

Campus A-02 Wired Lab Guide

Access Interface Configuration



This Lab Guide:

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

Table of Contents

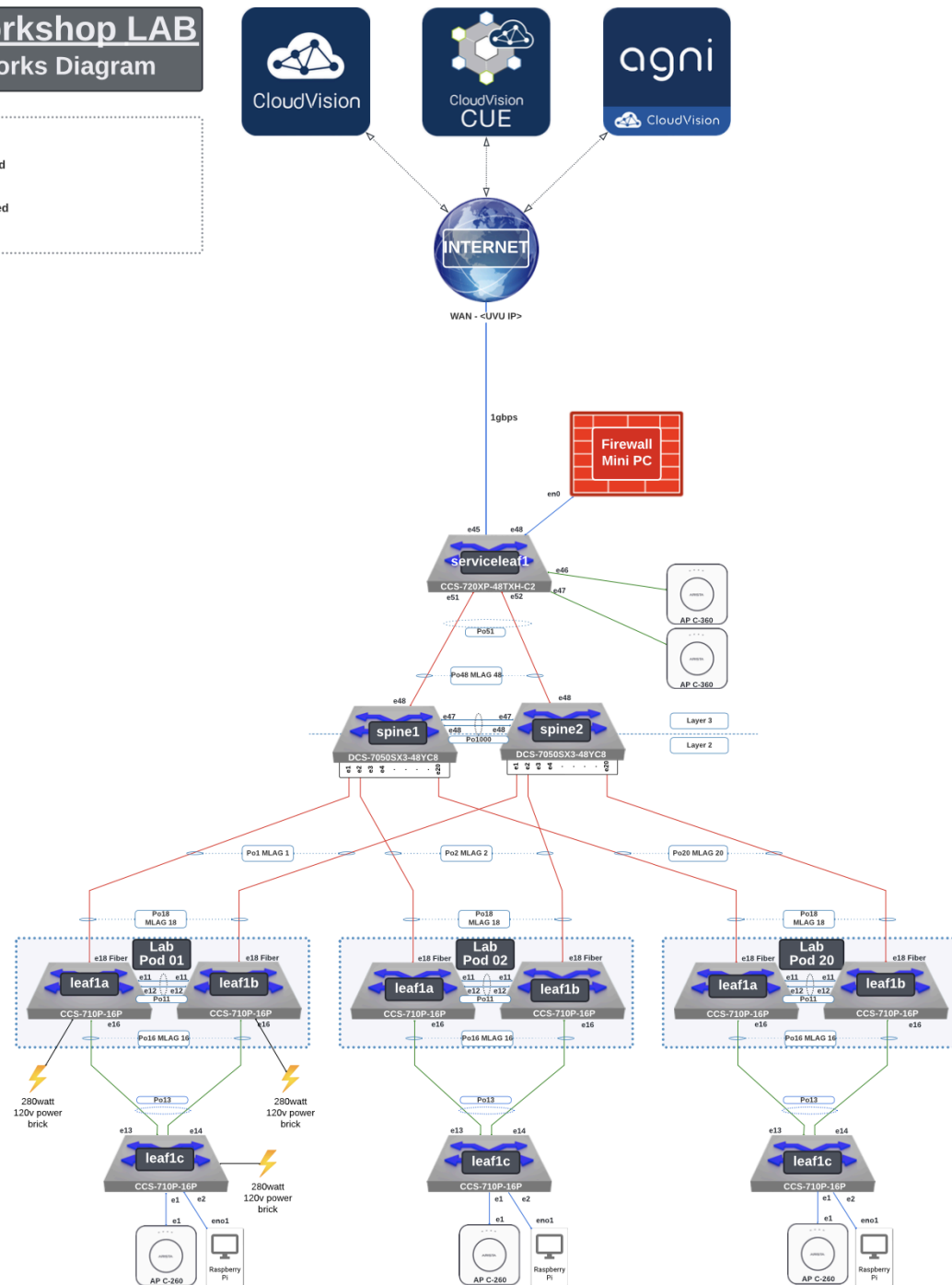
Full Lab Topology.....	3
POD Topology.....	4
1. Accessing CloudVision as a Service.....	5
2. Creating Port Profiles.....	7
3. Assigning Port Profiles for AP and RPI.....	13

Full Lab Topology

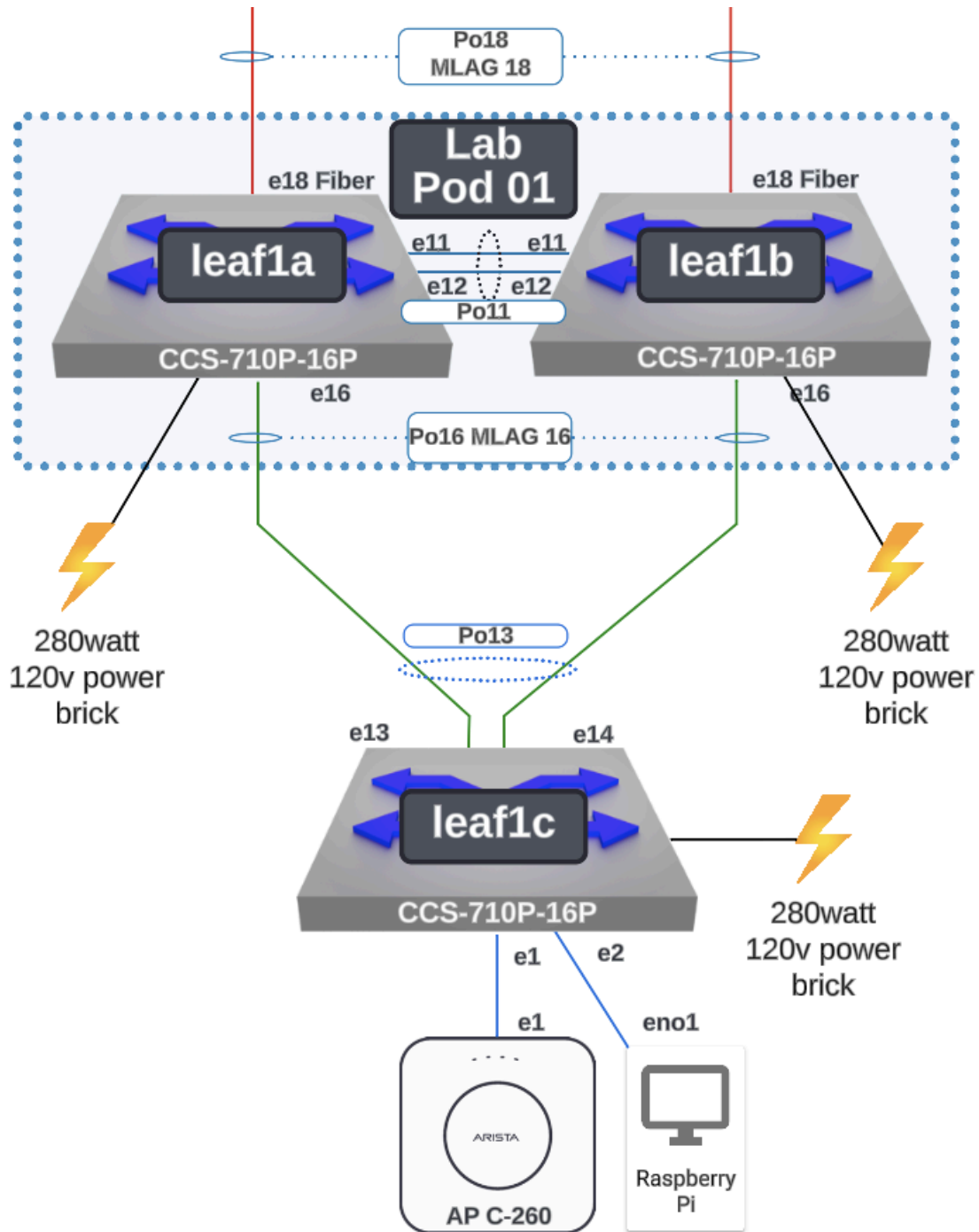
Arista Workshop LAB Lab Networks Diagram

Key:

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



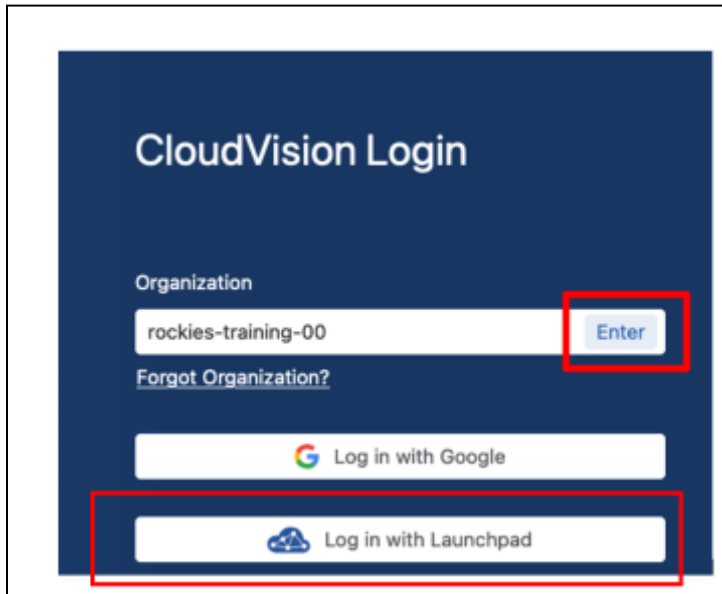
POD Topology



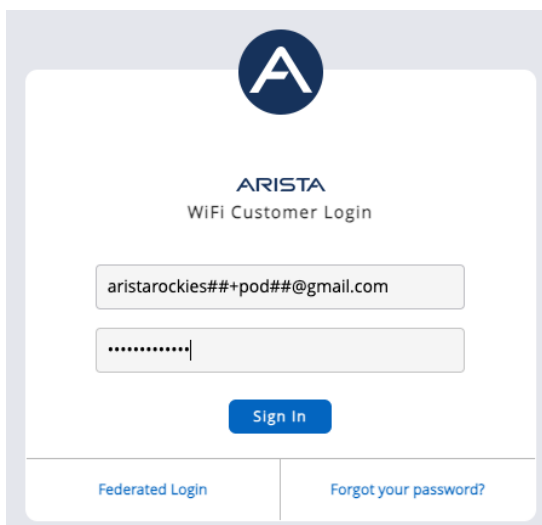
1. Accessing CloudVision as a Service

In your Google Chrome browser, enter the following URL: <https://www.arista.io/> to access CloudVision as a Service (CVaaS).

1. in the “**Organization**” box enter the Organization name “**rockies-training-##**” where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod, then click “**Enter**”.

The image shows the CloudVision Login interface. It has a dark blue background with the title "CloudVision Login" at the top. Below the title is an "Organization" input field containing the text "rockies-training-00". To the right of this field is a blue button labeled "Enter", which is highlighted with a red rectangular box. Below the input field is a link that says "Forgot Organization?". Further down are two login options: "Log in with Google" with the Google logo and "Log in with Launchpad" with the Launchpad logo. The "Log in with Launchpad" button is also highlighted with a red rectangular box.

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

The image shows the ARISTA WiFi Customer Login screen. At the top is the ARISTA logo, a stylized 'A' inside a circle. Below the logo is the text "ARISTA WiFi Customer Login". There are two input fields: the first contains the email address "aristarockies##+pod##@gmail.com" and the second is a password field with dots. Below these fields is a blue "Sign In" button. At the bottom of the form are two links: "Federated Login" and "Forgot your password?".

3. You will now be logged into CloudVision

Search

Home

Inventory

Alerts

Tools

Reports

Settings

Campus Health Overview

Aug 9, 2024 10:32:28 (1 hour)

aristaros1+pod13
rockies...ining-13

[View in Network Inventory](#)

No data to display

[View in Endpoint Overview](#)

No data to display

Connectivity Monitor Anomalies

No Monitoring Set Up

[Connectivity Monitor Studio >](#)

Network Topology

[View cluster in Topology](#)

Events

0

0

3

CVE Threat Exposure 2d ago

campus-pod13-leaf1c

CVE Threat Exposure 1w ago

campus-pod13-leaf1a

CVE Threat Exposure 1w ago

campus-pod13-leaf1b

[View in Events](#)

Quick Actions

[Access Interface Configuration](#)
Access Interface Configuration

[Interface Diagnostics](#)
Run Interface Diagnostics

Top Flows by Source

Source	Flow
uslax1-vip-bx-004.aaplimg.com	2G
10.0.113.42	0.5G
lax31s16-in-f1.1e100.net	0.2G

Top Flows by Destination

Destination	Flow
10.0.113.42	2.5G
lax17s55-in-f10.1e100.net	0.5G
lax31s16-in-f14.1e100.net	0.2G

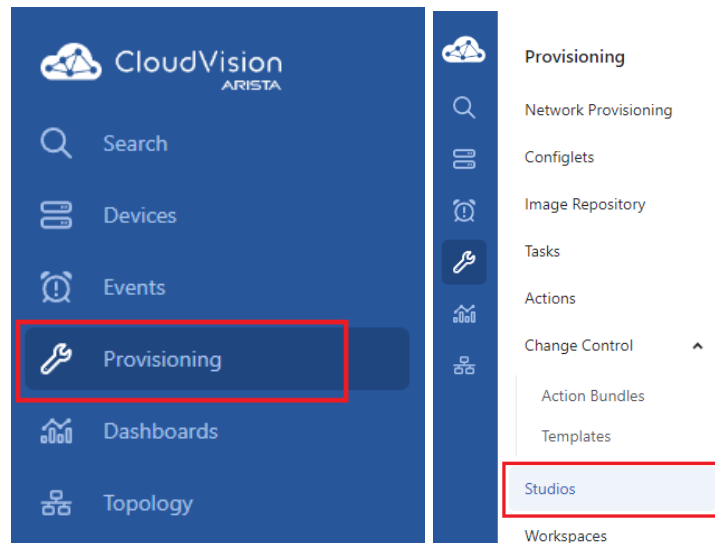
Compliance Issues

Bug Exposure	3
CVE Threats	3
Configuration	0
Image	0
End of life: Software	0
End of life: Hardware	0

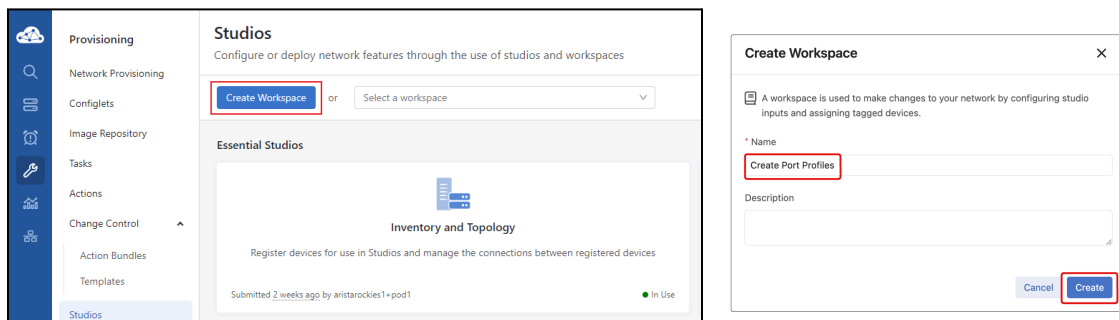
2. Creating Port Profiles

This lab will help you create port profiles and apply them to interfaces in your ATD network.

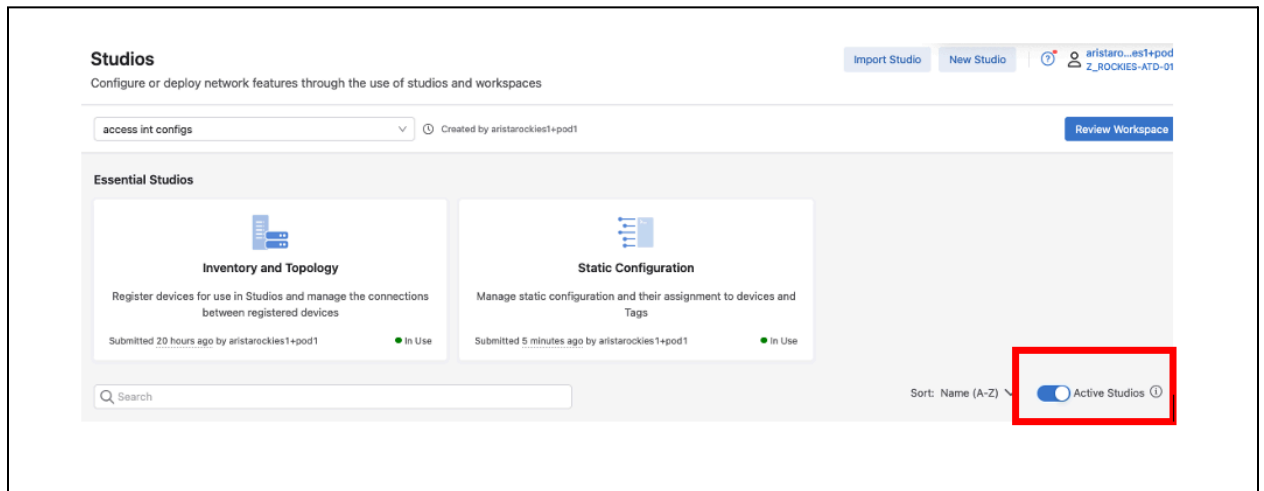
1. Click on the **Provisioning** menu option, then choose **Studios**



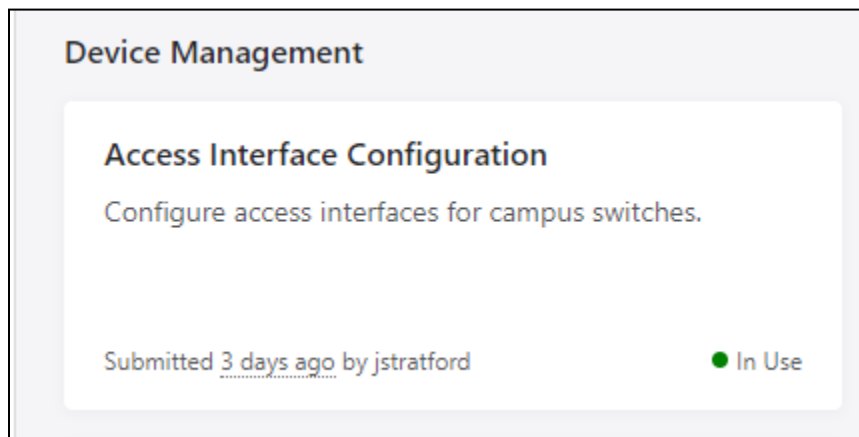
2. Click **Create Workspace** and name it **Create Port Profiles** then select **Create**. A workspace acts as a sandbox where you can stage your configuration changes before deploying them



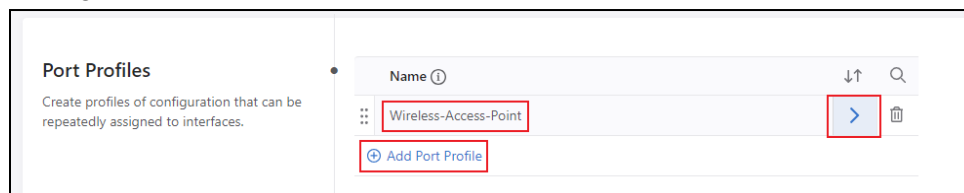
3. Disable the **Active Studios** toggle to display all available CloudVision Studios (which when enabled will only show used/active Studios). ***Note:- the toggle may already be in the disabled position.**



4. Create two port profiles using the **Access Interface Configuration** studio that will be used to provision connected hosts.
- a. Launch the **Access Interface Configuration**



- b. Click **Add Port Profile**, name it **“Wireless-Access-Point”**, and click the arrow on the right



- c. Enter the following values on this configuration page
- Description: **“Wireless-Access-Point”**
 - Enabled: **Yes**

Configuration for
Wireless-Access-Point

Parent Profile

Use and modify the configuration of another profile. All blank inputs will use the configuration of the parent profile.

Parent Profile ⓘ

Description

Description to be used on all ports.

Description ⓘ

Enabled

Administrative state, setting to "No" will set the port to "shutdown" in the intended configuration.

Enabled ⓘ

- iii. Mode: **Access**
- iv. VLANs: "1##" where ## is a 2 digit character between 01-20 that was assigned to your lab/Pod. e.g Pod01 is VLAN101, Pod13 is VLAN113
- v. POE:
 1. Reboot Action: **Maintain**
 2. Link Down Action: **Maintain**
 3. Shutdown Action: **Maintain**

Mode

Interface mode

Mode ⓘ

VLANs

VLANs ⓘ

Spanning Tree

Portfast

BPDU Filter

BPDU Guard

802.1X

Enabled

POE

Power Over Ethernet settings applied on port. Only configured if the platform supports PoE.

Priority ⓘ

Reboot Action ⓘ

Link Down Action ⓘ

Shutdown Action ⓘ

- d. Navigate back to **Access interface Configuration** by clicking on the top

Access Interface Configuration

Wireless-Access-Point

Configuration for

Wireless-Access-Point

- e. Click **Add Port Profile**, name it **“Wired-RasPI”**, and click the arrow on the right

- f. Enter the following values on this configuration page

- Description: **“Wired-RasPI”**
- Enabled: **Yes**

- iii. Mode: **Access**
- iv. VLANs: “**1##**” where **##** is a 2 digit character between 01-20 that was assigned to your lab/Pod. e.g Pod01 is VLAN101, Pod13 is VLAN113
- v. 802.1X: Enabled = **Yes**
- vi. Click **MAC Based Authentication**

Mode
Interface mode.
access

VLANs
VLANs
108

Spanning Tree
Portfast
Select
BPDU Filter
Select
BPDU Guard
Select

802.1X
Enabled
Yes
Port Control
auto
Port Control Force Authorized Phone
Select
Reauthentication
Select
PAE
PAE
Authentication Failure
Authentication Failure
Host Mode
Host Mode
MAC Based Authentication
MAC Based Authentication
Unauthorized
Unauthorized
Timeouts
Timeouts

- vii. Set Enabled:**Yes**
 - 1. Navigate back to the previous page

Access Interface Configuration / Wired-RasPI / 802.1X / MAC Based Authentication

Enabled
Enabled
Yes
Always
Always
Select

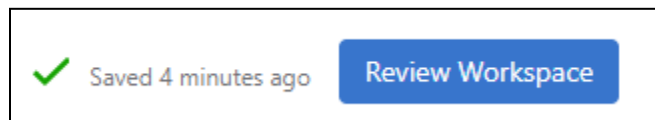
viii. **POE:**

1. Reboot Action: **Maintain**
2. Link Down Action: **Maintain**
3. Shutdown Action: **Maintain**

POE Power Over Ethernet settings applied on port. Only configured if the platform supports PoE.	• Priority ⓘ	Reboot Action ⓘ	Link Down Action ⓘ	Shutdown Action ⓘ
	Select ▼	maintain ▼	maintain ▼	maintain ▼

5. Review and Submit the Workspace

- i. Click **Review Workspace**



- ii. Note that none of the device configurations have been changed after submitting this workspace

Workspaces

Workspace ⓘ ⓘ Build Succeeded

No description ⓘ

Rebuild

Submit Workspace

ⓘ jstratford
Z_ROCKIES-ATD-01

ⓘ jstratford Last Modified: 28 seconds ago

Summary

View All Modification Details

Studios Modified	Modification Type
Access Interface Configuration	Input
Number of Tag Changes	
0	

Build Status

View Build Details

Last built 26 seconds ago

✓

Input Validation

✓

Configlet Compilation

✓

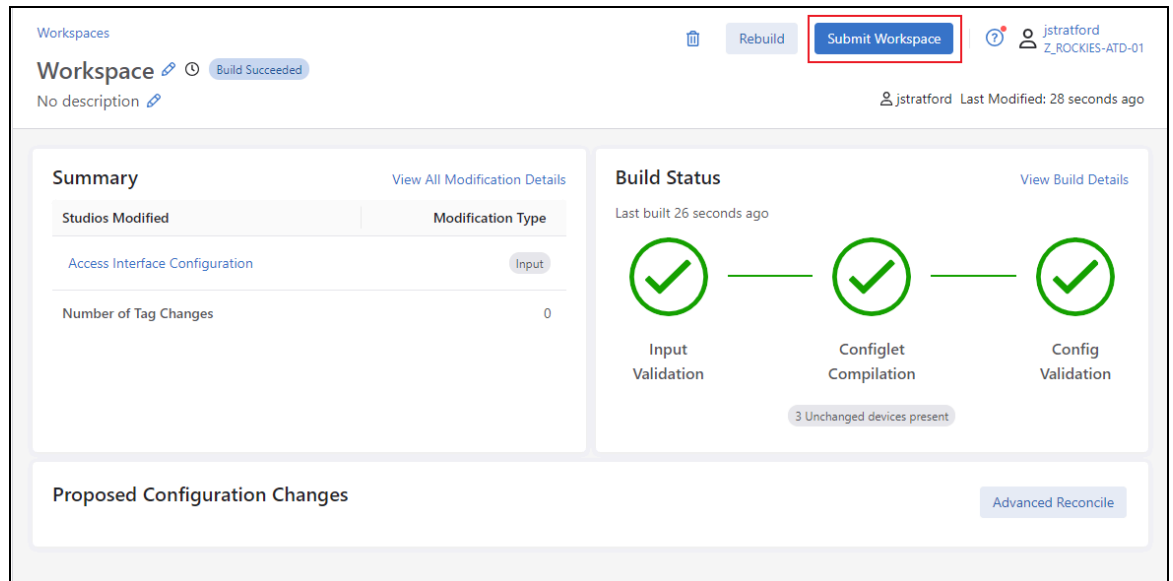
Config Validation

3 Unchanged devices present

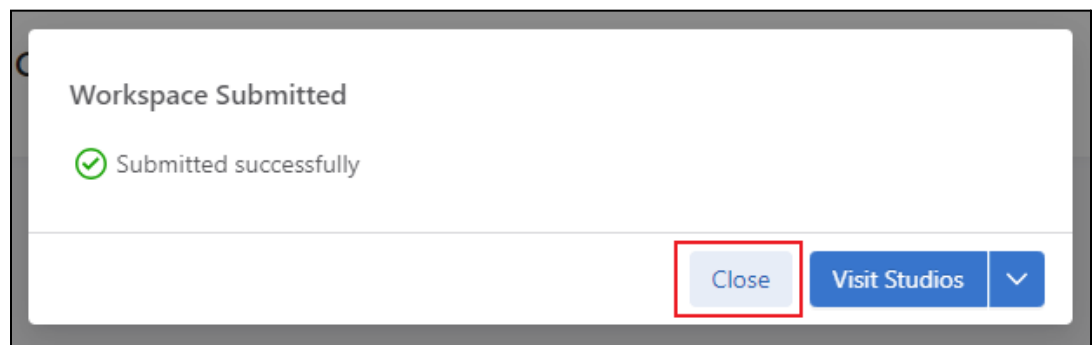
Proposed Configuration Changes

Advanced Reconcile

- iii. Click **Submit Workspace**

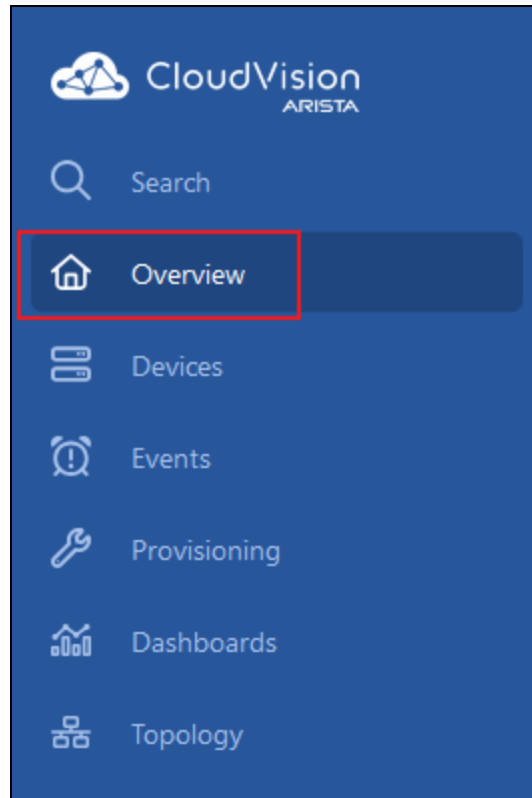


iv. Click **Close**

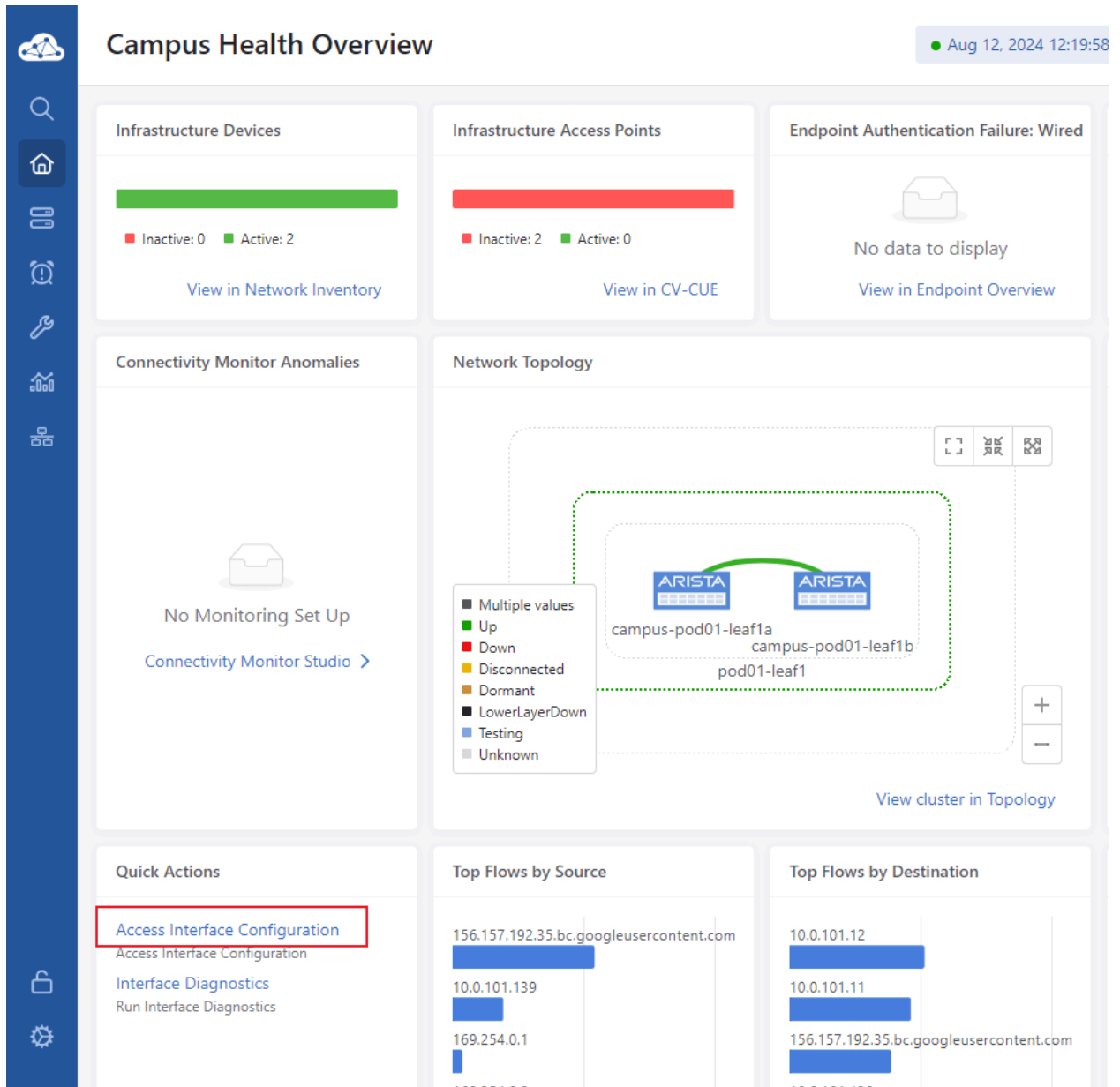


3. Assigning Port Profiles for AP and RPI

1. Assign the configured port profiles to the switches access ports
 - a. Click **Overview** option on the navigation bar



- b. Locate the Quick Actions panel on the lower left of the screen and Click **Access Interface Configuration**



- c. Select the Campus (Workshop), Campus Pod (IT-Bldg), and Access Pod(IDF1)
***Note:** there is only one option for each drop-down.

Access Interface Configuration

Campus

Workshop
▼

Campus Pod

IT-Bldg
▼

Access Pod

IDF1
▼

Port Profile ⓘ

Select an interface to select profile or configure overrides

- d. Select to highlight port **Ethernet1** on bottom switch: campus-pod<##>-leaf1c
**Note: you will may see the bottom device with a hostname format: sw-<IP>*
Example: sw-10.0.113.40
- e. Choose the Port Profile of **Wireless-Access-Point**
- f. Click **Yes** radio button under **Enabled**
- g. Click **Submit**

Access Interface Configuration

Campus

Workshop
▼

Campus Pod

IT-Bldg
▼

Access Pod

IDF1
▼

Port Profile ⓘ

Wireless-Access-Point
▼

Enabled

☒ Yes
 ☐ No

Description

Description

> Advanced Options

Device

campus-pod01-leaf1a

ARISTA 710P-16P

campus-pod01-leaf1b

ARISTA 710P-16P

campus-pod01-leaf1c

ARISTA 710P-16P

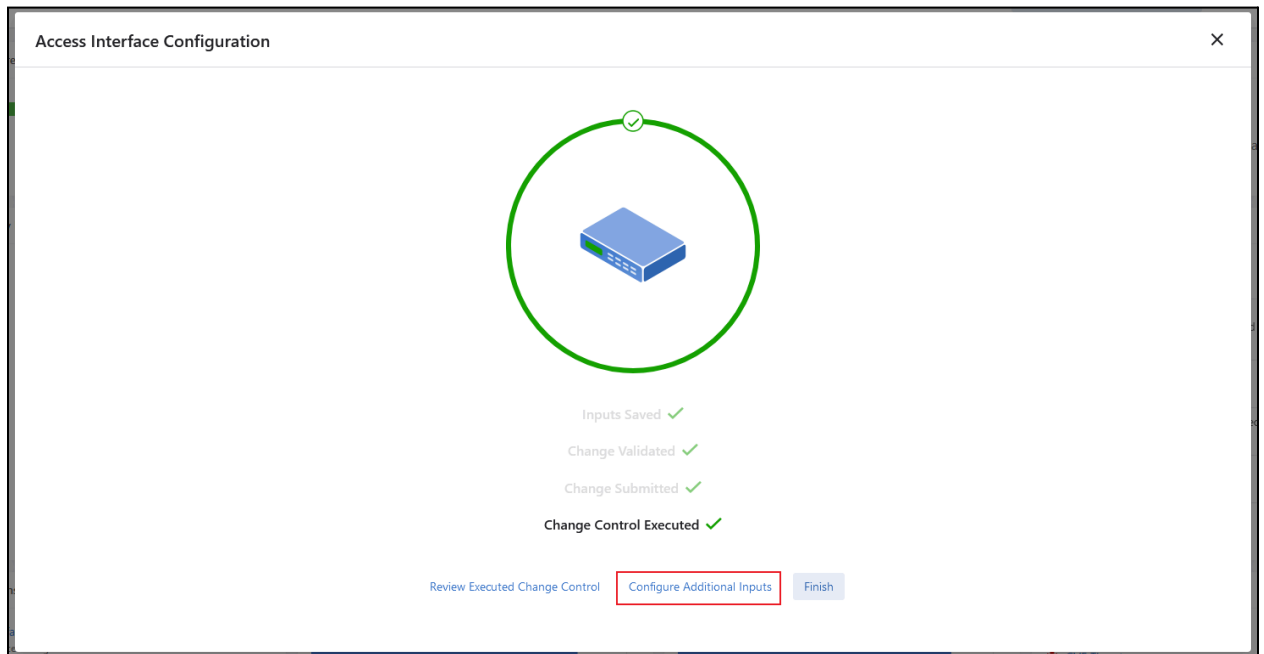
☰

Cancel

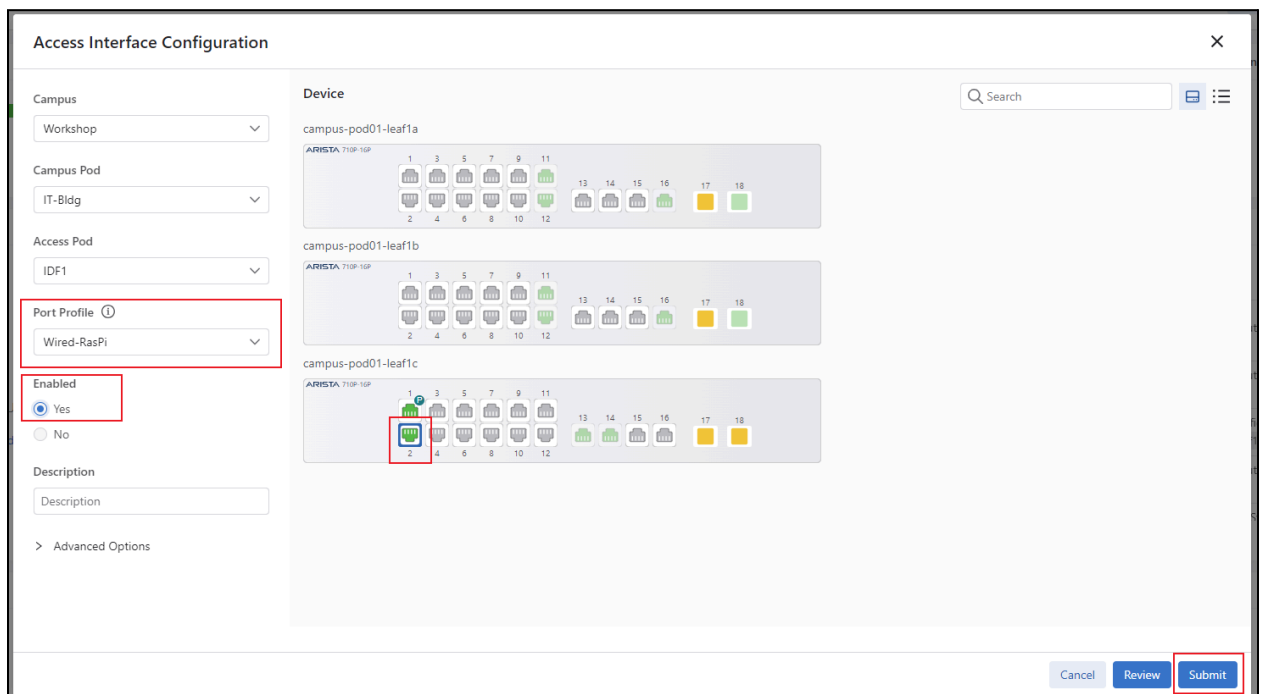
Review

Submit

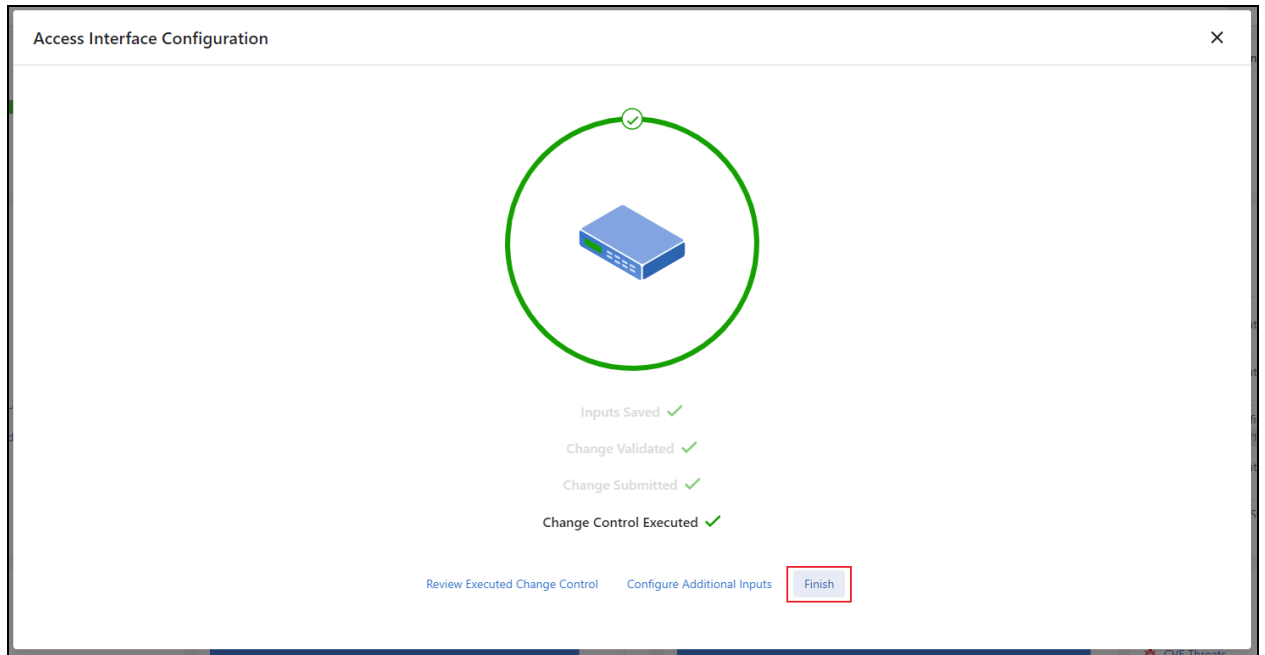
- h. Once the Change Control has been executed, click **Configure Additional Inputs** to configure another access port



- i. Again, select the Campus (Workshop), Campus Pod (IT-Bldg), and Access Pod (IDF1)
- j. Select to highlight port **Ethernet2** on campus-pod<##>-leaf1c (hostname may not match)
- k. Choose the Port Profile of “**Wired-RasPI**”
- l. Click **Yes** radio button under **Enabled**
- m. Click **Submit**



- n. Once the Change Control has been executed, click **Finish**



LAB GUIDE COMPLETE