/8/2024 12:14:22.642
- Session Stop Time: -

User (Enabled)

- aristaatd01@outlook.com
- Arista

Client (Enabled)

- d8:3a:dd:98:61:83
- Arista Raspi

Access Device (Arista Switch)

- 2c:dd:e9:f6:e8:89
- 710P-16P
- Switches

Network (Enabled)

- Wired-EAP-TLS
- Wired
- Client Certificate (EAP-TLS)

Actions

- Allow Access

Input Request Attributes

Output Response Attributes

Session logs for request: Rcnlkerh9ci3s72u197e0

Show Logs

You can also validate the session on the switch by issuing the following commands in the switch CLI

```
710P-16P#show dot1x host
```

Port	Supplicant MAC	Auth State	Fallback	VLAN
Et2	d83a.dd98.6183	EAPOL SUCCESS	NONE	

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: 1x00000004

Captive portal:

AAA Server Returned:

Arista-WebAuth:

Class: Rcnlkerh9ci3s72u197e0|C4151a596-baab-444b-a4fd-ad40946d8b5f

Filter-Id:

Framed-IP-Address: 192.168.101.21 sourceArp

NAS-Filter-Rule:

Service-Type: None

Session-Timeout: 86400 seconds

Termination-Action: RADIUS-REQUEST

Tunnel-Private-GroupId:

Arista-PeriodicIdentity:

NAC LAB #3 COMPLETE

Additional Information

A. 802.1x High-Level Overview

For more information please refer to the TOI. [802.1X on Arista Switches](#)

Overview

802.1X is an IEEE standard protocol that prevents unauthorized devices from gaining access to the network.

802.1X defines three device roles:

- Supplicant (client)
- Authenticator (switch)
- Authentication server (RADIUS)

Before authentication is successful the switchport is in unauthorized mode and all traffic is blocked, but after authentication has succeeded, normal data can then flow through the switchport.

Description

802.1X port security controls who can send traffic through and receive traffic from individual switch ports. A supplicant needs to authenticate itself using “**Extensible Authentication Protocol over Lan**” (EAPoL) packets with the switch before it gains full access to the port. Arista switches act as an authenticator, passing the messages from 802.1X supplicants through to the RADIUS server and vice versa. 802.1X can operate in three different modes:

- Single Host Mode: Once the 802.1X supplicant is authenticated on the port, ONLY the traffic coming from the supplicant's MAC is allowed through the port.
- Multi-Host Mode: Once the 802.1X supplicant is authenticated on the port, traffic coming from ANY source MAC is allowed through the port.
- Multi-Host authenticated Mode: Multiple 802.1X supplicants can be allowed and ONLY the traffic coming from all authenticated supplicant's MAC is allowed through the port.

Single Host and Multi Host modes allow only one 802.1X supplicant to be authenticated for one port. Once it is successfully authenticated, no other 802.1X supplicant can be authenticated unless the current one logs off, but Multi-Host authenticated Mode allows multiple 802.1X supplicants simultaneously to be authenticated and provided access to the network. From

release 4.28.2F, one supplicant can replace another supplicant's session in single-host mode. For more details on the session replace configuration, please see [here](#)

Apart from 802.1X authentication, Arista switches also support MAC-Based Authentication (MBA) which allows devices not speaking 802.1X to have access to the network. By default the authenticator uses the non delimited MAC address(i.e. 001c73ff9b11) of such devices as the username/password in its RADIUS request packets. Depending on the MAC-Based Authentication configuration on the RADIUS server, it decides whether to authenticate the supplicant or not. Unlike 802.1X supplicants, multiple MBA supplicants can be allowed on a single port (irrespective of 802.1X mode). The MBA configuration is independent of the 802.1X host modes. MBA supplicants will not be considered to allow or reject unauthenticated traffic based on the host mode.

***Note:** From release 4.25.1F MBA supplicants can be controlled by Dot1x Host modes, for more details please refer [here](#).

Arista switches also support Dynamic VLAN assignment, which allows the RADIUS server to indicate the desired VLAN for the supplicant using the tunnel attributes with the Access-Accept message ("**Tunnel-Private-Group-ID**" in <https://tools.ietf.org/html/rfc2868>). Both 802.1X and MBA supplicants can be assigned a VLAN via the RADIUS server using this feature. It should be noted that only one VLAN per port is supported for platforms that do not support "**MAC based VLAN assignment**". On these platforms when the first host authenticates, the authenticator port is put in the respective VLAN (via dynamic VLAN assignment) and subsequently, all other hosts must belong to that VLAN as well. For details about which platforms support "**MAC Based VLAN Assignment**", please refer to the table in the "**Platform Compatibility**" paragraph.

802.1X features are supported on 802.1Q trunk ports allowing the user to have Port-Based Network Access Control (PNAC) on such a port. With this feature, traffic coming into an 802.1X enabled port with a VLAN tag can also be authenticated via both 802.1X or MBA.

By default, traffic from any unauthenticated device on an 802.1X enabled port is dropped. By configuring Authentication Failure VLAN on the authenticator switch, 802.1X or MBA supplicants' traffic can be put into a specific VLAN if the supplicant fails to authenticate via the RADIUS server.

B. Configuring RadSec profile in EOS

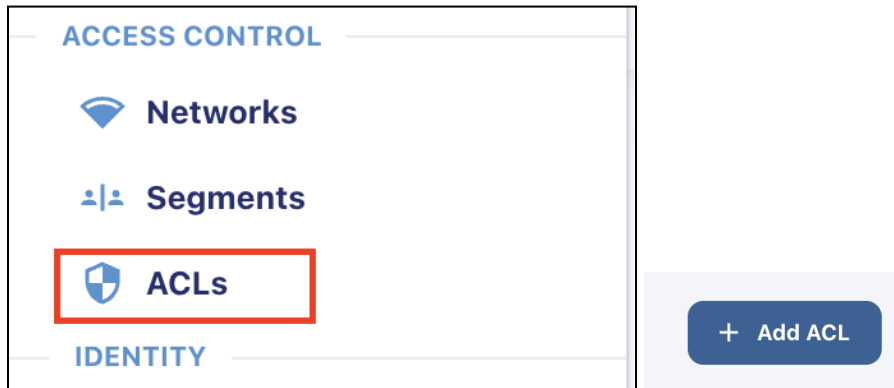
Reference the following article to Configure the RadSec profile in EOS:

<https://arista.my.site.com/AristaCommunity/s/article/Configuring-RadSec-profile-in-EOS>

C. Adding Access Control Lists for Wired Users


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
```



Add ACL

Provide the following details to add a new ACL

← Back

Name

Guest Access

Description

Guest Access

Type

Standard ACL

ACL


Add/Edit ACE entries according to [standard](#) format [Page 45] Show Sample

```
#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
```

Cancel

Add ACL

It should now show in the Access Control list



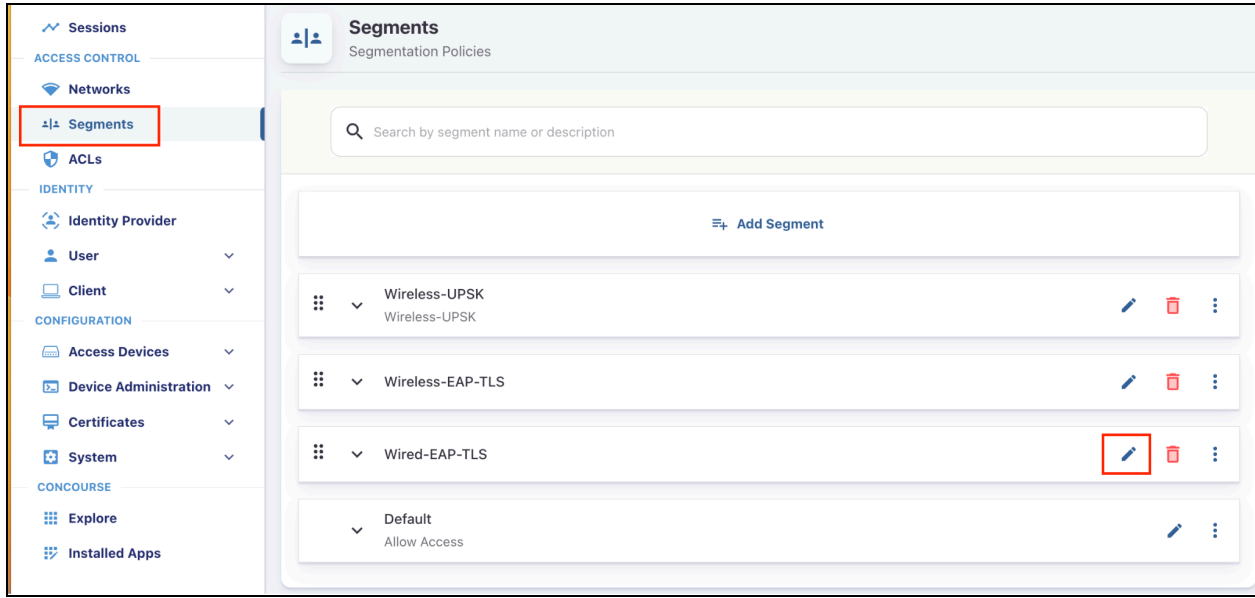
Access Control List

Manage the list of ACLs

Search by name or description ...

#	NAME	DESCRIPTION	TYPE
1	Guest Access	Guest Access	Standard ACL

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**”

Name
Wired-EAP-TLS

Description

Status: Enabled Disable | Monitor

Conditions MATCHES ALL

Network: Name is Wired-EAP-TLS

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

[Add Condition](#)

Actions

Allow Access Allow default access

Apply ACL Apply ACL through RADIUS response

Standard ACL Guest Access

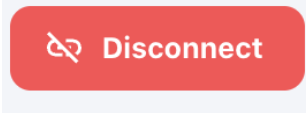
[Add Action](#)

[Cancel](#) [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.

MONITORING						
Dashboard						
Sessions						
1	aristaatd01@outlook.com	Client Certificate	d8:3a:dd:98:61:83	192.168.101.21	Success	3/14/2024 10:25:07.146


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

▼	1	aristaatd01@outlook.com	Client Certificate	d8:3a:dd:98:61:83	192.168.101.21	Success	3/14/2024 11:03:27.706	
▼	2	aristaatd01@outlook.com	Client Certificate	d8:3a:dd:98:61:83	192.168.101.21	Success	3/14/2024 10:25:07.146	

Actions

 Allow Access

 Apply ACL

Standard ACL = Guest Access

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: Rcnpgghgo78m8s712rvjbg|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.