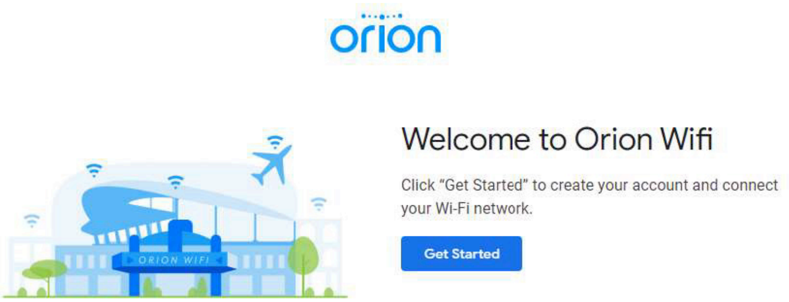
# Cambium Enterprise Wi-Fi and Google Orion Wi-Fi Deployment Guide

## Contents

## Introduction

This document describes about the step by step instruction for integrating Google's Orion Wi-Fi with Cambium Enterprise Wi-Fi Access Points.



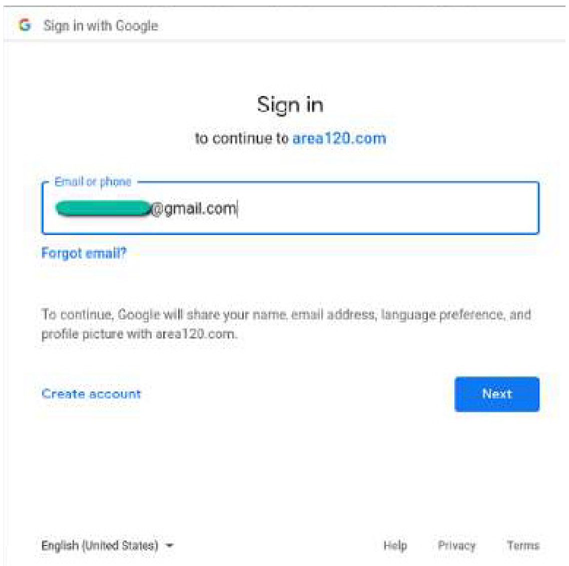
Welcome to Orion Wifi

Click "Get Started" to create your account and connect your Wi-Fi network.

## Sign up for Orion Wi-Fi

As a pre-request step, need to create Orion Wi-Fi account by following steps

- **Enter your google account or you can use your corporate email address , instructions are mentioned**
- **In my example I have used my Gmail id for creating a Orion account, please find the below screen prints**



Sign in

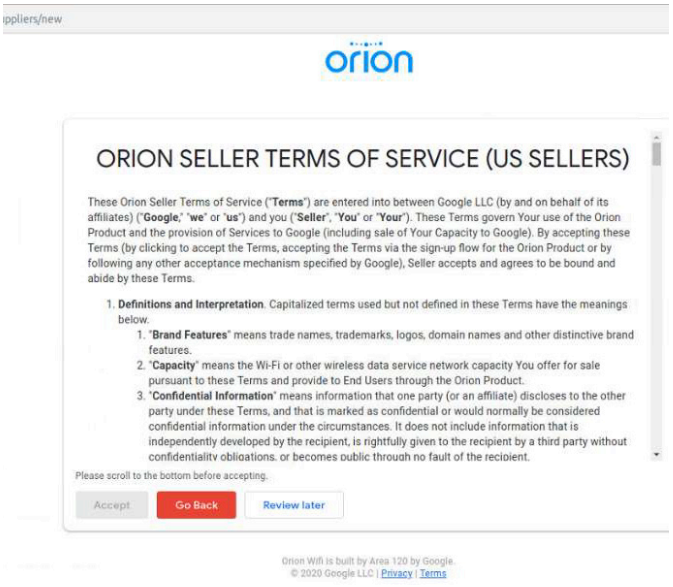
to continue to area120.com

Email or phone: [redacted]@gmail.com

To continue, Google will share your name, email address, language preference, and profile picture with area120.com.

# Cambium Networks and Orion Wi-Fi Integration

## Read and Accept the Terms of Service Agreement



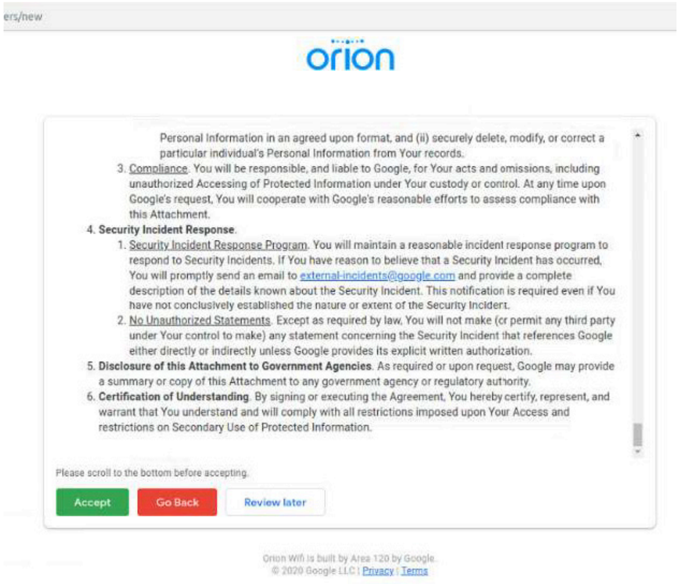
ORION SELLER TERMS OF SERVICE (US SELLERS)

These Orion Seller Terms of Service ("**Terms**") are entered into between Google LLC (by and on behalf of its affiliates) ("**Google**," "**we**" or "**us**") and you ("**Seller**", "**You**" or "**Your**"). These Terms govern Your use of the Orion Product and the provision of Services to Google (including sale of Your Capacity to Google). By accepting these Terms (by clicking to accept the Terms, accepting the Terms via the sign-up flow for the Orion Product or by following any other acceptance mechanism specified by Google), Seller accepts and agrees to be bound and abide by these Terms.

1. **Definitions and Interpretation**. Capitalized terms used but not defined in these Terms have the meanings below.
   1. "**Brand Features**" means trade names, trademarks, logos, domain names and other distinctive brand features.
   2. "**Capacity**" means the Wi-Fi or other wireless data service network capacity You offer for sale pursuant to these Terms and provide to End Users through the Orion Product.
   3. "**Confidential Information**" means information that one party (or an affiliate) discloses to the other party under these Terms, and that is marked as confidential or would normally be considered confidential information under the circumstances. It does not include information that is independently developed by the recipient, is rightfully given to the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient.

Please scroll to the bottom before accepting.

Orion Wifi is built by Area 120 by Google.
© 2020 Google LLC | Privacy | Terms



Personal Information in an agreed upon format, and (ii) securely delete, modify, or correct a particular individual's Personal Information from Your records.

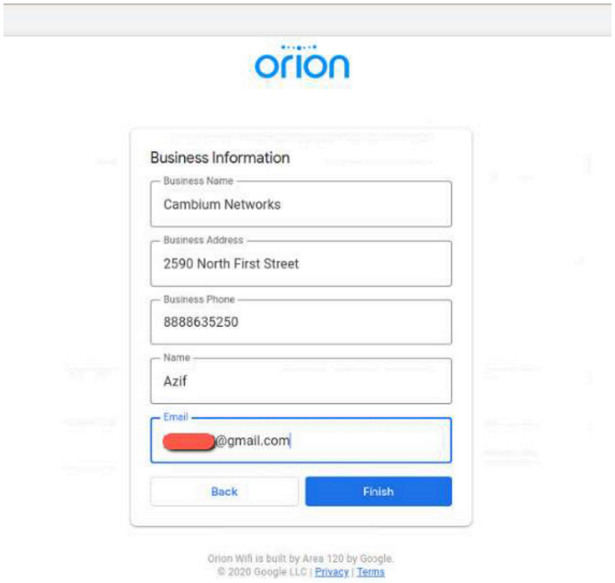
3. Compliance. You will be responsible, and liable to Google, for Your acts and omissions, including unauthorized Accessing of Protected Information under Your custody or control. At any time upon Google's request, You will cooperate with Google's reasonable efforts to assess compliance with this Attachment.

4. **Security Incident Response**.
   1. Security Incident Response Program. You will maintain a reasonable incident response program to respond to Security Incidents. If You have reason to believe that a Security Incident has occurred, You will promptly send an email to external-incidents@google.com and provide a complete description of the details known about the Security Incident. This notification is required even if You have not conclusively established the nature or extent of the Security Incidert.
   2. No Unauthorized Statements. Except as required by law, You will not make (cr permit any third party under Your control to make) any statement concerning the Security Incident that references Google either directly or indirectly unless Google provides its explicit written authorization.
5. **Disclosure of this Attachment to Government Agencies**. As required or upon request, Google may provide a summary or copy of this Attachment to any government agency or regulatory authority.
6. **Certification of Understanding**. By signing or executing the Agreement, You hereby certify, represent, and warrant that You understand and will comply with all restrictions imposed upon Your Access and restrictions on Secondary Use of Protected Information.

Please scroll to the bottom before accepting.

Orion Wifi is built by Area 120 by Google.
© 2020 Google LLC | Privacy | Terms

## Enter the basic business information to create the account



Business Information

Business Name: Cambium Networks

Business Address: 2590 North First Street

Business Phone: 8888635250

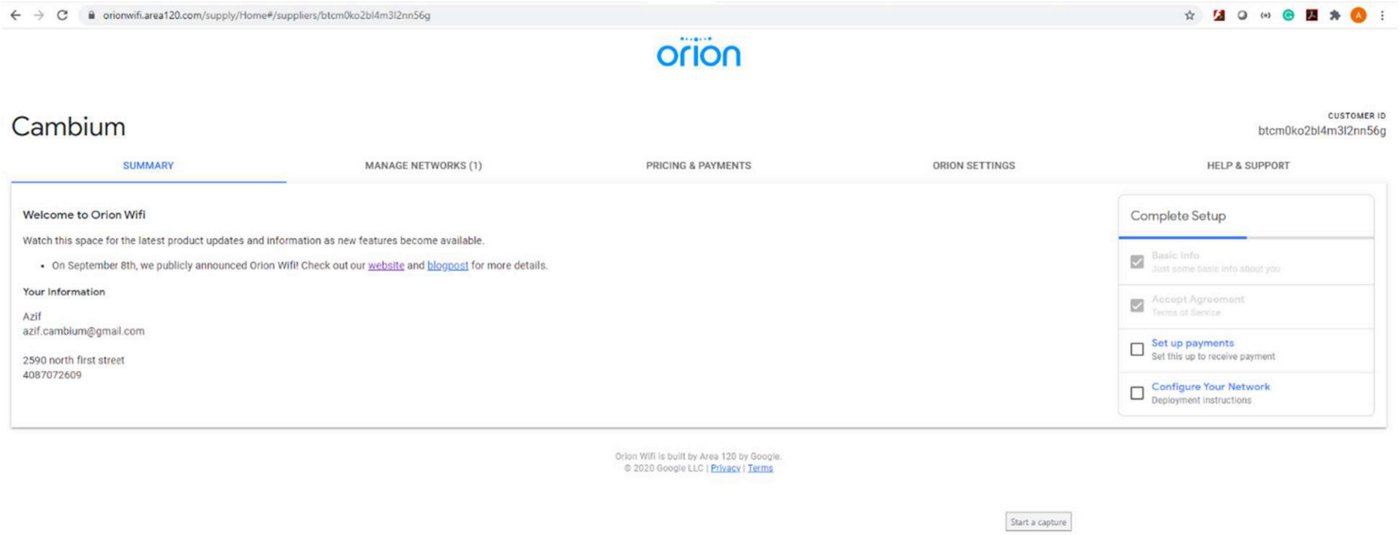
Name: Azif

Email: [redacted]@gmail.com

Orion Wifi is built by Area 120 by Google.
© 2020 Google LLC | Privacy | Terms

Cambium Networks and Orion Wi-Fi Integration

### You will get an Orion login page and click on “configure your network”, which will redirect you to the documentation page



Welcome to Orion Wifi

Watch this space for the latest product updates and information as new features become available.

- On September 8th, we publicly announced Orion Wifi! Check out our website and blogpost for more details.

Your Information

Azif
azif.cambium@gmail.com

2590 north first street
4087072609

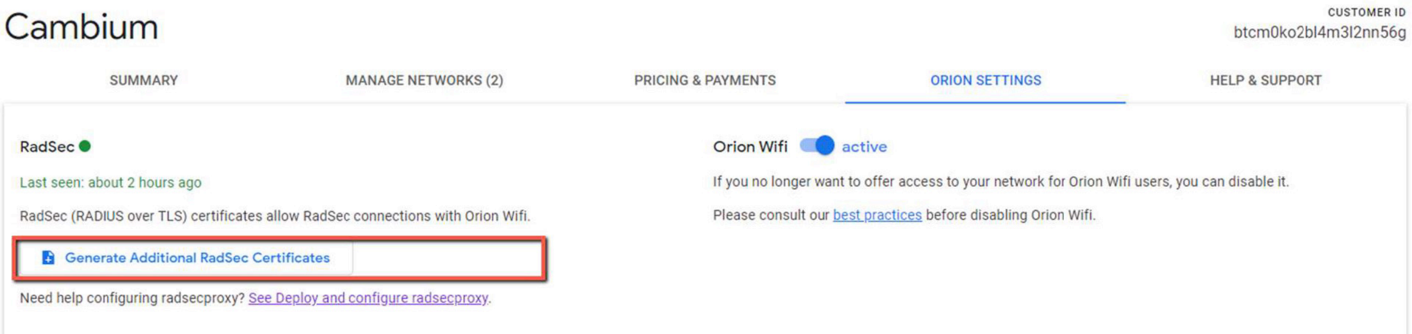
Orion Wifi is built by Area 120 by Google.
© 2020 Google LLC | Privacy | Terms

## Download RadSec Certificates from Orion

Next step is to download the RadSec Certificates from your Orion account, so that you can install a RadSec proxy and connect to Orion RadSec server.

https://docs.google.com/document/u/1/d/e/2PACX-1vSInmW7BBvl9LxNpOTavfftwYhAxs8beRIlETfjp3W-1979b8BabV2HX7931QC4xc1j9GqVf_Zy0sye/pub#h.cf7ovk570ms3

### Click on “Orion Settings” tab and click “Generate RadSec Certificate Bundle” for generating RadSec certificate bundle



Last seen: about 2 hours ago

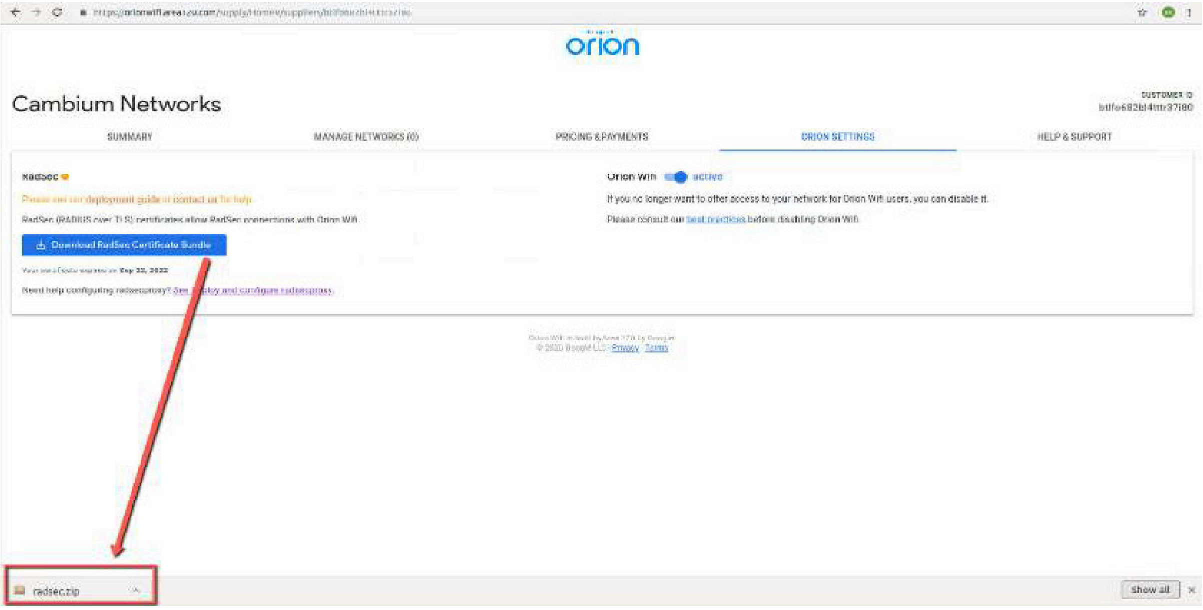
RadSec (RADIUS over TLS) certificates allow RadSec connections with Orion Wifi.

Need help configuring radsecproxy? See Deploy and configure radsecproxy.

If you no longer want to offer access to your network for Orion Wifi users, you can disable it.

Please consult our best practices before disabling Orion Wifi.

### Click on “Download RadSec Certificate Bundle” and save to your local PC



Cambium Networks

CUSTOMER ID
btlfo682bl4ttr37180

Radsec

Please see our deployment guide or contact us for help.

RadSec (RADIUS over TLS) certificates allow RadSec connections with Orion Wifi.

Your certificate expires on Sep 22, 2022

Need help configuring radsecproxy? See Deploy and configure radsecproxy.

Orion Wifi active

If you no longer want to offer access to your network for Orion Wifi users, you can disable it.

Please consult our best practices before disabling Orion Wifi.

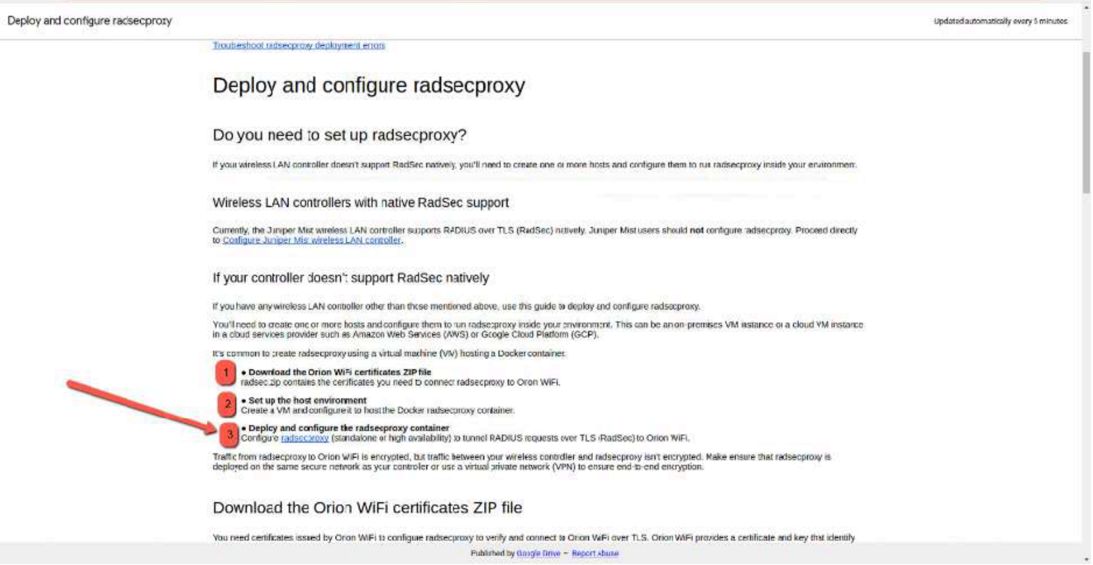
Orion Wifi is built by Area 120 by Google
© 2020 Google LLC · Privacy · Terms

## Create Ubuntu VM for installing proxy RadSec

Create an Ubuntu VM and spawn a docker container for running RadSec. Note down the IP address of the VM, so that can be configured as the radius server in WLAN profile. And proxy RadSec running as a container in Ubuntu VM will initiate a RadSec connection to the Orion Radius server for TLS authentication.

### Click the below URL for opening the RadSec Deployment and configuration

https://docs.google.com/document/d/e/2PACX-1vSl84bfdCireGISY87ZQxZfzq4-J1RVxhlx6zl2NnqO6AcvZkdxu7ojD02qB1-B5xdPlktICvH4t0ar/pub



Deploy and configure radsecproxy

Updated automatically every 5 minutes

Troubleshoot radsecproxy deployment errors

Deploy and configure radsecproxy

Do you need to set up radsecproxy?

If your wireless LAN controller doesn't support RadSec natively, you'll need to create one or more hosts and configure them to run radsecproxy inside your environment.

Wireless LAN controllers with native RadSec support

Currently, the Juniper Mist wireless LAN controller supports RADIUS over TLS (RadSec) natively. Juniper Mist users should **not** configure radsecproxy. Proceed directly to Configure Juniper Mist wireless LAN controller.

If your controller doesn't support RadSec natively

If you have any wireless LAN controller other than those mentioned above, use this guide to deploy and configure radsecproxy.

You'll need to create one or more hosts and configure them to run radsecproxy inside your environment. This can be an on-premises VM instance or a cloud VM instance in a cloud services provider such as Amazon Web Services (AWS) or Google Cloud Platform (GCP).

It's common to create radsecproxy using a virtual machine (VM) hosting a Docker container.

1 • **Download the Orion WiFi certificates ZIP file**
radsec.zip contains the certificates you need to connect radsecproxy to Orion WiFi.

2 • **Set up the host environment**
Create a VM and configure it to host the Docker radsecproxy container.

3 • **Deploy and configure the radsecproxy container**
Configure radsecproxy (standalone or high availability) to tunnel RADIUS requests over TLS (RadSec) to Orion WiFi.

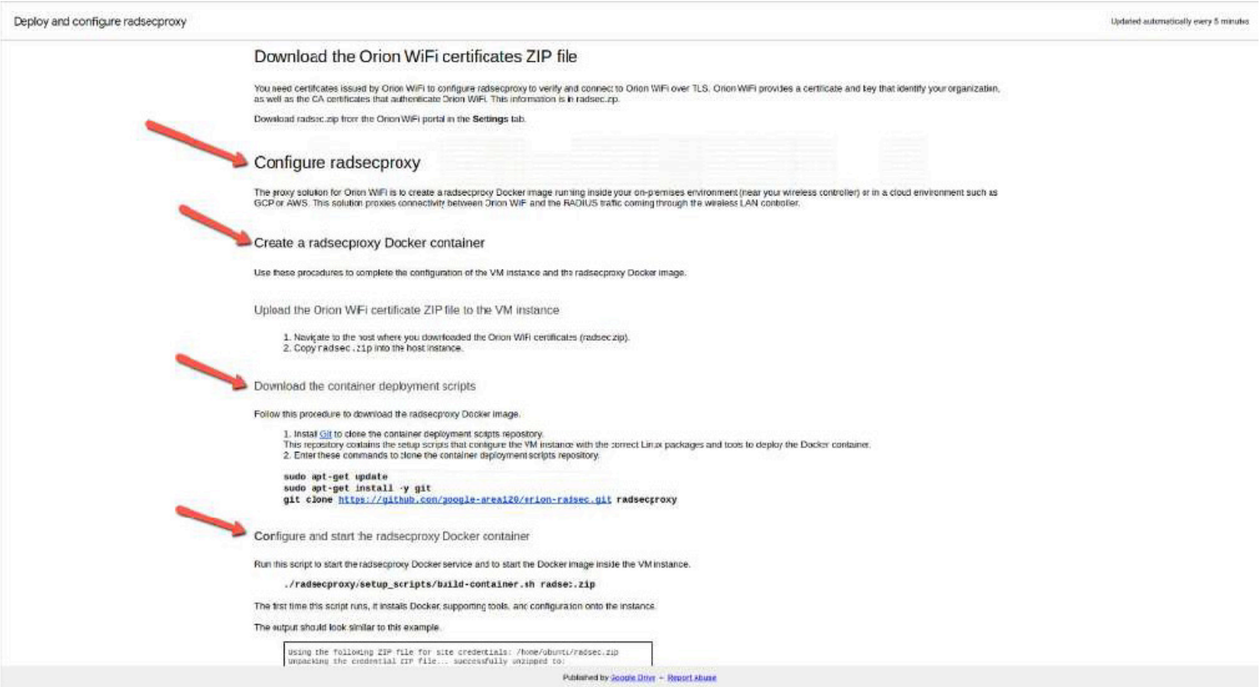
Traffic from radsecproxy to Orion WiFi is encrypted, but traffic between your wireless controller and radsecproxy isn't encrypted. Make ensure that radsecproxy is deployed on the same secure network as your controller or use a virtual private network (VPN) to ensure end-to-end encryption.

Download the Orion WiFi certificates ZIP file

You need certificates issued by Orion WiFi to configure radsecproxy to verify and connect to Orion WiFi over TLS. Orion WiFi provides a certificate and key that identify

Published by Google Drive – Report Abuse

**Please follow the below git commands to get the RadSec container and initialize the same in Ubuntu VM**



Deploy and configure radsecproxy

Updated automatically every 5 minutes

Download the Orion WiFi certificates ZIP file

You need certifcates issued by Orion WiFi to configure radsecproxy to verify and connect to Orion WiFi over TLS. Orion WiFi provides a certificate and key that identify your organization, as well as the CA certificates that authenticate Orion WiFi. This information is in radsec.zip.

Download radsec.zip from the Orion WiFi portal in the **Settings** tab.

Configure radsecproxy

The proxy solution for Orion WiFi is to create a radsecproxy Docker image running inside your on-premises environment (near your wireless controller) or in a cloud environment such as GCP or AWS. This solution proxies connectivity between Orion WiFi and the RADIUS traffic coming through the wireless LAN controller.

Create a radsecproxy Docker container

Use these procedures to complete the configuration of the VM instance and the radsecproxy Docker image.

Upload the Orion WiFi certificate ZIP file to the VM instance

1. Navigate to the host where you downloaded the Orion WiFi certificates (radsec.zip).
2. Copy `radsec.zip` into the host instance.

Download the container deployment scripts

Follow this procedure to download the radsecproxy Docker image.

1. Install Git to clone the container deployment scripts repository.
This repository contains the setup scripts that configure the VM instance with the correct Linux packages and tools to deploy the Docker container.
2. Enter these commands to clone the container deployment scripts repository.

```
sudo apt-get update
sudo apt-get install -y git
git clone https://github.com/google-area120/orion-radsec.git radsecproxy
```

Configure and start the radsecproxy Docker container

Run this script to start the radsecproxy Docker service and to start the Docker image inside the VM instance.

```
./radsecproxy/setup_scripts/build-container.sh radsec.zip
```

The first time this script runs, it installs Docker, supporting tools, and configuration onto the instance.

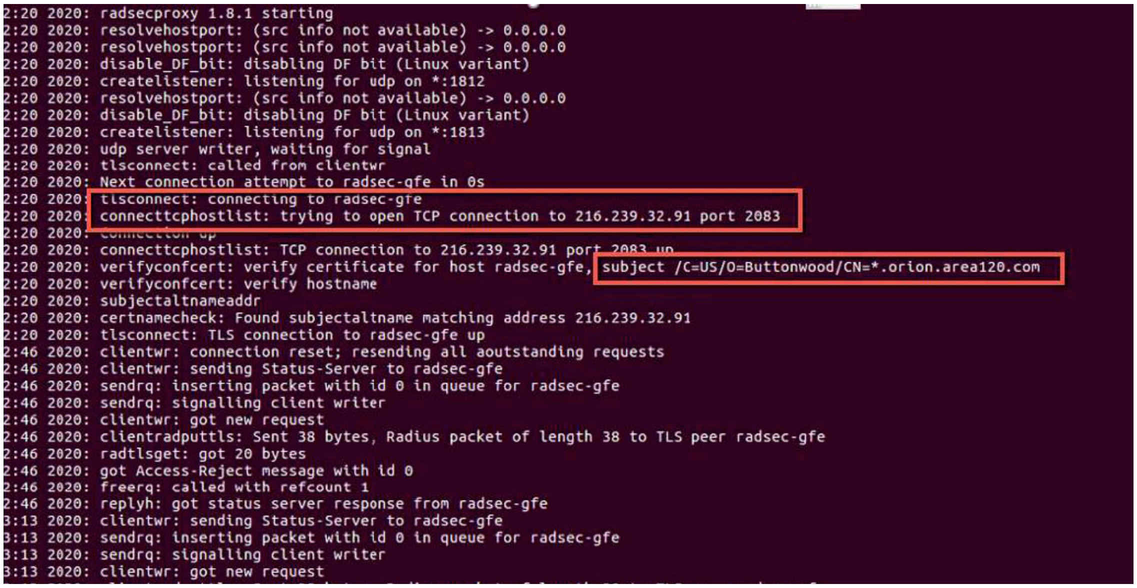
The output should look similar to this example.

```
Using the following ZIP file for site credentials: /home/ubuntu/radsec.zip
Unpacking the credential ZIP file... successfully unzipped to:
```

Published by Google Drive – Report Abuse

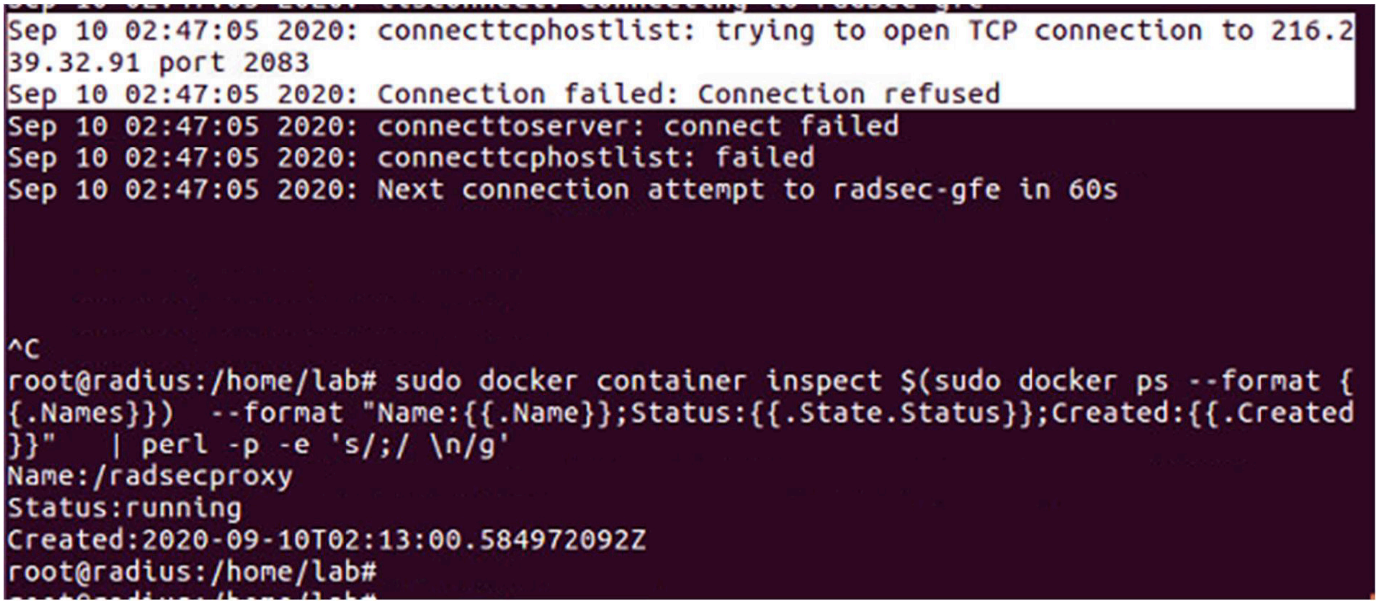
## Troubleshooting RadSec connection

**RadSec proxy will establish the TCP connection with Orion RadSec IP address using port number 2083. If your organization firewall is blocking the port please request your IT department to unblock it.**



```
2:20 2020: radsecproxy 1.8.1 starting
2:20 2020: resolvehostport: (src info not available) -> 0.0.0.0
2:20 2020: resolvehostport: (src info not available) -> 0.0.0.0
2:20 2020: disable_DF_bit: disabling DF bit (Linux variant)
2:20 2020: createlistener: listening for udp on *:1812
2:20 2020: resolvehostport: (src info not available) -> 0.0.0.0
2:20 2020: disable_DF_bit: disabling DF bit (Linux variant)
2:20 2020: createlistener: listening for udp on *:1813
2:20 2020: udp server writer, waiting for signal
2:20 2020: tlsconnect: called from clientwr
2:20 2020: Next connection attempt to radsec-gfe in 0s
2:20 2020: tlsconnect: connecting to radsec-gfe
2:20 2020: connecttcphostlist: trying to open TCP connection to 216.239.32.91 port 2083
2:20 2020: connection up
2:20 2020: connecttcphostlist: TCP connection to 216.239.32.91 port 2083 up
2:20 2020: verifyconfcert: verify certificate for host radsec-gfe, subject /C=US/O=Buttonwood/CN=*.orion.area120.com
2:20 2020: verifyconfcert: verify hostname
2:20 2020: subjectaltnameaddr
2:20 2020: certnamecheck: Found subjectaltname matching address 216.239.32.91
2:20 2020: tlsconnect: TLS connection to radsec-gfe up
2:46 2020: clientwr: connection reset; resending all aoutstanding requests
2:46 2020: clientwr: sending Status-Server to radsec-gfe
2:46 2020: sendrq: inserting packet with id 0 in queue for radsec-gfe
2:46 2020: sendrq: signalling client writer
2:46 2020: clientwr: got new request
2:46 2020: clientradputtls: Sent 38 bytes, Radius packet of length 38 to TLS peer radsec-gfe
2:46 2020: radtlsget: got 20 bytes
2:46 2020: got Access-Reject message with id 0
2:46 2020: freerq: called with refcount 1
2:46 2020: replyh: got status server response from radsec-gfe
3:13 2020: clientwr: sending Status-Server to radsec-gfe
3:13 2020: sendrq: inserting packet with id 0 in queue for radsec-gfe
3:13 2020: sendrq: signalling client writer
3:13 2020: clientwr: got new request
```

### If your organization is blocking the port or not able to reach the external RadSec, then you will see the below error



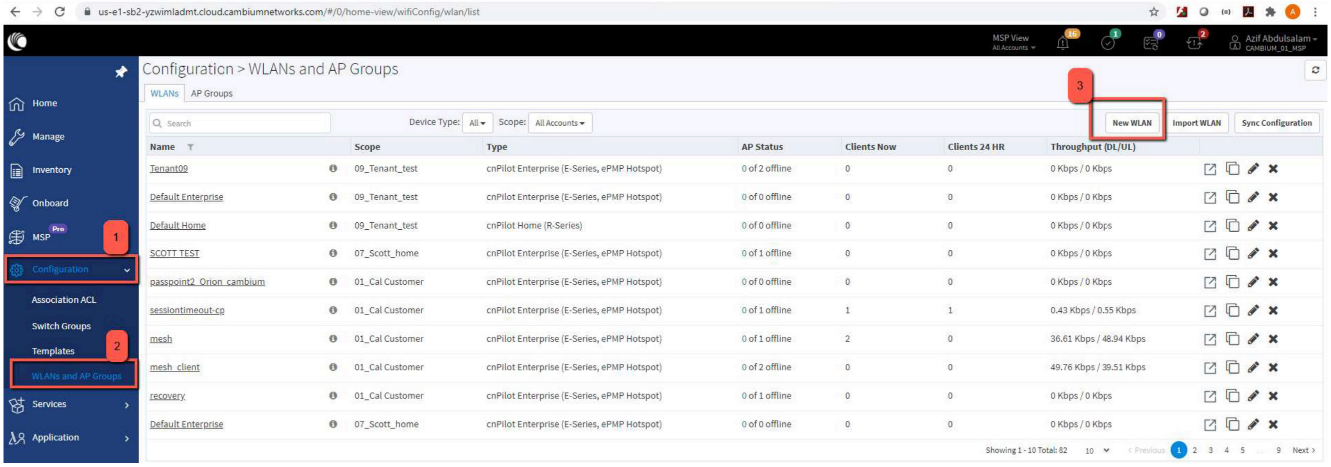
```
Sep 10 02:47:05 2020: connecttcphostlist: trying to open TCP connection to 216.2
39.32.91 port 2083
Sep 10 02:47:05 2020: Connection failed: Connection refused
Sep 10 02:47:05 2020: connecttoserver: connect failed
Sep 10 02:47:05 2020: connecttcphostlist: failed
Sep 10 02:47:05 2020: Next connection attempt to radsec-gfe in 60s



^C
root@radius:/home/lab# sudo docker container inspect $(sudo docker ps --format {
{.Names}})  --format "Name:{{.Name}};Status:{{.State.Status}};Created:{{.Created
}}"    | perl -p -e 's/;/ \n/g'
Name:/radsecproxy
Status:running
Created:2020-09-10T02:13:00.584972092Z
root@radius:/home/lab#
```

## Passpoint configuration in cnMaestro

### Navigate to “Configuration” -> “WLANs and AP Groups” for creating a new WLAN



us-e1-sb2-yzwimladmt.cloud.cambiumnetworks.com/#/0/home-view/wifiConfig/wlan/list

Configuration > WLANs and AP Groups

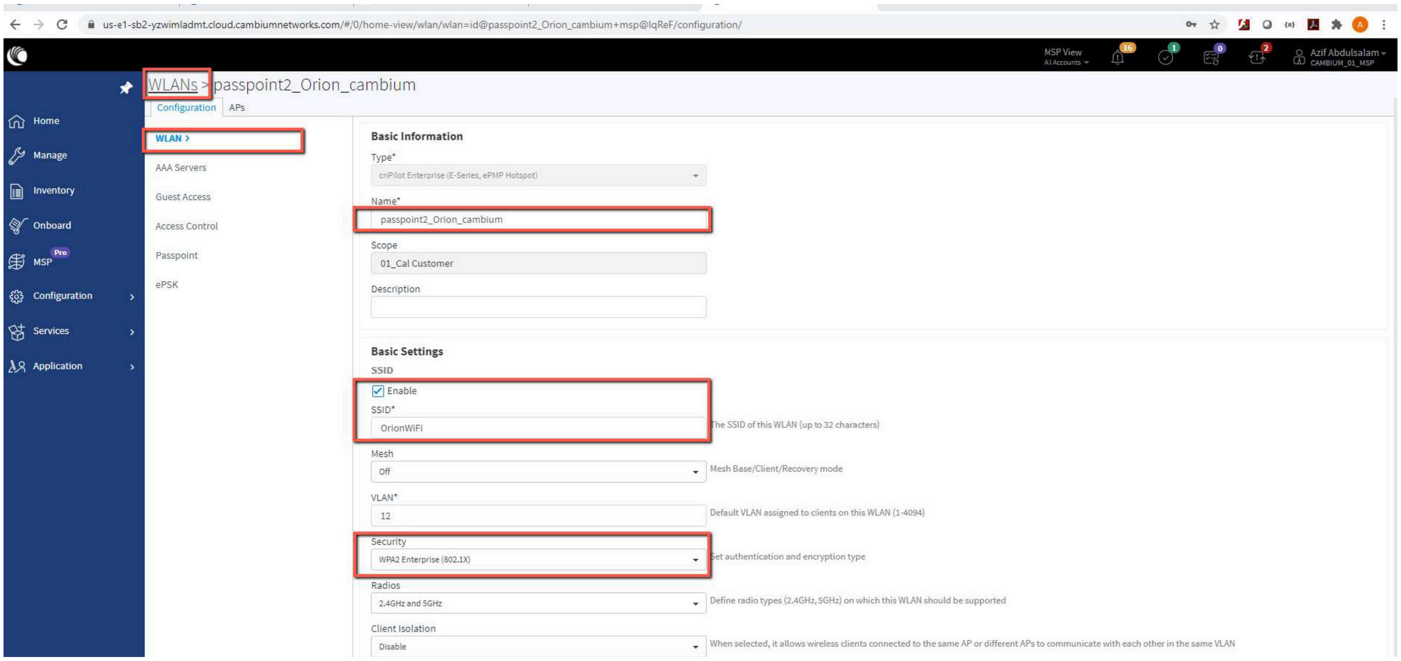
Device Type: All ▾ Scope: All Accounts ▾

| Name | Scope | Type | AP Status | Clients Now | Clients 24 HR | Throughput (DL/UL) |
|---|---|---|---|---|---|---|
| Tenant09 | 09_Tenant_test | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 2 offline | 0 | 0 | 0 Kbps / 0 Kbps |
| Default Enterprise | 09_Tenant_test | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 0 offline | 0 | 0 | 0 Kbps / 0 Kbps |
| Default Home | 09_Tenant_test | cnPilot Home (R-Series) | 0 of 0 offline | 0 | 0 | 0 Kbps / 0 Kbps |
| SCOTT TEST | 07_Scott_home | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 1 offline | 0 | 0 | 0 Kbps / 0 Kbps |
| passpoint2_Orion_cambium | 01_Cal Customer | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 0 offline | 0 | 0 | 0 Kbps / 0 Kbps |
| sessiontimeout-cp | 01_Cal Customer | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 1 offline | 1 | 1 | 0.43 Kbps / 0.55 Kbps |
| mesh | 01_Cal Customer | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 1 offline | 2 | 0 | 36.61 Kbps / 48.94 Kbps |
| mesh_client | 01_Cal Customer | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 2 offline | 0 | 0 | 49.76 Kbps / 39.51 Kbps |
| recovery | 01_Cal Customer | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 1 offline | 0 | 0 | 0 Kbps / 0 Kbps |
| Default Enterprise | 07_Scott_home | cnPilot Enterprise (E-Series, ePMP Hotspot) | 0 of 0 offline | 0 | 0 | 0 Kbps / 0 Kbps |

Showing 1 - 10 Total: 82 10 ‹ Previous 1 2 3 4 5 … 9 Next ›

# Cambium Networks and Orion Wi-Fi Integration

## Configure the SSID and Security as “WAP2 Enterprise (802.1x)”



Basic Information

Type*: cnPilot Enterprise (E-Series, ePMP Hotspot)

Name*: passpoint2_Orion_cambium

Scope: 01_Cal Customer

Description:

Basic Settings

SSID

☑ Enable

SSID*: OrionWiFi — The SSID of this WLAN (up to 32 characters)

Mesh: Off — Mesh Base/Client/Recovery mode

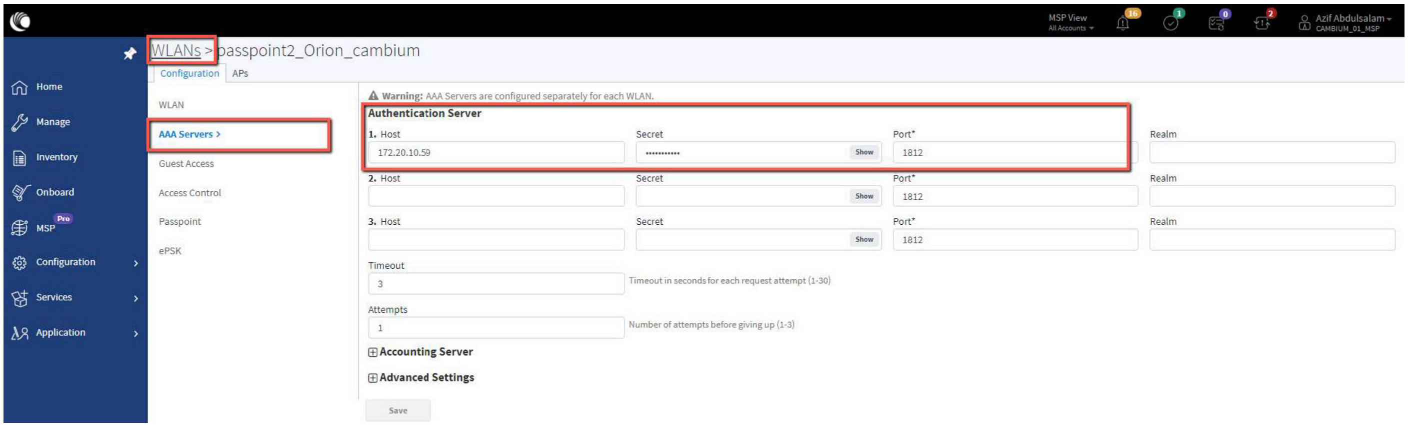
VLAN*: 12 — Default VLAN assigned to clients on this WLAN (1-4094)

Security: WPA2 Enterprise (802.1X) — Set authentication and encryption type

Radios: 2.4GHz and 5GHz — Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

Client Isolation: Disable — When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

## Configure the AAA server as the local Ubuntu VM that is running the RadSec proxy server.



⚠ Warning: AAA Servers are configured separately for each WLAN.

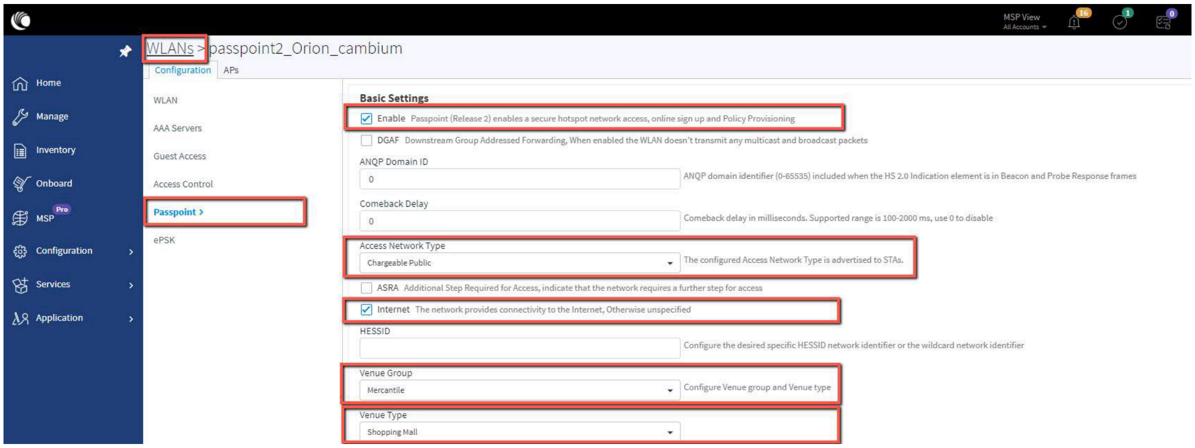
Authentication Server

| | Host | Secret | Port* | Realm |
|---|---|---|---|---|
| 1. | 172.20.10.59 | ••••••••••• | 1812 | |
| 2. | | | 1812 | |
| 3. | | | 1812 | |

Timeout: 3 — Timeout in seconds for each request attempt (1-30)

Attempts: 1 — Number of attempts before giving up (1-3)

## Configure the Passpoint with below settings



WLANs > passpoint2_Orion_cambium

**Basic Settings**

☑ Enable Passpoint (Release 2) enables a secure hotspot network access, online sign up and Policy Provisioning

☐ DGAF Downstream Group Addressed Forwarding, When enabled the WLAN doesn't transmit any multicast and broadcast packets

ANQP Domain ID: 0 — ANQP domain identifier (0-65535) included when the HS 2.0 Indication element is in Beacon and Probe Response frames

Comeback Delay: 0 — Comeback delay in milliseconds. Supported range is 100-2000 ms, use 0 to disable

Access Network Type: Chargeable Public — The configured Access Network Type is advertised to STAs.

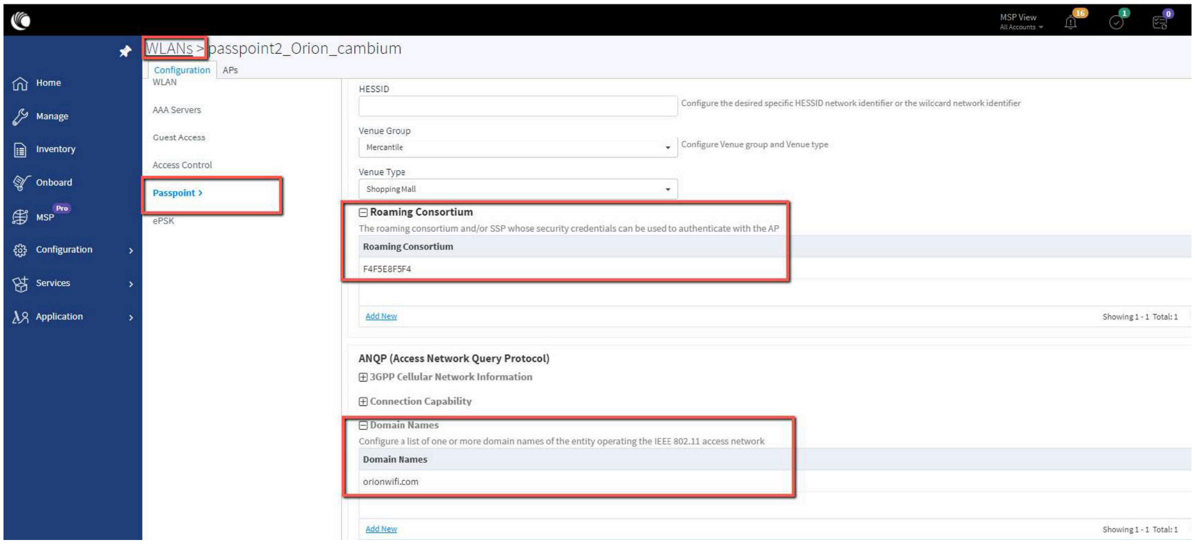
☐ ASRA Additional Step Required for Access, indicate that the network requires a further step for access

☑ Internet The network provides connectivity to the Internet, Otherwise unspecified

HESSID: — Configure the desired specific HESSID network identifier or the wildcard network identifier

Venue Group: Mercantile — Configure Venue group and Venue type

Venue Type: Shopping Mall



WLANs > passpoint2_Orion_cambium

HESSID: — Configure the desired specific HESSID network identifier or the wilccard network identifier

Venue Group: Mercantile — Configure Venue group and Venue type

Venue Type: Shopping Mall

⊟ **Roaming Consortium**

The roaming consortium and/or SSP whose security credentials can be used to authenticate with the AP

| Roaming Consortium |
|---|
| F4F5E8F5F4 |

Showing 1 - 1 Total: 1

**ANQP (Access Network Query Protocol)**

⊞ 3GPP Cellular Network Information

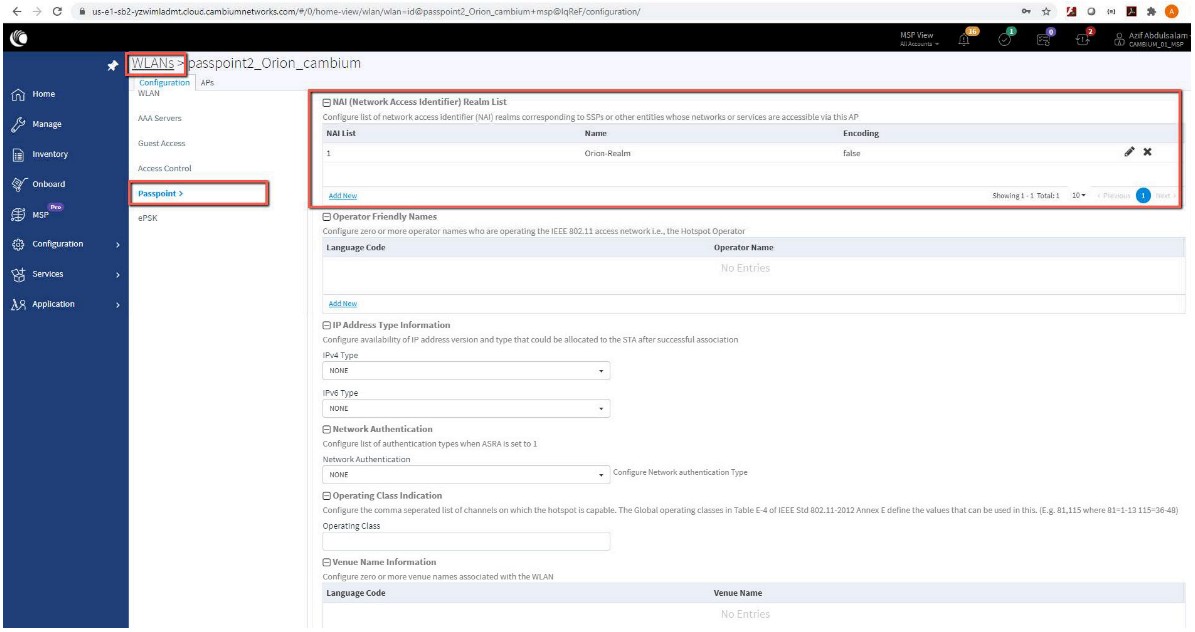
⊞ Connection Capability

⊟ **Domain Names**

Configure a list of one or more domain names of the entity operating the IEEE 802.11 access network

| Domain Names |
|---|
| orionwifi.com |

Showing 1 - 1 Total: 1



us-e1-sb2-yzwimladmt.cloud.cambiumnetworks.com/#/0/home-view/wlan/wlan=id@passpoint2_Orion_cambium+msp@IqReF/configuration/

WLANs > passpoint2_Orion_cambium

⊟ **NAI (Network Access Identifier) Realm List**

Configure list of network access identifier (NAI) realms corresponding to SSPs or other entities whose networks or services are accessible via this AP

| NAI List | Name | Encoding |
|---|---|---|
| 1 | Orion-Realm | false |

Showing 1 - 1 Total: 1

⊟ **Operator Friendly Names**

Configure zero or more operator names who are operating the IEEE 802.11 access network i.e., the Hotspot Operator

| Language Code | Operator Name |
|---|---|
| No Entries | |

⊟ **IP Address Type Information**

Configure availability of IP address version and type that could be allocated to the STA after successful association

IPv4 Type: NONE

IPv6 Type: NONE

⊟ **Network Authentication**

Configure list of authentication types when ASRA is set to 1

Network Authentication: NONE — Configure Network authentication Type

⊟ **Operating Class Indication**

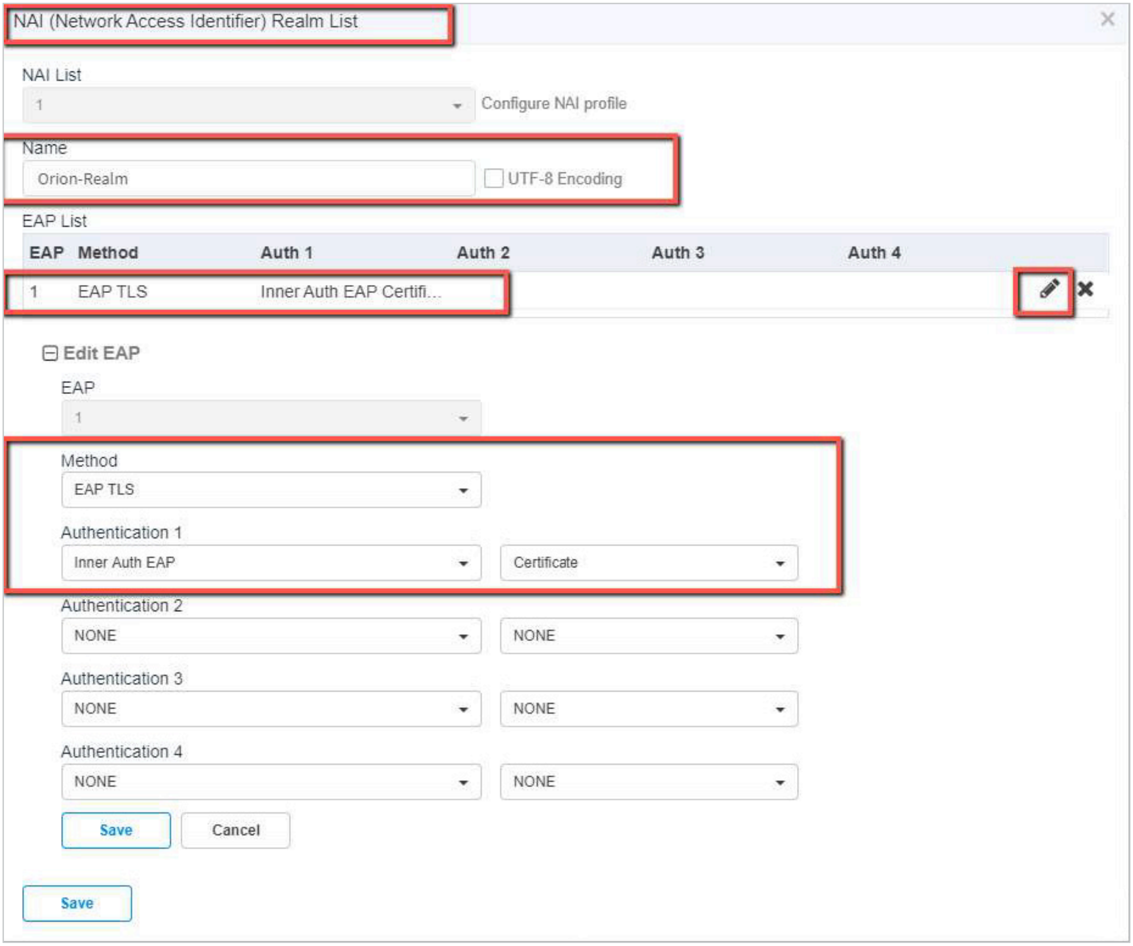
Configure the comma seperated list of channels on which the hotspot is capable. The Global operating classes in Table E-4 of IEEE Std 802.11-2012 Annex E define the values that can be used in this. (E.g. 81,115 where 81=1-13 115=36-48)

Operating Class:

⊟ **Venue Name Information**

Configure zero or more venue names associated with the WLAN

| Language Code | Venue Name |
|---|---|
| No Entries | |



NAI (Network Access Identifier) Realm List

NAI List: 1 — Configure NAI profile

Name: Orion-Realm

□ UTF-8 Encoding

EAP List

| EAP | Method | Auth 1 | Auth 2 | Auth 3 | Auth 4 |
|---|---|---|---|---|---|
| 1 | EAP TLS | Inner Auth EAP Certifi... | | | |

⊟ Edit EAP

EAP: 1

Method: EAP TLS

Authentication 1: Inner Auth EAP — Certificate

Authentication 2: NONE — NONE

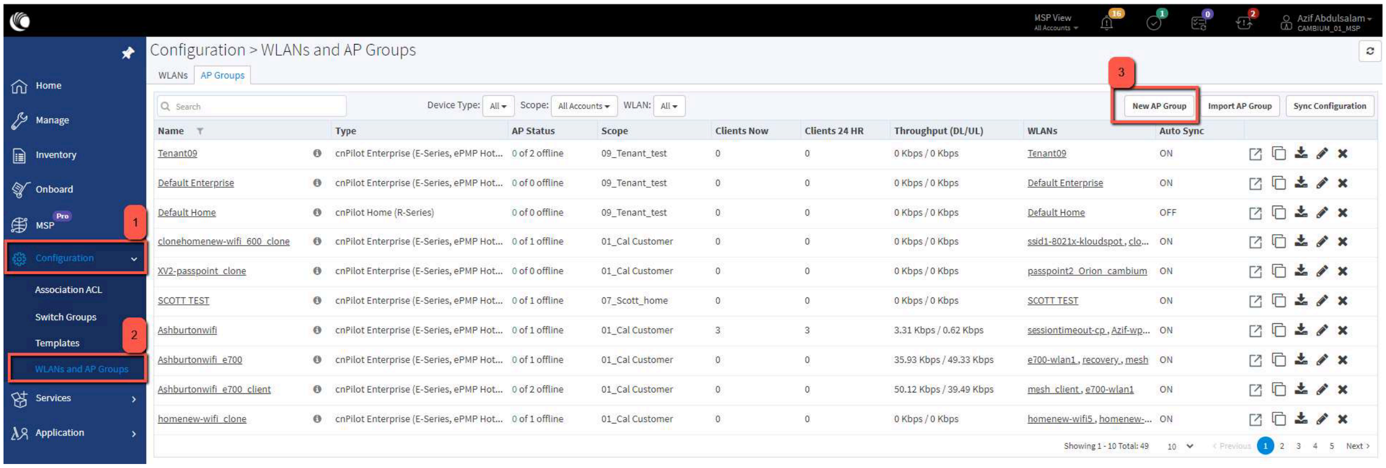
Authentication 3: NONE — NONE

Authentication 4: NONE — NONE

**Save the WLAN configuration**

## Create AP Group and attach the same to Enterprise Wi-Fi AP

### Navigate to “configuration” -> “WLANs and AP Group” -> click “New AP Group”



Configuration > WLANs and AP Groups

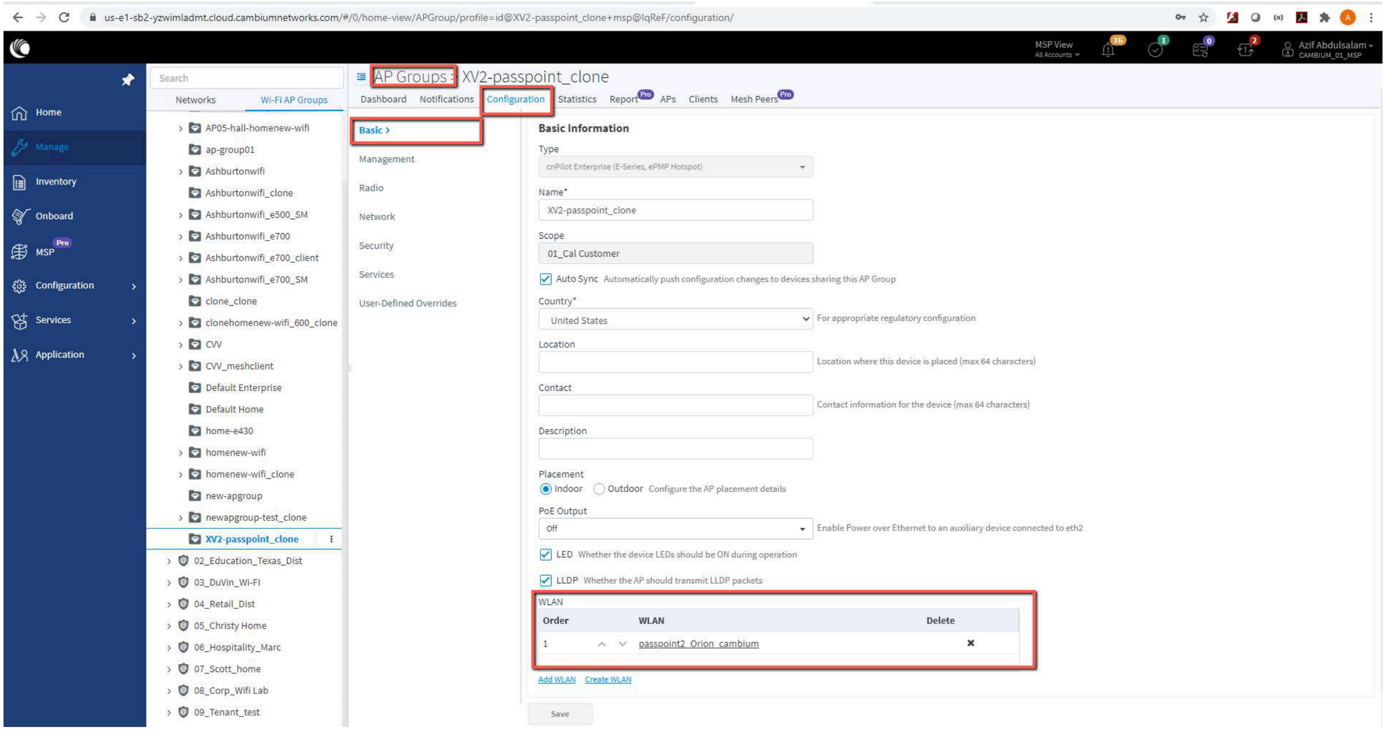
WLANs | AP Groups

Search | Device Type: All | Scope: All Accounts | WLAN: All

| Name | Type | AP Status | Scope | Clients Now | Clients 24 HR | Throughput (DL/UL) | WLANs | Auto Sync |
|---|---|---|---|---|---|---|---|---|
| Tenant09 | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 2 offline | 09_Tenant_test | 0 | 0 | 0 Kbps / 0 Kbps | Tenant09 | ON |
| Default Enterprise | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 0 offline | 09_Tenant_test | 0 | 0 | 0 Kbps / 0 Kbps | Default Enterprise | ON |
| Default Home | cnPilot Home (R-Series) | 0 of 0 offline | 09_Tenant_test | 0 | 0 | 0 Kbps / 0 Kbps | Default Home | OFF |
| clonehomenew-wifi_600_clone | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 1 offline | 01_Cal Customer | 0 | 0 | 0 Kbps / 0 Kbps | ssid1-8021x-kloudspot , clo... | ON |
| XV2-passpoint_clone | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 0 offline | 01_Cal Customer | 0 | 0 | 0 Kbps / 0 Kbps | passpoint2_Orion_cambium | ON |
| SCOTT TEST | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 1 offline | 07_Scott_home | 0 | 0 | 0 Kbps / 0 Kbps | SCOTT TEST | ON |
| Ashburtonwifi | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 1 offline | 01_Cal Customer | 3 | 3 | 3.31 Kbps / 0.62 Kbps | sessiontimeout-cp , Azif-wp... | ON |
| Ashburtonwifi_e700 | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 1 offline | 01_Cal Customer | 0 | 0 | 35.93 Kbps / 49.33 Kbps | e700-wlan1 , recovery , mesh | ON |
| Ashburtonwifi_e700_client | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 2 offline | 01_Cal Customer | 0 | 0 | 50.12 Kbps / 39.49 Kbps | mesh_client , e700-wlan1 | ON |
| homenew-wifi_clone | cnPilot Enterprise (E-Series, ePMP Hot... | 0 of 1 offline | 01_Cal Customer | 0 | 0 | 0 Kbps / 0 Kbps | homenew-wifi5 , homenew-... | ON |

Showing 1 - 10 Total: 49 | 10 | ‹ Previous 1 2 3 4 5 Next ›

### Navigate to “configuration” -> “WLANs and AP Group” -> click “New AP Group”



AP Groups > XV2-passpoint_clone

**Basic Information**

Type: cnPilot Enterprise (E-Series, ePMP Hotspot)

Name*: XV2-passpoint_clone

Scope: 01_Cal Customer

☑ Auto Sync Automatically push configuration changes to devices sharing this AP Group

Country*: United States — For appropriate regulatory configuration

Location: — Location where this device is placed (max 64 characters)

Contact: — Contact information for the device (max 64 characters)

Description:

Placement: ● Indoor ○ Outdoor Configure the AP placement details

PoE Output: Off — Enable Power over Ethernet to an auxiliary device connected to eth2

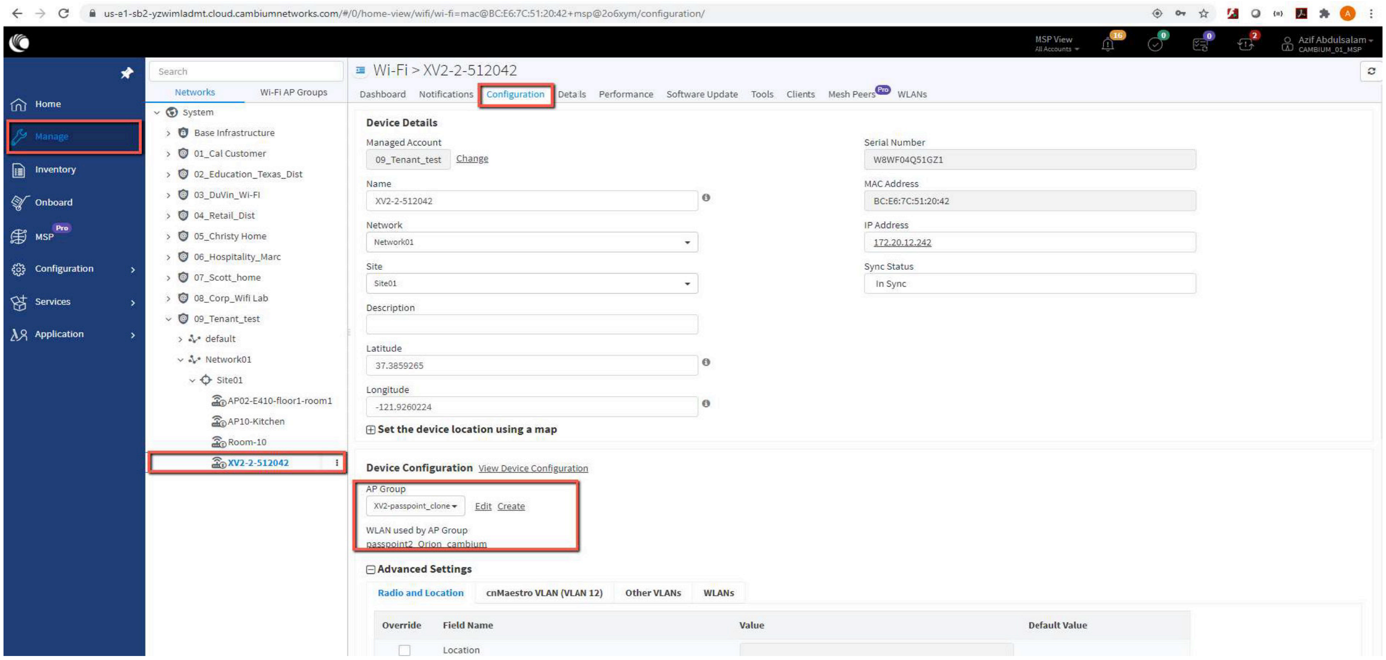
☑ LED Whether the device LEDs should be ON during operation

☑ LLDP Whether the AP should transmit LLDP packets

WLAN

| Order | WLAN | Delete |
|---|---|---|
| 1 | passpoint2_Orion_cambium | ✖ |

**Select the AP group configuration to the respective AP by navigating -> Manage -> Specific device -> Configuration and in AP group drop down, select the newly created AP Group.**



Wi-Fi > XV2-2-512042

Device Details

Managed Account: 09_Tenant_test

Name: XV2-2-512042

Network: Network01

Site: Site01

Description:

Latitude: 37.3859265

Longitude: -121.9260224

Serial Number: W8WF04Q51GZ1

MAC Address: BC:E6:7C:51:20:42

IP Address: 172.20.12.242

Sync Status: In Sync

Device Configuration

AP Group: XV2-passpoint_clone

WLAN used by AP Group: passpoint2_Orion_cambium

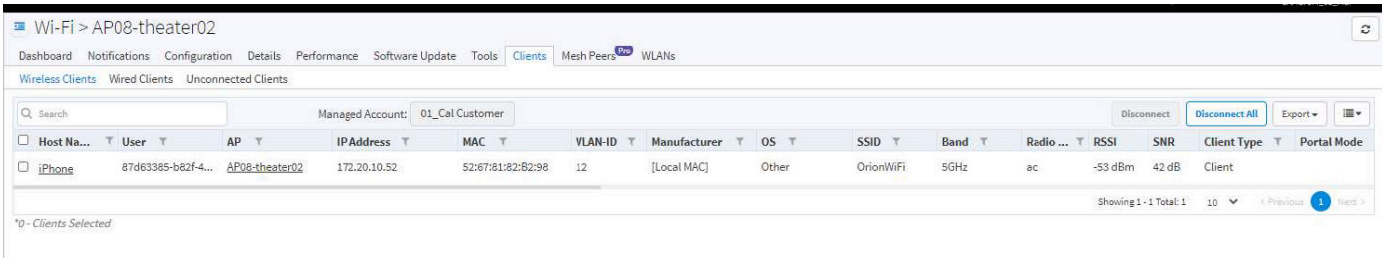
| Override | Field Name | Value | Default Value |
|---|---|---|---|
| □ | Location | | |

## Validating with a wireless client by connecting to Orion WLAN

**Follow the below link to download the profile to AP**

https://docs.google.com/document/d/e/2PACX-1vQhbx-MIqc_7Tmsp5SrJ435JlDhEbz7y0x8gtCiZAcErg-kTlCqbhWuTLf6SeiFTf52DMreoXa7im-W/pub#h.n2jmq2da97p

**After installing the profile, the wireless device should be connecting to the Orion Wireless LAN**



Wi-Fi > AP08-theater02

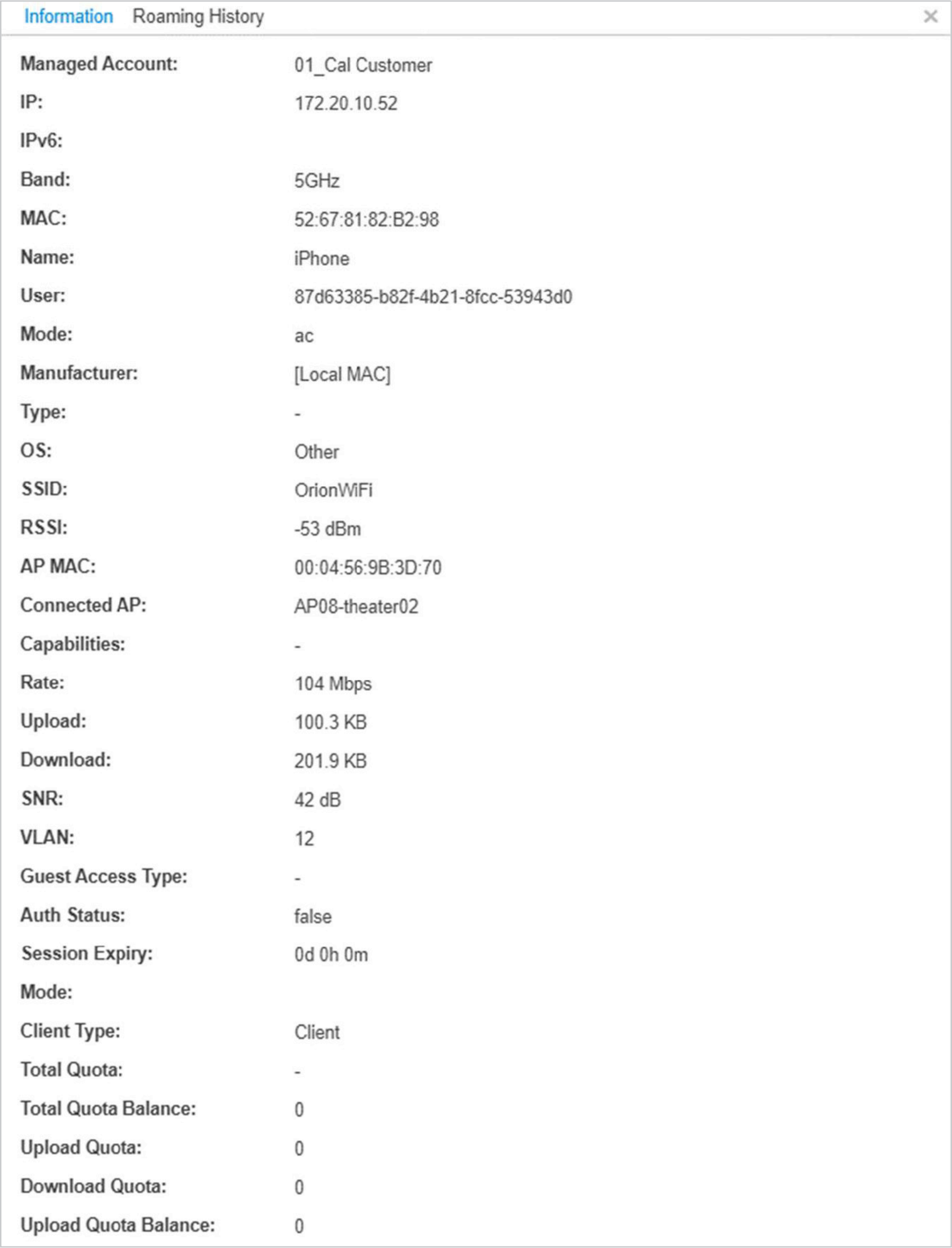
Managed Account: 01_Cal Customer

| □ | Host Na... | User | AP | IP Address | MAC | VLAN-ID | Manufacturer | OS | SSID | Band | Radio ... | RSSI | SNR | Client Type | Portal Mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | iPhone | 87d63385-b82f-4... | AP08-theater02 | 172.20.10.52 | 52:67:81:82:B2:98 | 12 | [Local MAC] | Other | OrionWiFi | 5GHz | ac | -53 dBm | 42 dB | Client | |

Showing 1 - 1 Total: 1   10   ‹ Previous 1 Next ›

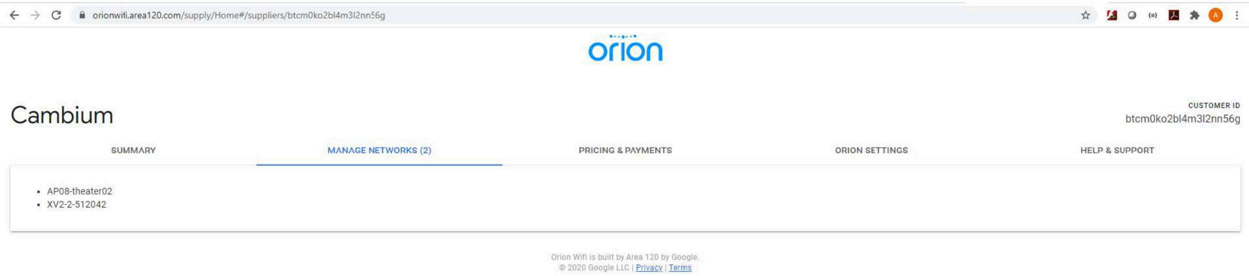
*0 - Clients Selected

## Cambium Networks and Orion Wi-Fi Integration



| | |
|---|---|
| Managed Account: | 01_Cal Customer |
| IP: | 172.20.10.52 |
| IPv6: | |
| Band: | 5GHz |
| MAC: | 52:67:81:82:B2:98 |
| Name: | iPhone |
| User: | 87d63385-b82f-4b21-8fcc-53943d0 |
| Mode: | ac |
| Manufacturer: | [Local MAC] |
| Type: | - |
| OS: | Other |
| SSID: | OrionWiFi |
| RSSI: | -53 dBm |
| AP MAC: | 00:04:56:9B:3D:70 |
| Connected AP: | AP08-theater02 |
| Capabilities: | - |
| Rate: | 104 Mbps |
| Upload: | 100.3 KB |
| Download: | 201.9 KB |
| SNR: | 42 dB |
| VLAN: | 12 |
| Guest Access Type: | - |
| Auth Status: | false |
| Session Expiry: | 0d 0h 0m |
| Mode: | |
| Client Type: | Client |
| Total Quota: | - |
| Total Quota Balance: | 0 |
| Upload Quota: | 0 |
| Download Quota: | 0 |
| Upload Quota Balance: | 0 |

### Login to your Orion account and confirm “Manage Network” should show the APs



Cambium

CUSTOMER ID
btcm0ko2bl4m3l2nn56g

- AP08-theater02
- XV2-2-512042

Orion Wifi is built by Area 120 by Google.
© 2020 Google LLC | Privacy | Terms

## CLI configuration of Orion Wi-Fi

**For reference, please find the CLI configuration for Orion Wi-Fi, radius server is pointing to the Ubuntu VM**

```
wireless wlan 1
ssid OrionWiFi
no shutdown
vlan 12
security wpa2-enterprise
no protected-mgmt-frames
passphrase $crypt$1$MATOIvimGr0WhHYcqQYU/MyOQchlnP/W
band both
dtim-interval 1
max-associated-client 127
proxy-arp
network-policy-id 0
mac-authentication policy deny
radius-server authentication host 1 172.20.10.59
radius-server authentication secret 1 $crypt$1$U2gc7eq8oDcCYl8kN/5PhZRKNR637dGz
radius-server called-sta-id AP-MAC:SSID
radius-server rad-attr service-type 1
radius-server accounting host 1 172.20.10.59
radius-server accounting secret 1 $crypt$1$YM1Ff7J/7rmXJiGn1XSCqsxeIs7QxRTf
radius-server accounting interim-update-interval 1800
radius-server accounting mode start-interim-stop
radius-server accounting acct-on
passpoint
passpoint interworking internet
passpoint interworking access-network-type chargeable-public
passpoint interworking venue-group 6
passpoint interworking venue-type 4
passpoint roam-cons F4F5E8F5F4
passpoint anqp nai-realm 1 name Orion-Realm
passpoint anqp nai-realm 1 eap 1 method eap-tls
passpoint anqp nai-realm 1 eap 1 auth 1 inner-auth-eap certificate
passpoint anqp domain-names orionwifi.com
no guest-access
!
```