ARISTA

Arista Guardian for Network Identity (AGNI) User Guide

www.arista.com

Arista NetVisor Version 2023.4.0
DOC-06557-02

Headquarters	Support	Sales
5453 Great America Parkway		
Santa Clara, CA 95054, USA	+1-408 547-5502	+1-408 547-5501
+1-408-547-5500	+1-866 476-0000	+1-866 497-0000
www.arista.com	support@arista.com	sales@arista.com

Introduction

This document provides information about Arista Networks' Arista Guardian for Network Identity (AGNI) software. The document explains in detail the various configuration options present in the AGNI portal. The URLs, credential information, and user objects mentioned in this document are for illustration purposes only. Use the values pertinent to your organization while configuring AGNI.

Pre-Requisite

You must log in as a network administrator to access and configure the AGNI portal.

Accessing the UI

AGNI provides single sign-on (SSO) integration with Arista Wi-Fi Launchpad for login and logout functionalities. You can access AGNI via the Arista Wi-Fi Launchpad.

The user management and other access control mechanisms are performed through the Arista Wi-Fi Launchpad. You can log in to Arista Wi-Fi Launchpad and navigate to the AGNI tile on the dashboard (see image below).

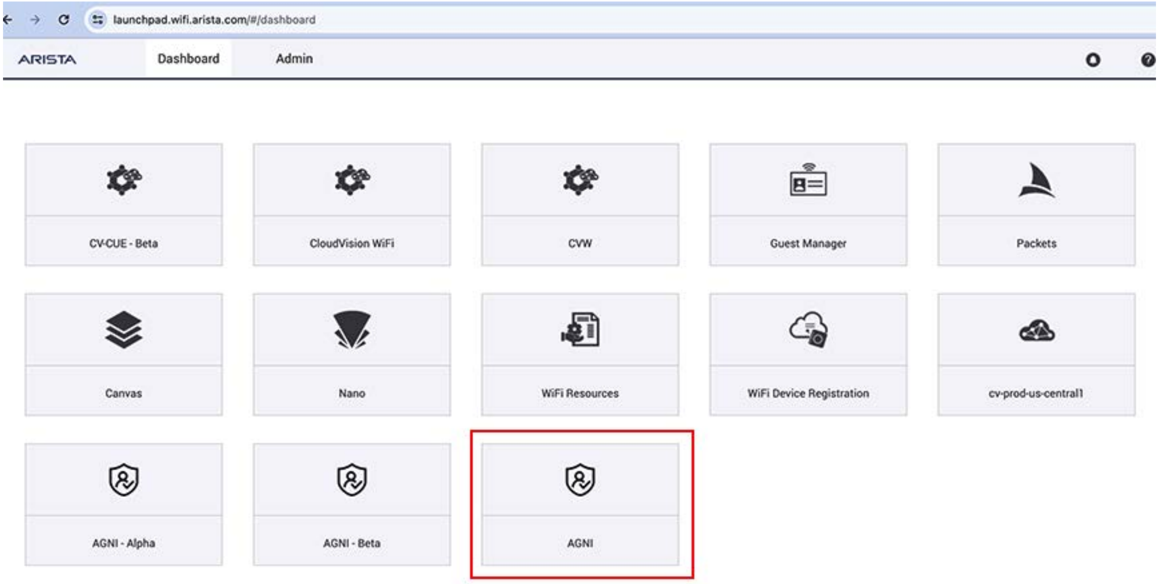


Figure: Arista Launchpad Displaying AGNI and Other Applications

On the Wi-Fi Launchpad, click on the AGNI tile, and the application redirects you to the AGNI portal. The Admin Console provides administration, configuration, monitoring, and troubleshooting of AGNI.

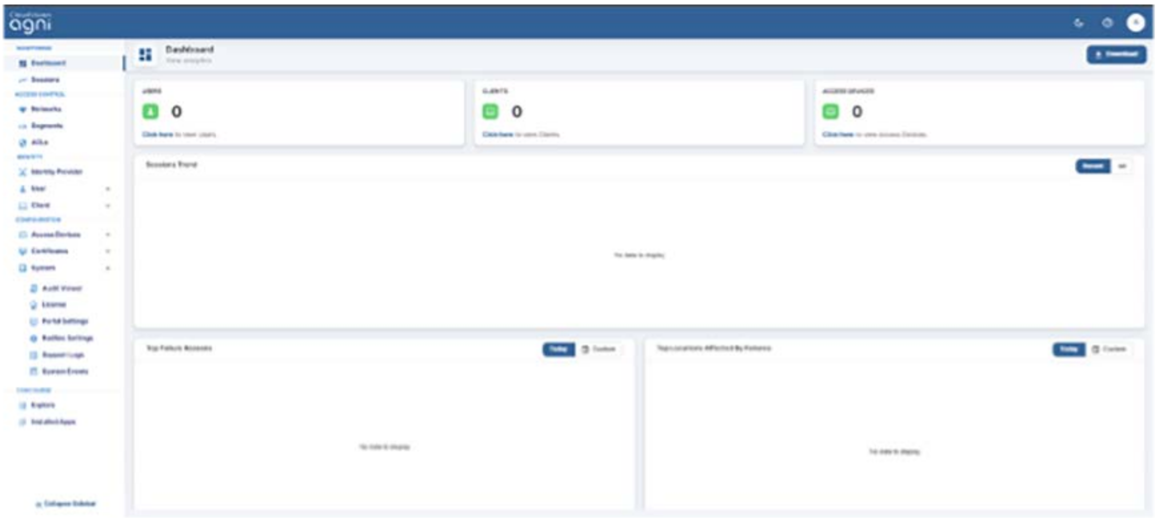
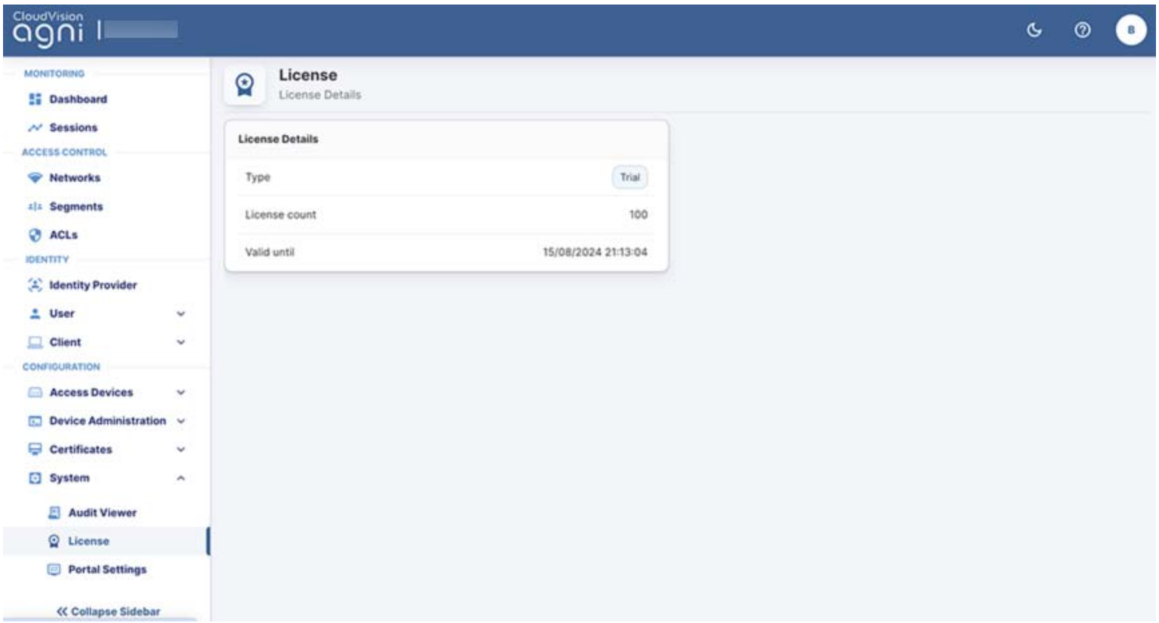


Figure: AGNI Dashboard

Viewing the Licensing Details

To view the licensing details, log in as a network administrator and navigate to: **Configuration→ System → License** (see image below).



License
License Details

License Details

Type	Trial
License count	100
Valid until	15/08/2024 21:13:04

Figure: AGNI License Details

User Interface (UI) Theme

AGNI user interface (UI) offers different themes and modes and as a network admin, you can use any theme of your preference. Then, by default, the system theme gets applied to AGNI UI. Additionally, you can change the placement of options on the UI. That is, you can move the option bar to the top, bottom, or left side of the page.

To change the theme and the placement of options, select **Navigation** from the top right side of the portal (see image below).

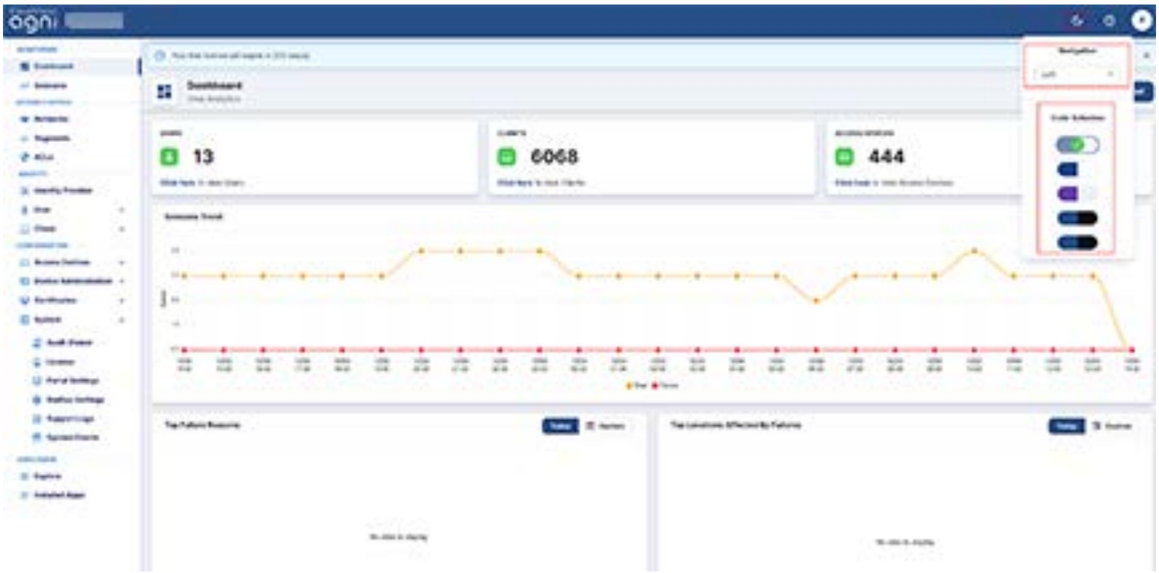


Figure: AGNI UI Theme (Navigation & Color) Settings

Third-Party Integrations

AGNI can integrate with various Arista and third-party applications by configuring the Concourse Application (see image below).

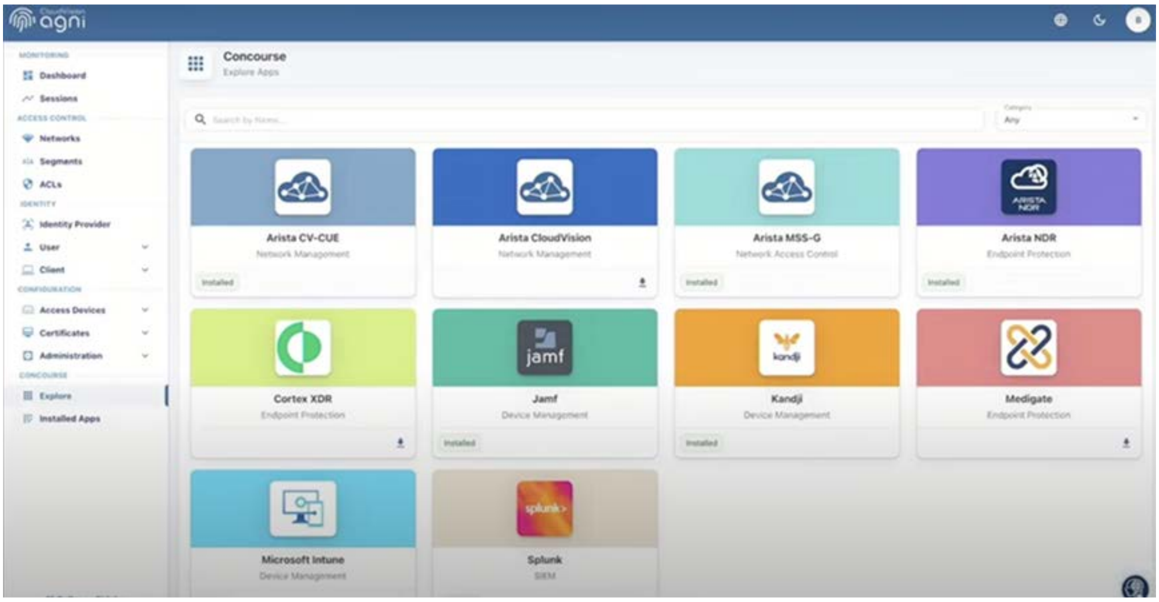


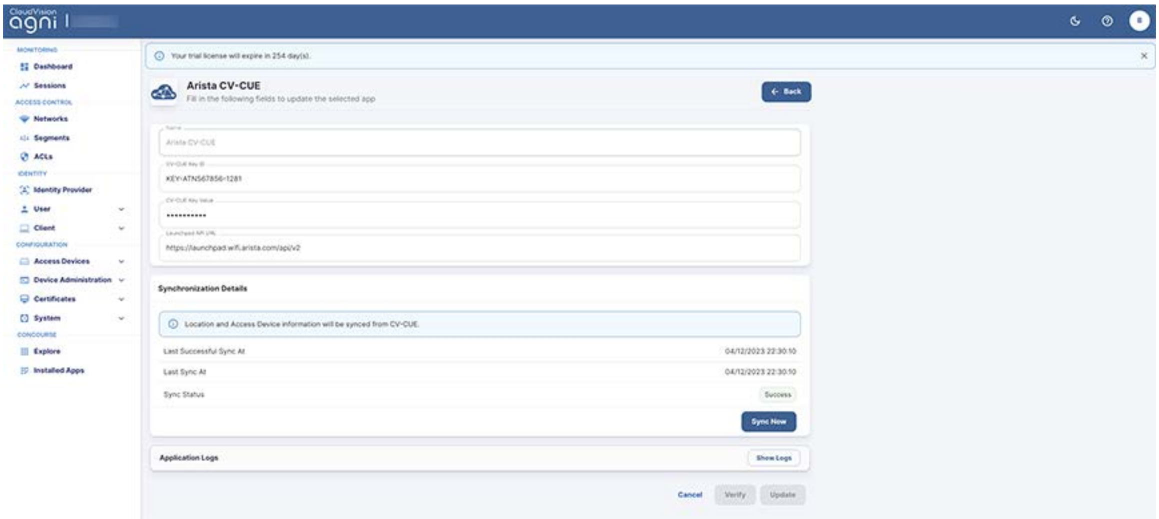
Figure:AGNI Concourse Applications

CV-CUE Integration

Arista's CloudVision Cognitive Unified Edge (CV-CUE) delivers an integrated management platform with built-in automation, visibility and security capabilities for wireless, wired, and WAN network infrastructure. For details, see the CV-CUE product documentation on Arista website.

You can integrate CV-CUE by installing the application as a Concourse App on the AGNI portal. To install CV-CUE:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Arista CV-CUE** application
3. Enter the following parameters:
    a. Arista CV-CUE in the **Name** field
    b. CV-CUE Key ID
    c. CV-CUE Key Value



Your trial license will expire in 254 day(s).

Arista CV-CUE

Fill in the following fields to update the selected app

Name: Arista CV-CUE

CV-CUE Key ID: KEY-ATN567856-1281

CV-CUE Key Value: ••••••••••

Launchpad API URL: https://launchpad.wifi.arista.com/api/v2

Synchronization Details

Location and Access Device information will be synced from CV-CUE.

Last Successful Sync At 04/12/2023 22:30:10

Last Sync At 04/12/2023 22:30:10

Sync Status Success

Application Logs

Figure: Installing Arista CV-CUE Concourse Application

4. Click the **Verify** button to validate the credentials
5. Click the **Install** button to complete the installation process.

The CV-CUE application gets displayed as an installed application in Concourse page.

6. Click the Sync Now button on the Arista CV-CUE page to initiate the synchronization process.

You can view the synchronized WiFi details by navigating to the: **Configuration** -> **Access Devices** -> **Devices**.

CloudVision Integration

CloudVision® is Arista's modern, multi-domain management platform that leverages cloud networking principles to deliver a simplified NetOps experience and enables zero-touch network operations. For details, see the CloudVision product documentation on Arista website.

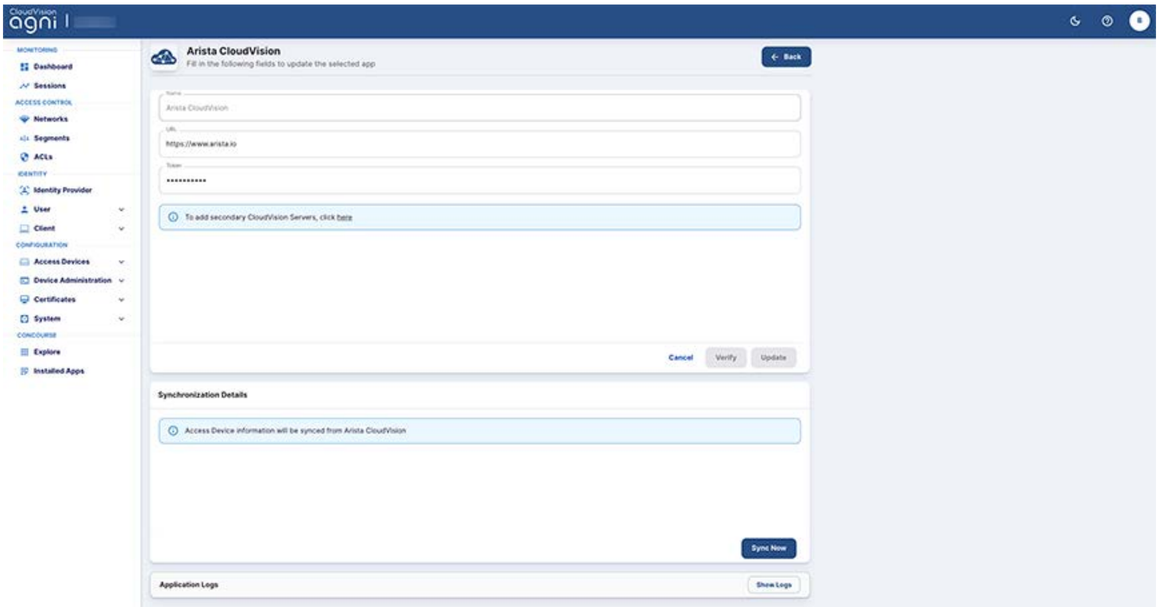
The integration of CloudVision enables AGNI to fetch the details of all the managed wired switches. These details are synchronized with AGNI and information such as MAC address and network device name are available as premium entities within AGNI while configuring segmentation policies.

Pre-requisites

The CloudVision integration requires an API token with necessary permissions to fetch the managed switch details. You can get the token from the CloudVision interface.

You can integrate CloudVision by installing the application as a Concourse App on the AGNI portal. To install CloudVision:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Arista CloudVision** application



Arista CloudVision
Fill in the following fields to update the selected app

Name: Arista CloudVision

URL: https://www.arista.io

Token: ••••••••••

To add secondary CloudVision Servers, click here

Synchronization Details

Access Device information will be synced from Arista CloudVision

Application Logs

Figure: Installing Arista CloudVision Concourse Application

3. Enter the following parameters:
    a. Arista CloudVision in the **Name** field
    b. The URL of the CloudVision application
    c. API Token value
4. Click the **Verify** button to validate the credentials
5. Click the **Install** button to complete the installation process.

The CloudVision application gets displayed as an installed application in the Concourse page.

6. Click the **Sync Now** button on the Arista CloudVision page to initiate the synchronization process.

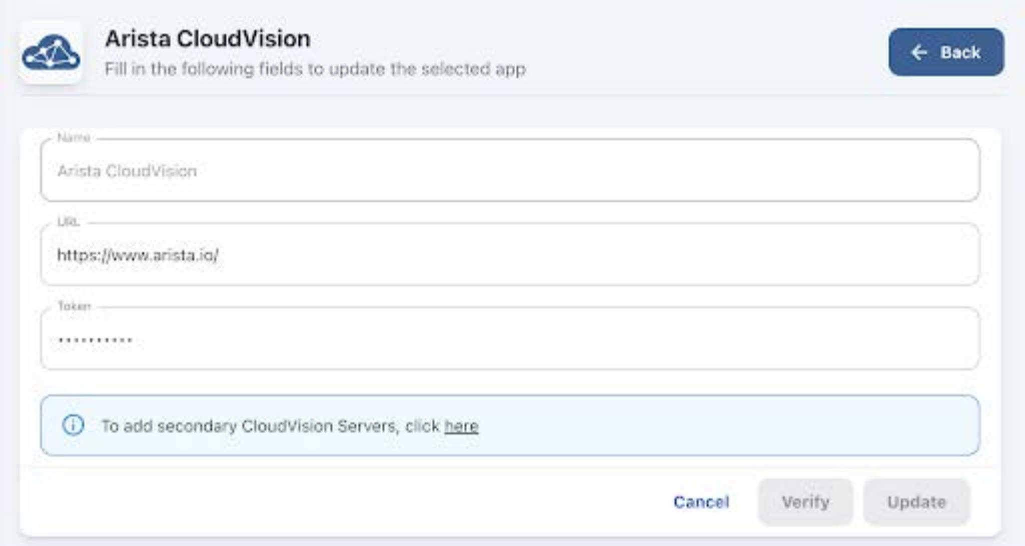
You can view the synchronized switch details by navigating to the: **Configuration** -> **Access Devices** -> **Devices**.

Adding Multiple CVaaS Instances in AGNI

This section describes the steps to configure multiple CVaaS instances linked to AGNI. When you add multiple CVaaS instances, AGNI fetches all the managed switches and adds them to the AGNI database. To add multiple CVaaS instances, you must log in as an admin and complete the AGNI configuration.

Configuring CVaas Instances

1. Log in to AGNI and navigate to **Concourse-> Explore-> Arista CloudVision**.
2. Add a CVaaS instance URL and Token to add a primary CVaaS in AGNI.
3. Click **Update** to save the profile.



Arista CloudVision

Fill in the following fields to update the selected app

Name: Arista CloudVision

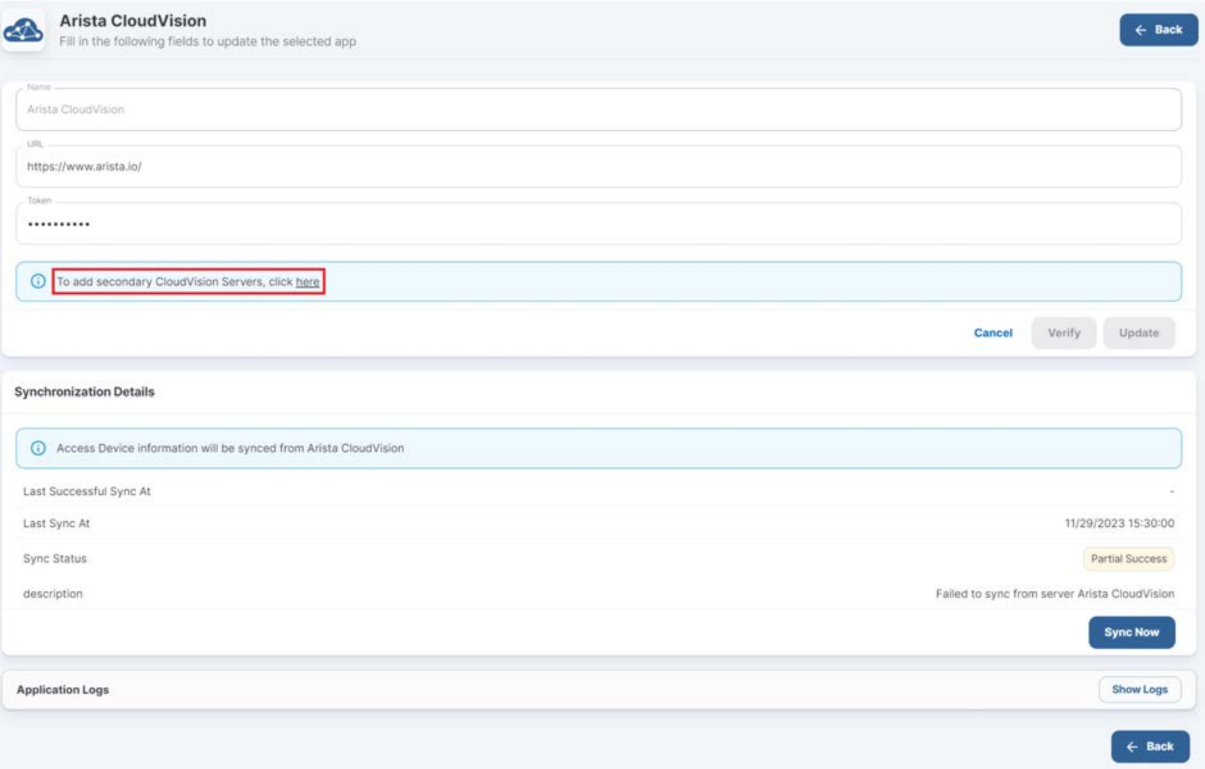
URL: https://www.arista.io/

Token: ••••••••••

To add secondary CloudVision Servers, click here

Figure: Updating Arista CloudVision Course App

4. To add multiple CVaaS instances, click **here** while editing the previously added CVaaS profile (see the highlighted text in the image below).



Arista CloudVision

Fill in the following fields to update the selected app

Name: Arista CloudVision

URL: https://www.arista.io/

Token: ••••••••••

To add secondary CloudVision Servers, click here

Synchronization Details

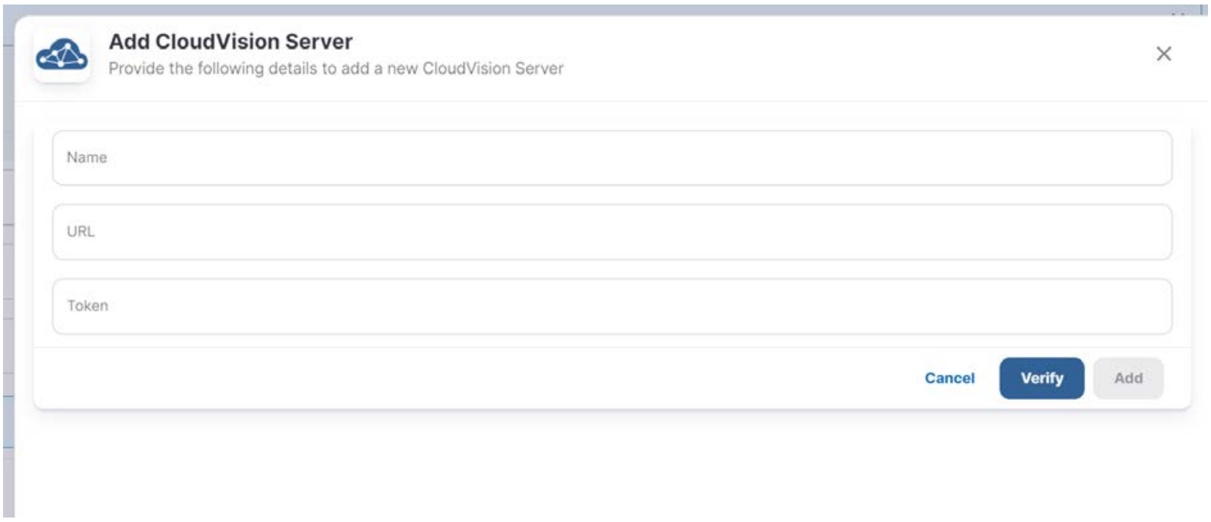
Access Device information will be synced from Arista CloudVision

Last Successful Sync At	-
Last Sync At	11/29/2023 15:30:00
Sync Status	Partial Success
description	Failed to sync from server Arista CloudVision

Application Logs

Figure: Adding Secondary Servers

5. On the displayed pop-up window, add the secondary CVaaS URL and API Token.



Add CloudVision Server

Provide the following details to add a new CloudVision Server

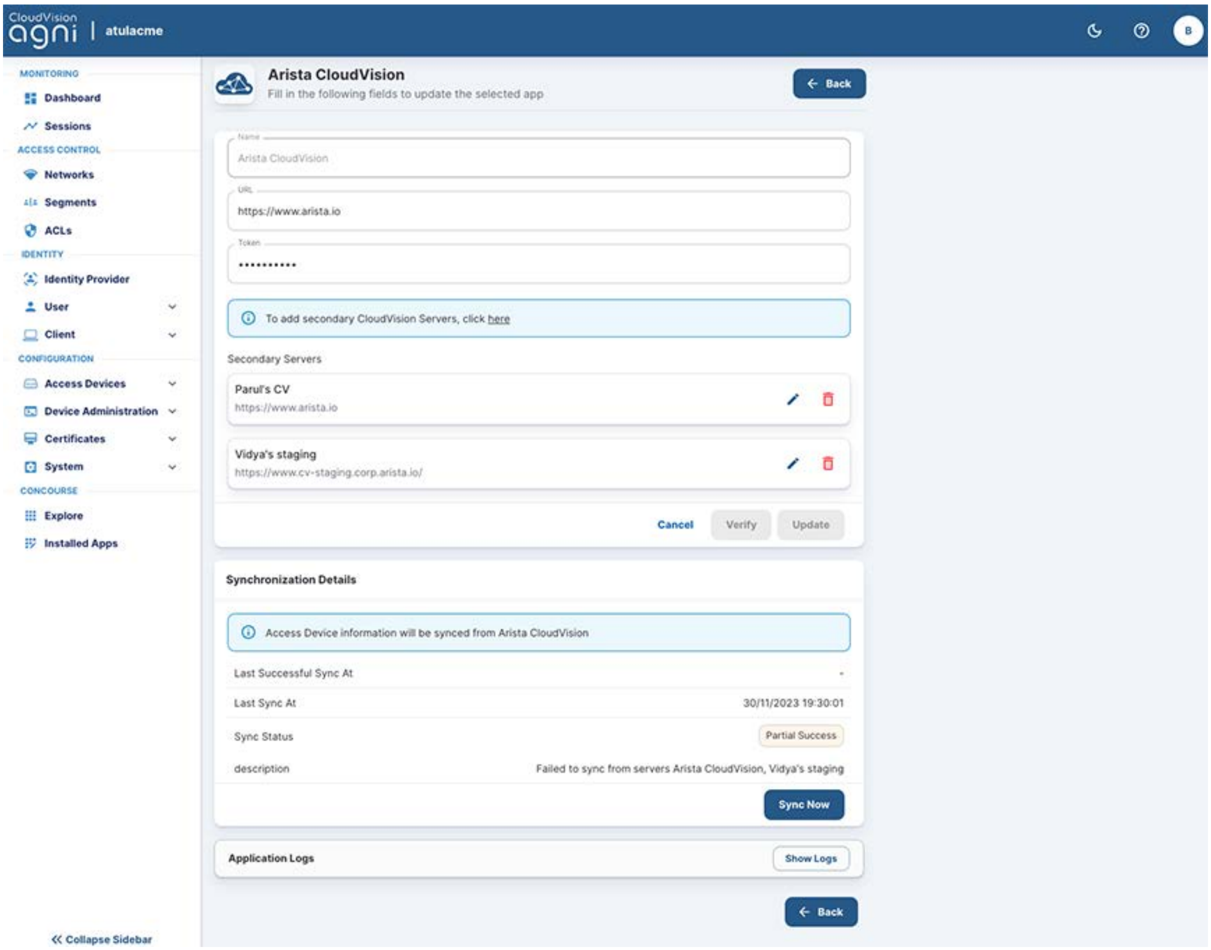
Name

URL

Token

Figure: Adding CloudVision Server

6. Click **Add** to save the secondary CVaaS. The dashboard displays multiple CVaaS instances in the Concourse application (see image below).



Arista CloudVision

Fill in the following fields to update the selected app

Name: Arista CloudVision

URL: https://www.arista.io

Token: ••••••••••

To add secondary CloudVision Servers, click here

Secondary Servers

Parul's CV
https://www.arista.io

Vidya's staging
https://www.cv-staging.corp.arista.io/

Synchronization Details

Access Device information will be synced from Arista CloudVision

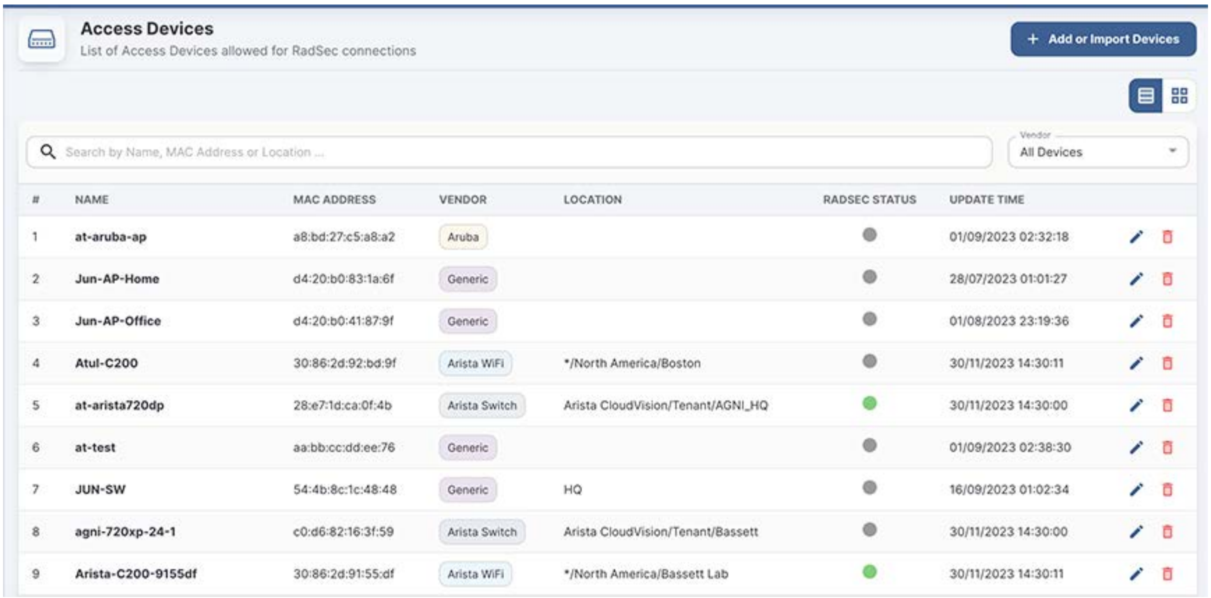
Last Successful Sync At	-
Last Sync At	30/11/2023 19:30:01
Sync Status	Partial Success
description	Failed to sync from servers Arista CloudVision, Vidya's staging

Application Logs

Figure: CVaaS Synchronization Details

After multiple CVaaS instances are added, the switches managed by those instances are synchronized in AGNI. To verify the device list, navigate to **Configuration**-> **Access**

Devices-> **Devices** on the AGNI portal. All the switches managed by multiple CVaaS instances are displayed in the device list (see image below). Admin can determine the CVaaS managing the switch by the location of the switch.



Access Devices

List of Access Devices allowed for RadSec connections

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS	UPDATE TIME
1	at-aruba-ap	a8:bd:27:c5:a8:a2	Aruba		●	01/09/2023 02:32:18
2	Jun-AP-Home	d4:20:b0:83:1a:6f	Generic		●	28/07/2023 01:01:27
3	Jun-AP-Office	d4:20:b0:41:87:9f	Generic		●	01/08/2023 23:19:36
4	Atul-C200	30:86:2d:92:bd:9f	Arista WiFi	*/North America/Boston	●	30/11/2023 14:30:11
5	at-arista720dp	28:e7:1d:ca:0f:4b	Arista Switch	Arista CloudVision/Tenant/AGNI_HQ	🟢	30/11/2023 14:30:00
6	at-test	aa:bb:cc:dd:ee:76	Generic		●	01/09/2023 02:38:30
7	JUN-SW	54:4b:8c:1c:48:48	Generic	HQ	●	16/09/2023 01:02:34
8	agni-720xp-24-1	c0:d6:82:16:3f:59	Arista Switch	Arista CloudVision/Tenant/Bassett	●	30/11/2023 14:30:00
9	Arista-C200-9155df	30:86:2d:91:55:df	Arista WiFi	*/North America/Bassett Lab	🟢	30/11/2023 14:30:11

Figure: Access Devices

MSS-G Integration

Multi-Domain Macro-Segmentation Service Group (MSS-G) is a security feature that allows users to classify network endpoints into segments and define forwarding policies between segments. For details, see the *Multi-Domain Macro-Segmentation Service Group (MSS-G) Design & Deployment Guide* on Arista website.

The integration of this feature with AGNI enables MSS-G enforcement based upon the segmentation conditions of an incoming access request through AGNI. This integration facilitates AGNI to fetch the segment details from CloudVision within the context of MSS-G enforcement. The details are then synchronized with AGNI and the MSS-G segments are available as premium entities within AGNI while configuring the segmentation policies.

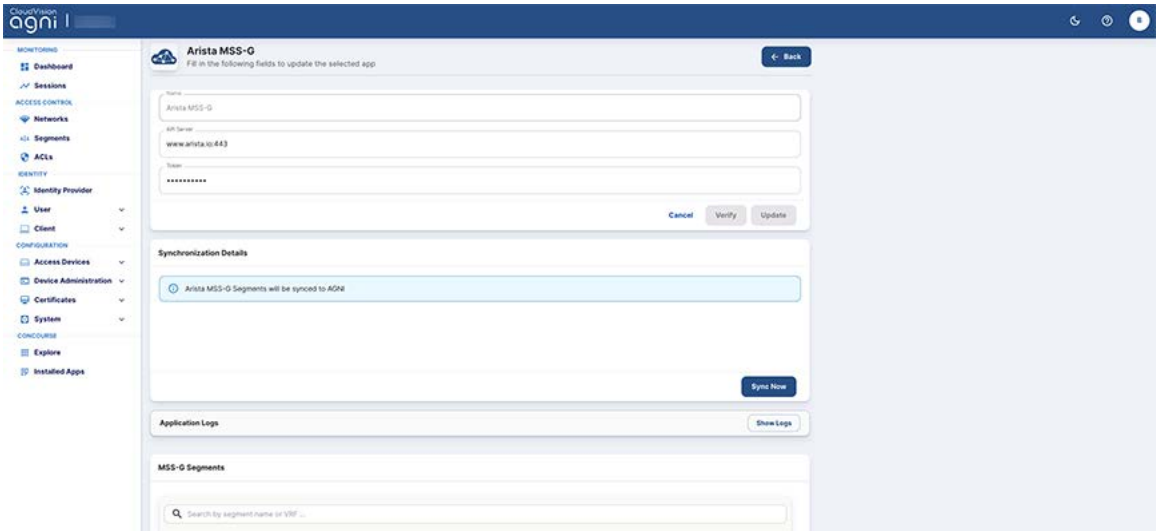
Prerequisites

The MSS-G integration requires an API token with necessary permissions to fetch the MSS-G segment details. You can get the token from the CloudVision interface.

Integration

You can integrate MSS-G by installing the application as a Concourse App on the AGNI portal. To install CV-CUE:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Arista MSS-G** application



Arista MSS-G
Fill in the following fields to update the selected app

Name: Arista MSS-G
API Server: www.arista.io:443
Token: ••••••••••

Synchronization Details
Arista MSS-G Segments will be synced to AGNI

Application Logs

MSS-G Segments

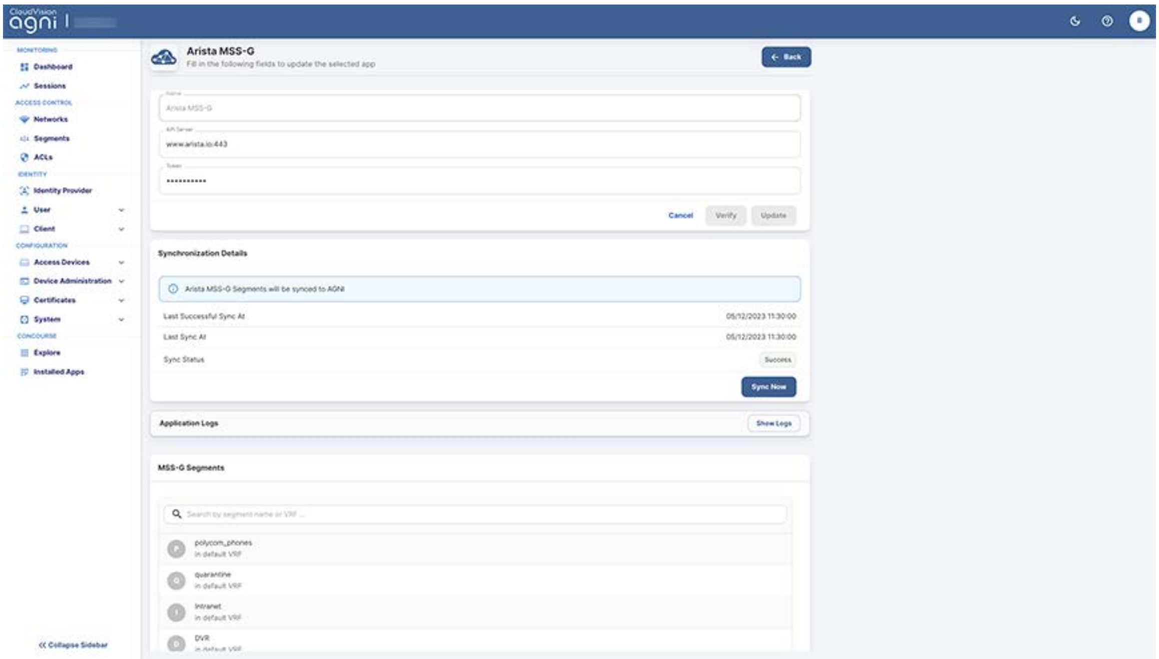
Figure: Installing Arista MSS-G Concourse Application

3. Enter the following parameters:
    a. Arista MSS-G in the **Name** field
    b. The API server URL and port number
    c. API Token value
4. Click the **Verify** button to validate the credentials
5. Click the **Install** button to complete the installation process.

The Arista MSS-G application gets displayed as an installed application in the Concourse page.

6. Click the **Sync Now** button on the Arista MSS-G page to initiate the synchronization process.

You can view the synchronized MSS-G details by navigating to the: **Concourse** -> **Installed Apps** -> **Arista MSS-G** (see image below).



Arista MSS-G
Fill in the following fields to update the selected app

Name: Arista MSS-G
API Server: www.arista.io:443
Token: ••••••••••

Synchronization Details

Arista MSS-G Segments will be synced to AGNI

Last Successful Sync At	05/12/2023 11:30:00
Last Sync At	05/12/2023 11:30:00
Sync Status	Success

Application Logs

MSS-G Segments

Search by segment name or VRF ...

polycom_phones
in default VRF

quarantine
in default VRF

Intranet
in default VRF

DVR
in default VRF

Figure: Installed Arista MSS-G Concourse Application

Arista NDR Integration

This section describes the process of integrating Arista NDR with AGNI to achieve the post-authentication profiling.

To integrate with AGNI version 2023.4.0, you should have Arista NDR version 5.1.0.
To integrate Arista NDR with AGNI:

- Navigate to ***Concourse-> Explore***. Select the **Arista NDR** application.

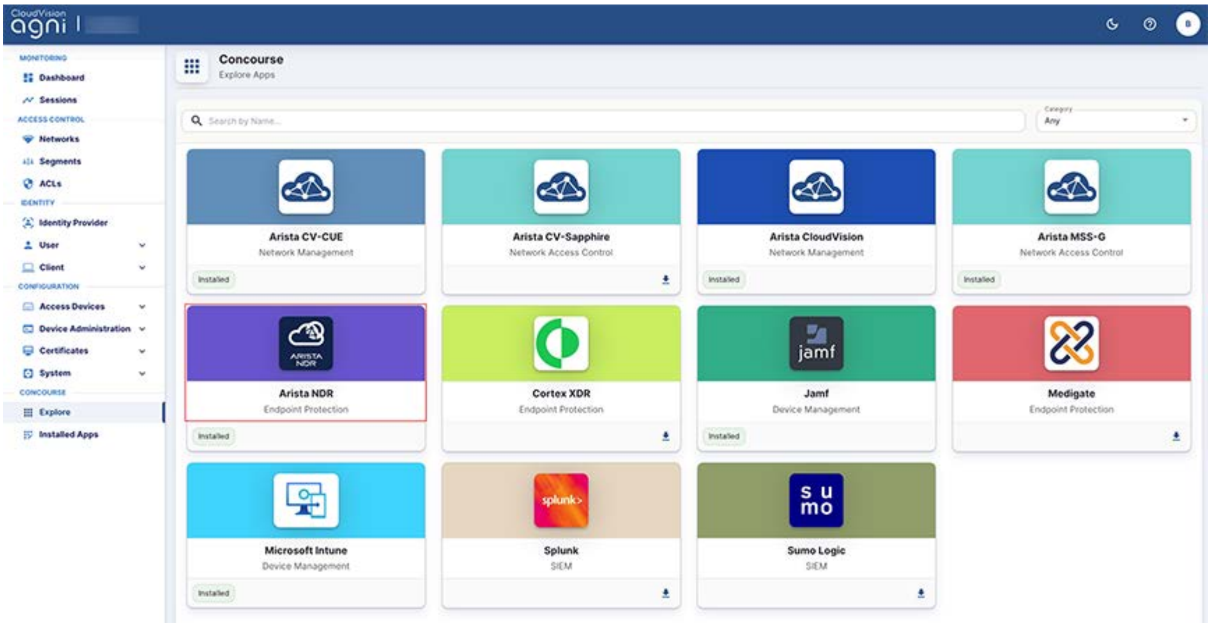
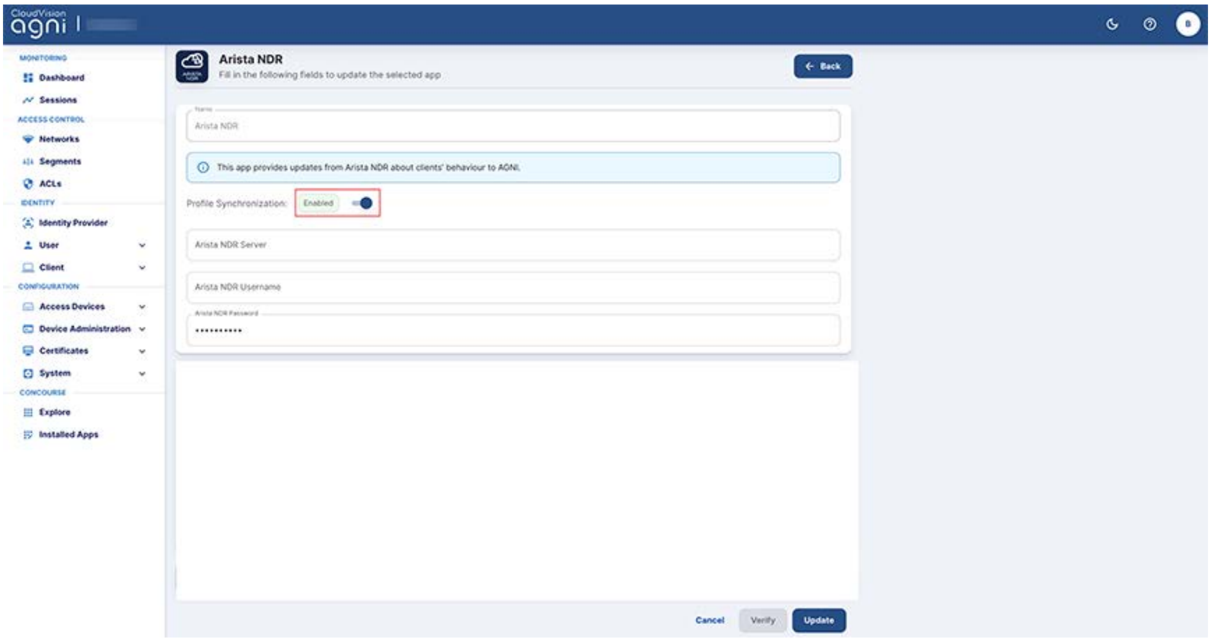


Figure : Arista NDR in Concourse App

- Enable **Profile Synchronization** and provide the **NDR server**, **username** and **password**.



Arista NDR
Fill in the following fields to update the selected app

Name
Arista NDR

This app provides updates from Arista NDR about clients' behaviour to AGNI.

Profile Synchronization: Enabled

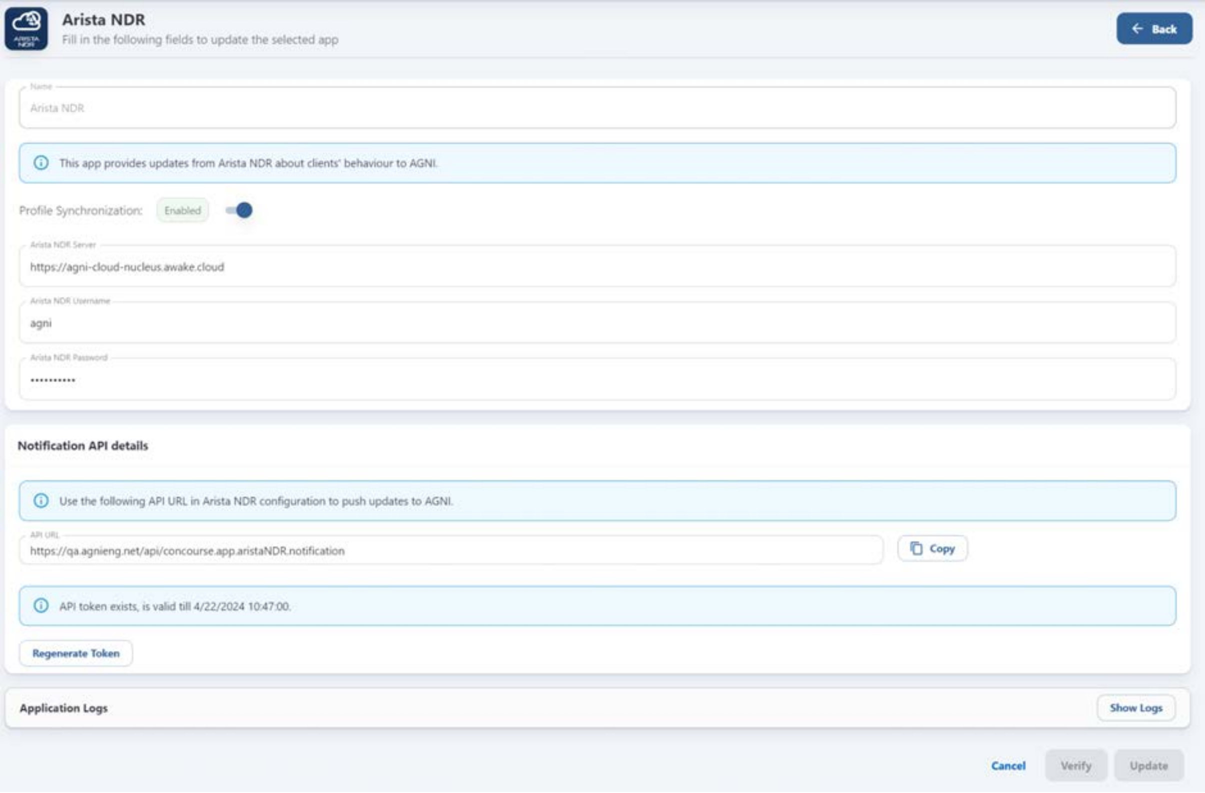
Arista NDR Server

Arista NDR Username

Arista NDR Password
••••••••••

Figure: Arista NDR Integration

- Click the **Verify** button to verify the details
- Click the **Install** button to Install the application. The AGNI API URL and an API token are generated. These details are used in the NDR solution to integrate with AGNI.
  Note: The Token is displayed only once at the install time.



Arista NDR
Fill in the following fields to update the selected app

Name
Arista NDR

This app provides updates from Arista NDR about clients' behaviour to AGNI.

Profile Synchronization: Enabled

Arista NDR Server
https://agni-cloud-nucleus.awake.cloud

Arista NDR Username
agni

Arista NDR Password
••••••••••

Notification API details

Use the following API URL in Arista NDR configuration to push updates to AGNI.

API URL
https://qa.agnieng.net/api/concourse.app.aristaNDR.notification

API token exists, is valid till 4/22/2024 10:47:00.

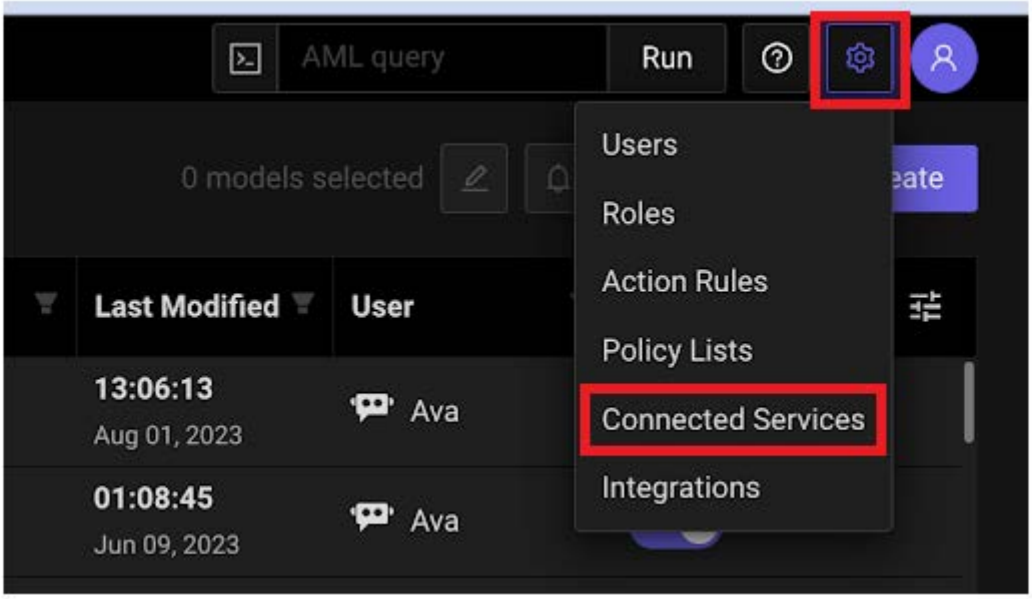
Application Logs

Figure: Arista NDR Integration page-2

Configuring Arista NDR

To configure Arista NDR:

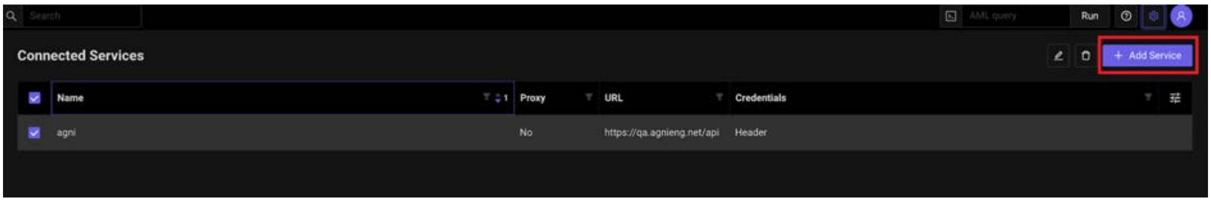
- Login to Arista NDR and navigate to the **Settings** option next to **User details** and select the **Connected Services** option (see image below).



Last Modified	User
13:06:13 Aug 01, 2023	Ava
01:08:45 Jun 09, 2023	Ava

Figure: Arista NDR Configuration Settings Page

- Click on the **Add Service** option to add a new connected service in NDR (see image below).

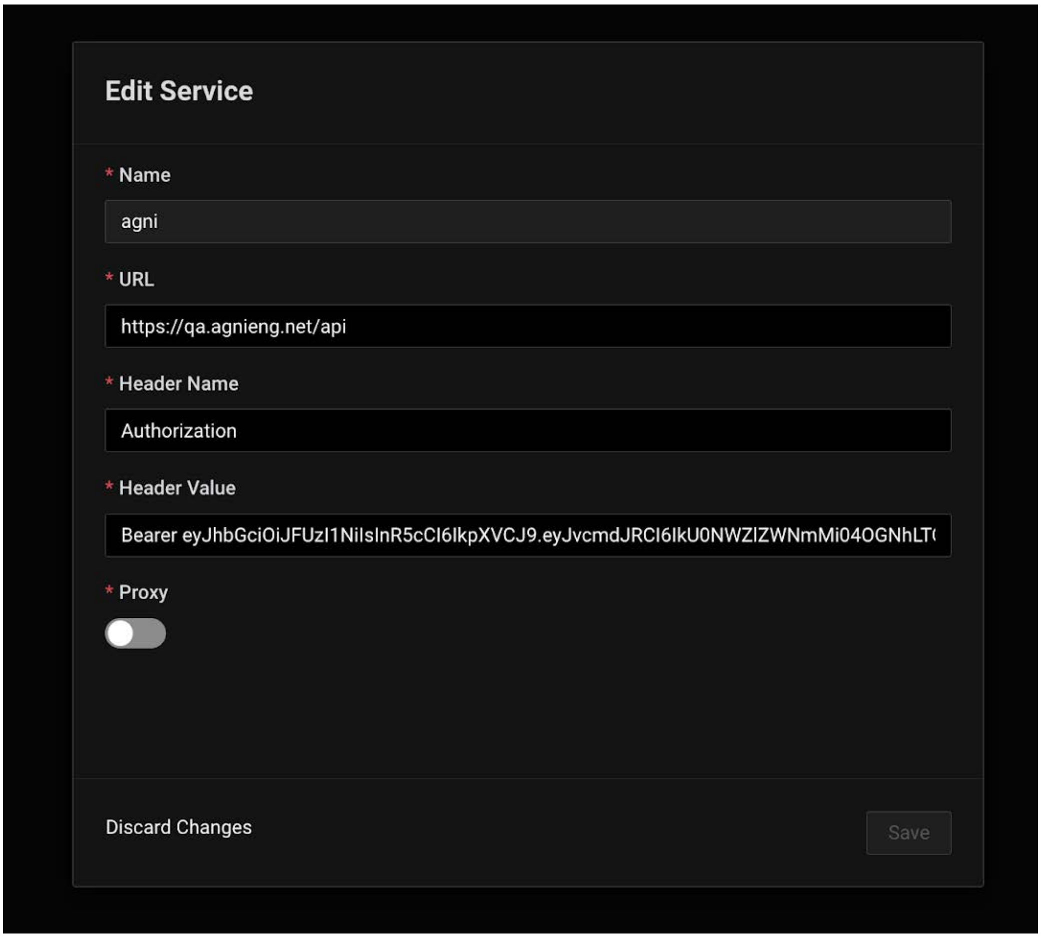


Connected Services

☑	Name	Proxy	URL	Credentials
☑	agni	No	https://qa.agnieng.net/api	Header

Figure: Arista NDR Configuration - Add Service

- Add the AGNI API URL and API Token generated previously in the AGNI Integration section.



* Name

agni

* URL

https://qa.agnieng.net/api

* Header Name

Authorization

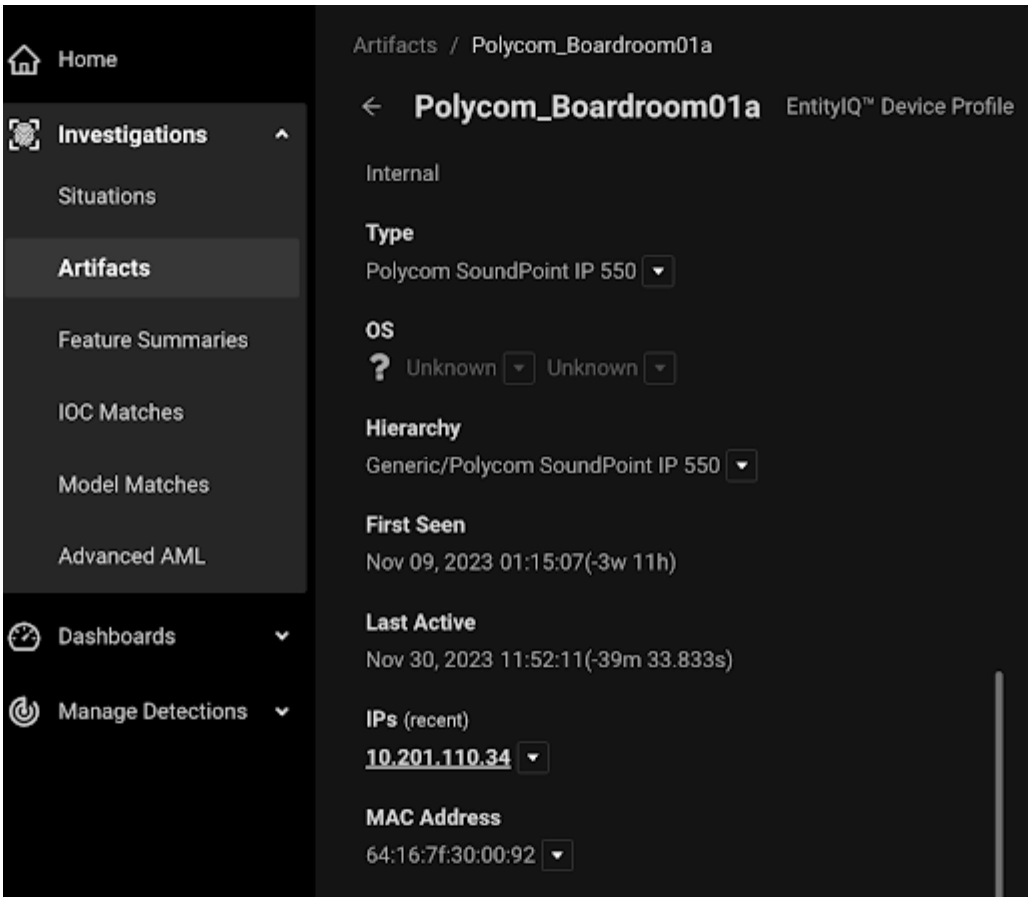
* Header Value

Bearer eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IkU0NWZlZWNmMi04OGNhLT

* Proxy

Figure: Arista NDR Configuration Details

- Click **Save** button to add AGNI service to NDR.
- Navigate to **Investigations**-> **Artifacts** from the left panel



Artifacts / Polycom_Boardroom01a

Polycom_Boardroom01a EntityIQ™ Device Profile

Internal

Type
Polycom SoundPoint IP 550

OS
Unknown Unknown

Hierarchy
Generic/Polycom SoundPoint IP 550

First Seen
Nov 09, 2023 01:15:07(-3w 11h)

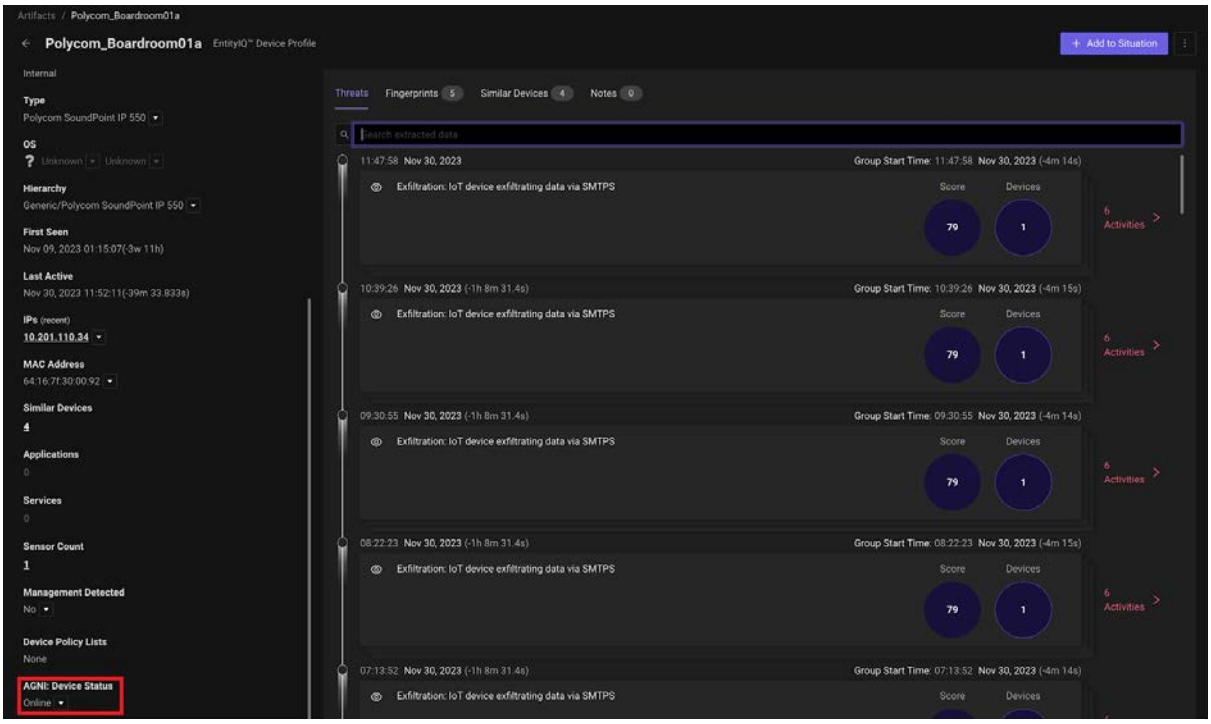
Last Active
Nov 30, 2023 11:52:11(-39m 33.833s)

IPs (recent)
10.201.110.34

MAC Address
64:16:7f:30:00:92

Figure: Arista NDR Configuration Artifacts Details

- Select the device authenticated through AGNI from the list. Verify that AGNI Device Status is **Online** for the device. The Online status indicates successful integration of AGNI and Arista NDR.



Artifacts / Polycom_Boardroom01a

Polycom_Boardroom01a EntityIQ™ Device Profile

Internal

Type
Polycom SoundPoint IP 550

OS
Unknown Unknown

Hierarchy
Generic/Polycom SoundPoint IP 550

First Seen
Nov 09, 2023 01:15:07(-3w 11h)

Last Active
Nov 30, 2023 11:52:11(-39m 33.833s)

IPs (recent)
10.201.110.34

MAC Address
64:16:7f:30:00:92

Similar Devices
4

Applications
0

Services
0

Sensor Count
1

Management Detected
No

Device Policy Lists
None

AGNI: Device Status
Online

11:47:58 Nov 30, 2023 — Group Start Time: 11:47:58 Nov 30, 2023 (-4m 14s)
Exfiltration: IoT device exfiltrating data via SMTPS — Score 79 — Devices 1 — 6 Activities

10:39:26 Nov 30, 2023 (-1h 8m 31.4s) — Group Start Time: 10:39:26 Nov 30, 2023 (-4m 15s)
Exfiltration: IoT device exfiltrating data via SMTPS — Score 79 — Devices 1 — 6 Activities

09:30:55 Nov 30, 2023 (-1h 8m 31.4s) — Group Start Time: 09:30:55 Nov 30, 2023 (-4m 14s)
Exfiltration: IoT device exfiltrating data via SMTPS — Score 79 — Devices 1 — 6 Activities

08:22:23 Nov 30, 2023 (-1h 8m 31.4s) — Group Start Time: 08:22:23 Nov 30, 2023 (-4m 15s)
Exfiltration: IoT device exfiltrating data via SMTPS — Score 79 — Devices 1 — 6 Activities

07:13:52 Nov 30, 2023 (-1h 8m 31.4s) — Group Start Time: 07:13:52 Nov 30, 2023 (-4m 14s)
Exfiltration: IoT device exfiltrating data via SMTPS — Score — Devices

Figure: Arista NDR - AGNI Integration Status

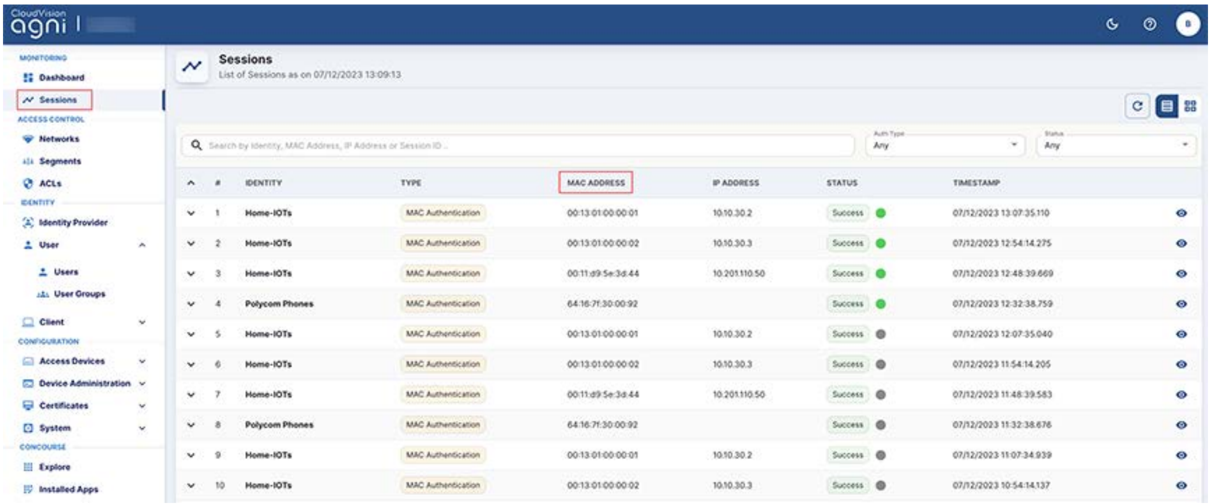
Configuring Segment Policies

After the successful integration of AGNI with Arista NDR, as a newtork admin, you can configure the segments in AGNI based on the parameters synchronised with NDR. This enables AGNI to leverage the profiling information through NDR.

The profiling information includes - Device Brand, Device Hierarchy, and Device Type. The **Risk Action** is administrator-driven. This is pushed to AGNI at the discretion of the administrator when the device is deemed risky through the NDR detection process.

You can view the list of attributes synchronized from NDR as below:

- Navigate to **Sessions** and select a device.
- Click on the MAC address of the device.

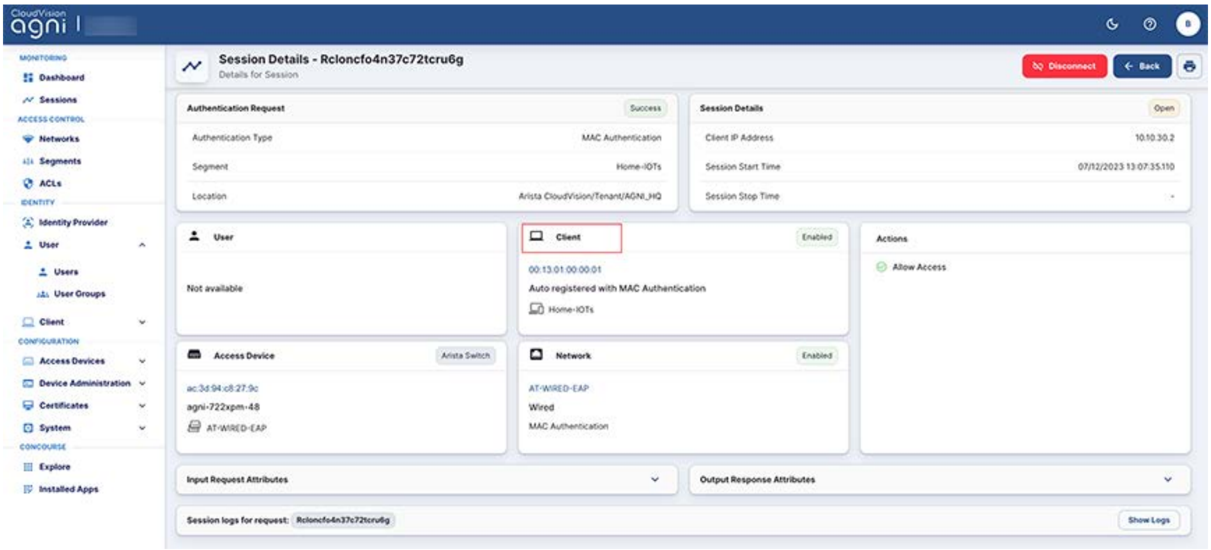


Sessions
List of Sessions as on 07/12/2023 13:09:13

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success ●	07/12/2023 13:07:35.110
2	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success ●	07/12/2023 12:54:14.275
3	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success ●	07/12/2023 12:48:39.669
4	Polycom Phones	MAC Authentication	64:16:7f:30:00:92		Success ●	07/12/2023 12:32:38.759
5	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success ●	07/12/2023 12:07:35.040
6	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success ●	07/12/2023 11:54:14.205
7	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success ●	07/12/2023 11:48:39.583
8	Polycom Phones	MAC Authentication	64:16:7f:30:00:92		Success ●	07/12/2023 11:32:38.676
9	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success ●	07/12/2023 11:07:34.939
10	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success ●	07/12/2023 10:54:14.137

Figure: Sessions Details

- In the **Client** tab, click the MAC address of the device:



Session Details - Rcloncfo4n37c72tcru6g
Details for Session

Authentication Request — Success

Authentication Type: MAC Authentication
Segment: Home-IOTs
Location: Arista CloudVision/Tenant/AGNI_HQ

Session Details — Open

Client IP Address: 10.10.30.2
Session Start Time: 07/12/2023 13:07:35.110
Session Stop Time: -

User

Not available

Client — Enabled

00:13:01:00:00:01
Auto registered with MAC Authentication
Home-IOTs

Actions

Allow Access

Access Device — Arista Switch

ac:3d:94:c8:27:9c
agni-722xpm-48
AT-WIRED-EAP

Network — Enabled

AT-WIRED-EAP
Wired
MAC Authentication

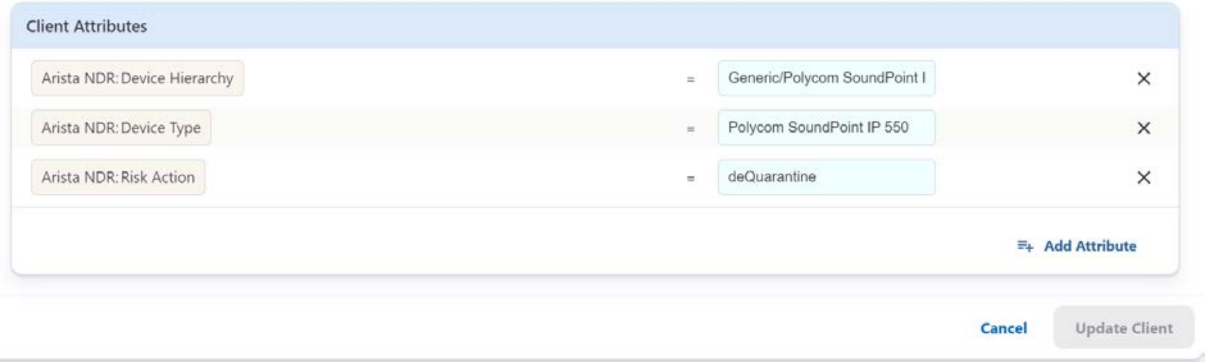
Input Request Attributes

Output Response Attributes

Session logs for request: Rcloncfo4n37c72tcru6g

Figure: Sessions Client Details

- Add the details and click Update Client:



Client Attributes

Arista NDR: Device Hierarchy = Generic/Polycom SoundPoint I

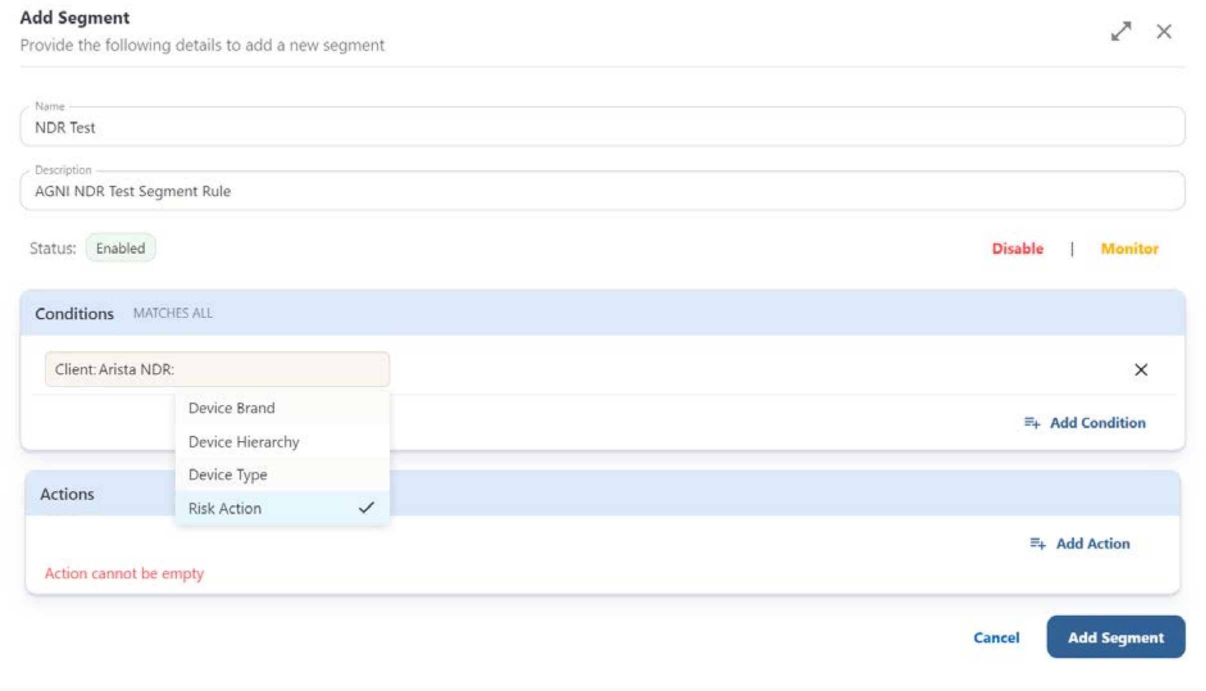
Arista NDR: Device Type = Polycom SoundPoint IP 550

Arista NDR: Risk Action = deQuarantine

Figure: NDR Client Details

The synchronized attributes can be used in the segmentation policies. The process involves:

- Navigate to ***Access Control-> Segment***
- Click **Add a Segment**. Based on the **Client-> Arista NDR**
  - **-> Device Brand**
  - **-> Device Hierarchy**
  - **-> Device Type**
  - **-> Risk Action**



Add Segment

Provide the following details to add a new segment

Name: NDR Test

Description: AGNI NDR Test Segment Rule

Status: Enabled

Conditions MATCHES ALL

Client: Arista NDR:

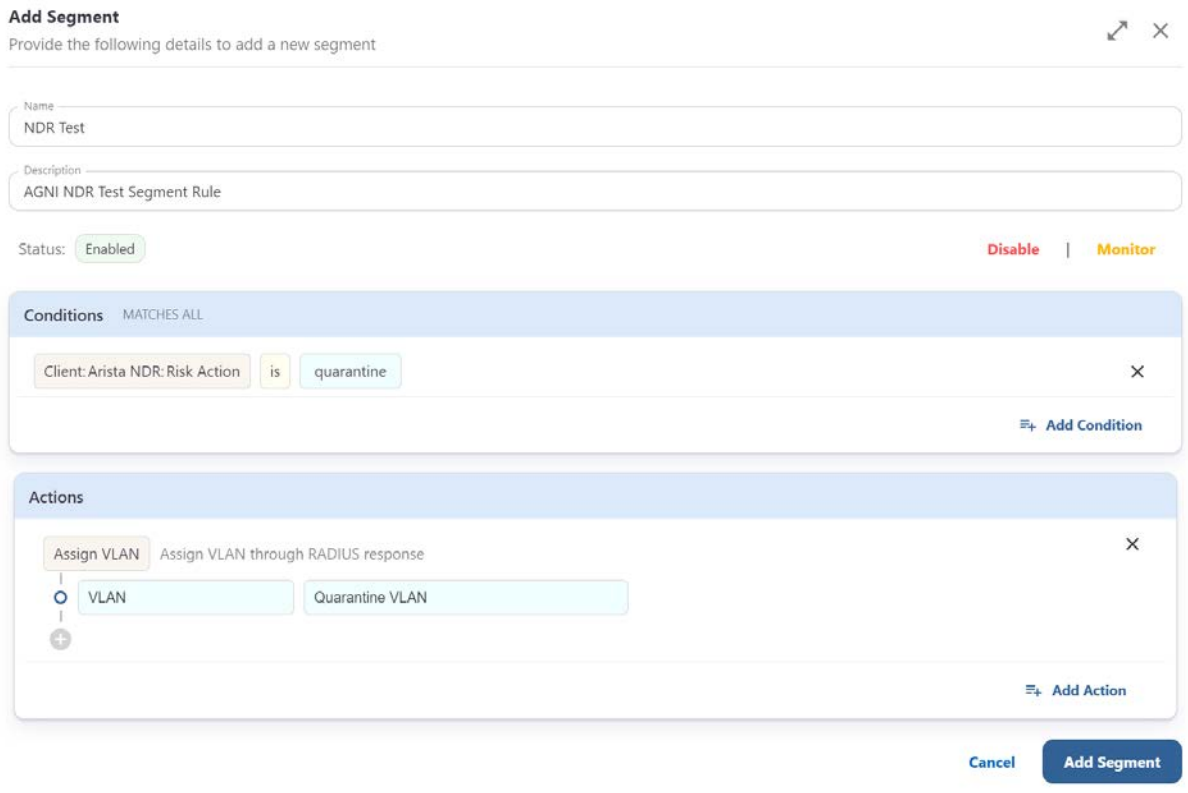
Action cannot be empty

Figure: Add Segment Details

Using Risk Action in Segment Policies

To use risk action in segmentation policy:

Arista NDR



Add Segment

Provide the following details to add a new segment

Name: NDR Test

Description: AGNI NDR Test Segment Rule

Status: Enabled

Conditions MATCHES ALL

Client: Arista NDR: Risk Action | is | quarantine

Actions

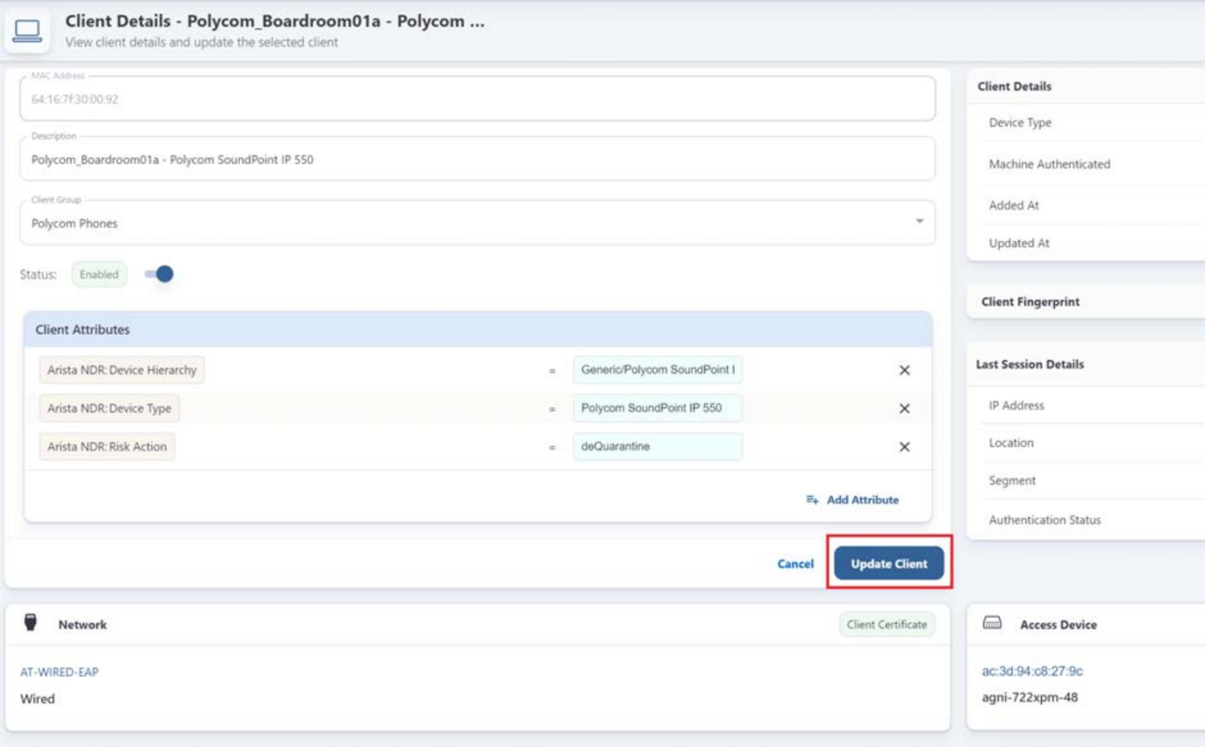
Assign VLAN — Assign VLAN through RADIUS response

VLAN | Quarantine VLAN

Figure: Add Segment Details for Risk Action

In Arista NDR, when a device is at risk, the admin changes the risk action to Quarantine, after which, AGNI applies the segment policy and as displayed in the above configuration, AGNI moves the client to Quarantine-VLAN after matching the segment policy. However, triggering the Risk Action is an administrative action on NDR. Refer to *NDR documentation* for the detailed process.

Once the admin rectifies the device, and changes the status to de-Quarantine in AGNI. On clicking the **Update Client** option, the admin updates the client attributes in the AGNI portal. When NDR loads the latest information of the client it pulls the latest attribute from AGNI and updates the device risk action from Quarantine to **Online**.



Client Details - Polycom_Boardroom01a - Polycom ...
View client details and update the selected client

MAC Address: 64:16:7f:30:00:92

Description: Polycom_Boardroom01a - Polycom SoundPoint IP 550

Client Group: Polycom Phones

Status: Enabled

Client Attributes

Arista NDR: Device Hierarchy	=	Generic/Polycom SoundPoint I
Arista NDR: Device Type	=	Polycom SoundPoint IP 550
Arista NDR: Risk Action	=	deQuarantine

Add Attribute

Cancel | Update Client

Network | Client Certificate
AT-WIRED-EAP
Wired

Client Details: Device Type, Machine Authenticated, Added At, Updated At

Client Fingerprint

Last Session Details: IP Address, Location, Segment, Authentication Status

Access Device
ac:3d:94:c8:27:9c
agni-722xpm-48

Figure: Update Client Details for Risk

External Integrations

AGNI enables you to integrate several third-party vendor applications as described below:

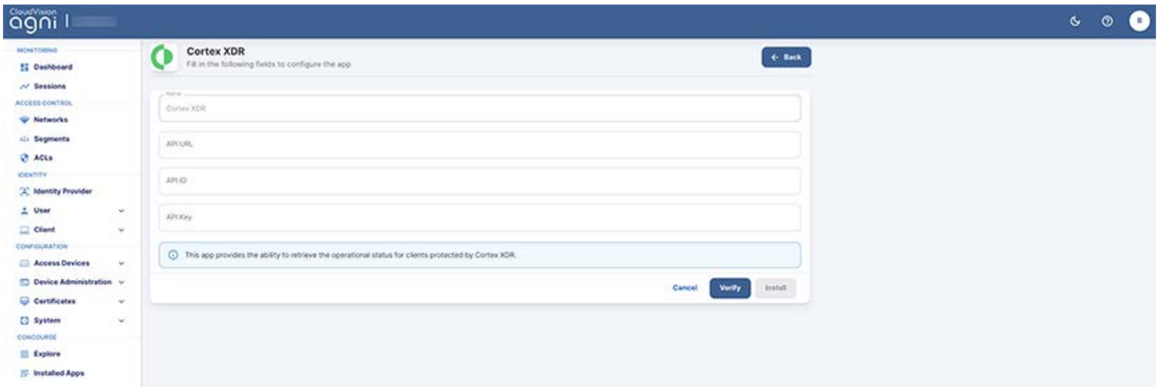
Palo Alto Cortex XDR Integration

Palo Alto Cortex XDR is an Endpoint Protection concourse application. Enabling Cortex XDR integration facilitates AGNI to retrieve the posture details from client devices managed by this external application. The posture details are associated with the clients and can be used in the segmentation conditions.

Prerequisites: The Cortex XDR integration with AGNI requires an API key with necessary permissions to retrieve the managed client device posture details. Refer to vendor documentation to configure and obtain the API key.

You can integrate Palo Alto Cortex XDR by installing the application as a Concourse App on the AGNI portal. To install Palo Alto Cortex XDR:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Cortex-XDR** application
3. Enter the following parameters:
    a. Cortex XDR in the **Name** field
    b. The API server URL
    c. The API ID
    d. API Key value



Cortex XDR

Fill in the following fields to configure the app

Name: Cortex XDR

API URL

API ID

API Key

This app provides the ability to retrieve the operational status for clients protected by Cortex XDR.

Figure: Installing Palo Alto Cortex XDR Concourse Application

4. Click the **Verify** button to validate the credentials
5. Click the **Install** button to complete the installation process.

The Palo Alto Cortex XDR application is displayed as an installed application in the Concourse page.

6. Click the **Sync Now** button on the Cortex XDR page to initiate the synchronization process.

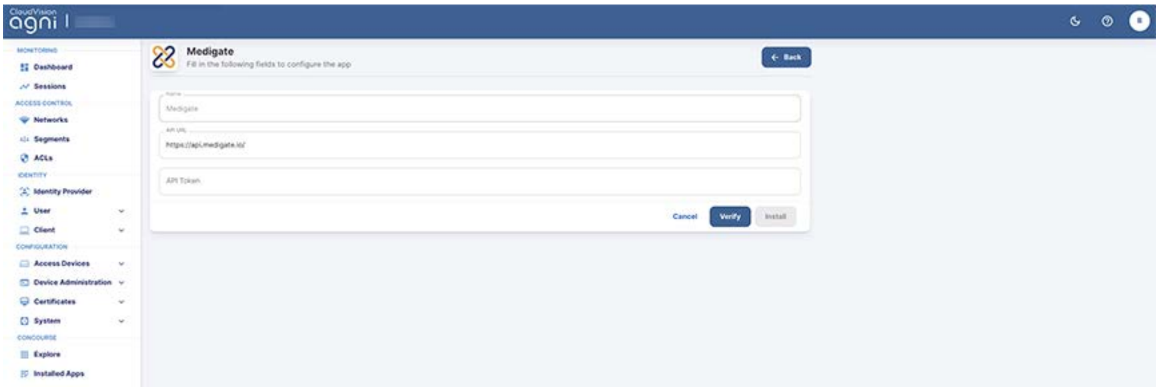
Medigate Integration

Medigate is an Endpoint Protection concourse application. Enabling Medigate integration facilitates AGNI to retrieve device profile details of the clients connecting to the network. Medigate profiles include medical, IoT, IoMT, and several other devices that are connected to the network. The profiled details are used in segmentation conditions.

Prerequisites: The Medigate integration requires an API token with necessary permissions to fetch the profiled client information. Refer to the vendor documentation to configure and obtain the API token.

You can integrate Medigate by installing the application as a Concourse App on the AGNI portal. To install Medigate:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Medigate** application (see image below)



Medigate

Fill in the following fields to configure the app

Name: Medigate

API URL: https://api.medigate.io/

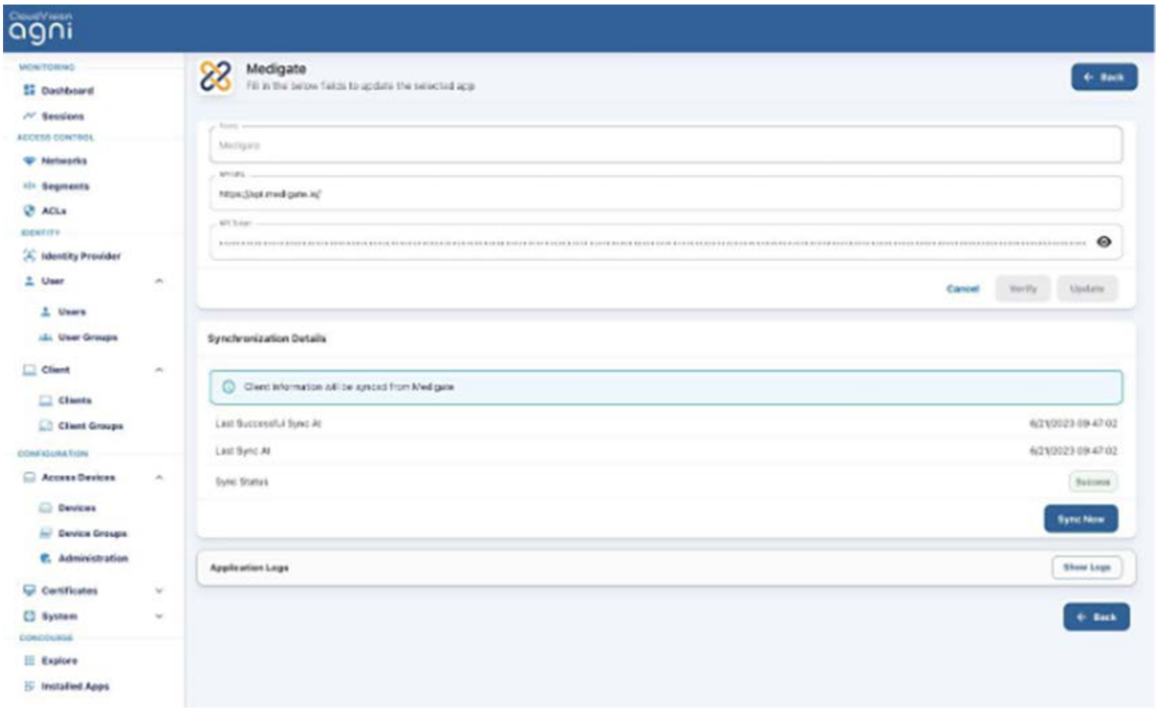
API Token

Figure: Installing Medigate Concourse Application

3. Enter the following parameters:
    a. Medigate in the **Name** field
    b. The API server URL
    c. The API Token
4. Click the **Verify** button to validate the credentials.
5. Click the **Install** button to complete the installation process.

The Medigate application gets displayed as an installed application in the Concourse page.

6. Click the **Sync Now** button on the Medigate page to initiate the synchronization process (see image below).



Name: Medigate

API URL: https://api.medigate.io/

API Token: ••

Synchronization Details

Client information will be synced from Medigate

Last Successful Sync At 6/21/2023 09:47:02

Last Sync At 6/21/2023 09:47:02

Sync Status Success

Application Logs

Figure: Installed Medigate Concourse Application

Microsoft Intune Integration

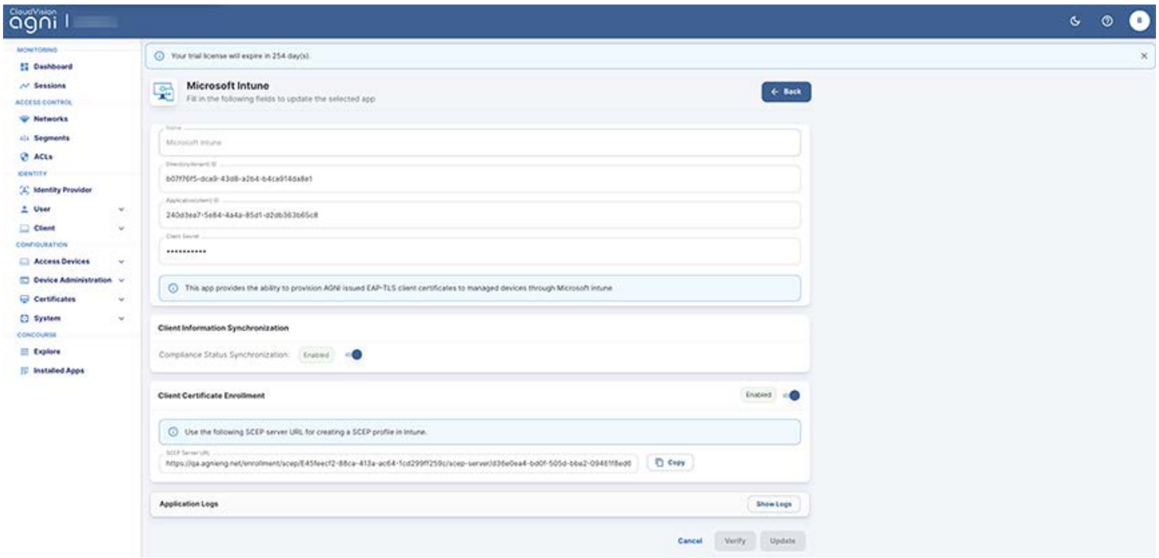
Microsoft Intune is a Device Management concourse application. Enabling Microsoft Intune integration provides the following capabilities:

- Provisioning of EAP-TLS client certificates through SCEP on the managed devices using AGNI's native PKI.
- Retrieving the client attributes and compliance status from the MDM provider. These attributes can be used in segmentation conditions.

Pre-requisites: The Intune integration requires API credentials with necessary permissions to fetch the client attributes and compliance information. Refer to vendor documentation to configure and obtain the API credentials.

You can integrate Microsoft Intune by installing the application as a Concourse App on the AGNI portal. To install Intune:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Microsoft Intune** application (see image below)



Your trial license will expire in 254 day(s).

Microsoft Intune
Fill in the following fields to update the selected app

Name: Microsoft Intune

Directory/tenant ID: b07f76f5-dca9-43d8-a2b4-b4ca914da8e1

Application/client ID: 240d3ea7-5e84-4a4a-85d1-d2db363b65c8

Client Secret: •••••••••••

This app provides the ability to provision AGNI issued EAP-TLS client certificates to managed devices through Microsoft intune

Client Information Synchronization

Compliance Status Synchronization: Enabled

Client Certificate Enrollment: Enabled

Use the following SCEP server URL for creating a SCEP profile in Intune.

SCEP Server URL: https://qa.agnieng.net/enrollment/scep/E45feecf2-88ca-413a-ac64-1cd299ff259c/scep-server/d36e0ea4-bd0f-505d-bba2-09481f8ed6

Application Logs

Figure: Installing Microsoft Intune Concourse Application

3. Enter the following parameters:
   a. Microsoft Intune in the **Name** field
   b. Directory (Tenant) ID
   c. Application (Client) ID
   d. Client Secret
4. Copy the generated SCEP URL and enter in Intune to create the SCEP profile.
5. Click the **Verify** button to validate the credentials.
6. Click the **Install** button to complete the installation process.

The Microsoft Intune application gets displayed as an installed application in the Concourse page.

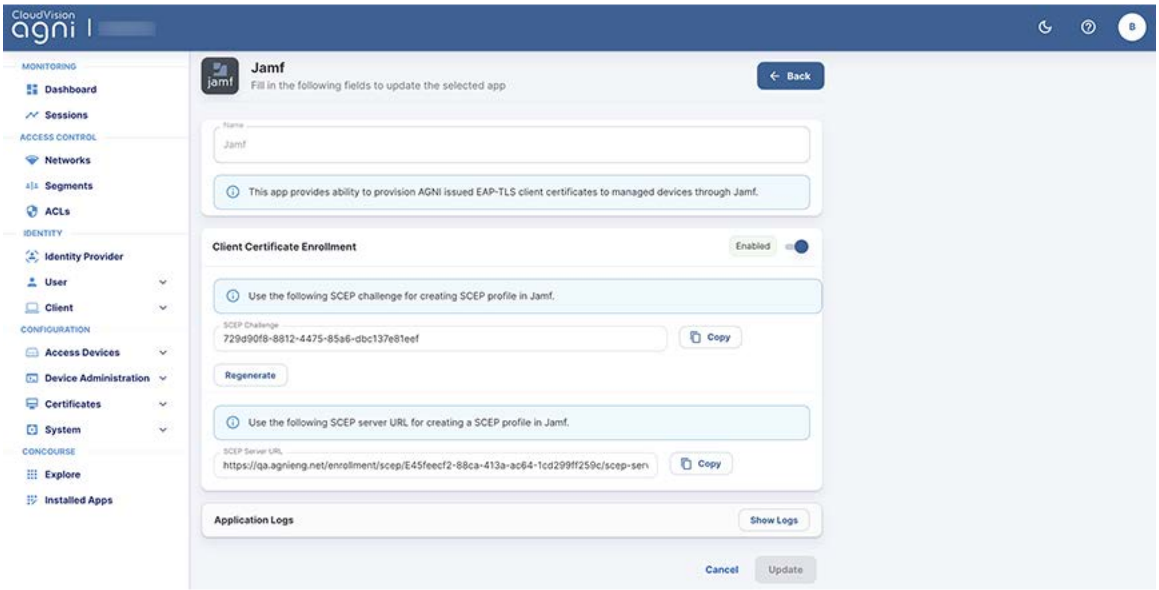
Jamf Integration

Jamf is a Device Management concourse application, which facilitates integration of MDM solutions with AGNI. Jamf integration enables the provisioning of EAP-TLS client certificates through SCEP on the managed devices using AGNI's native PKI.

Pre-requisites: The Jamf integration requires the SCEP challenge and the URL generated in AGNI for configuration in Jamf administration portal. Refer to vendor documentation for the details to configure these parameters.

You can integrate Jamf by installing the application as a Concourse App on the AGNI portal. To install Jamf:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Jamf** application (see image below)



Jamf
Fill in the following fields to update the selected app

Name: Jamf

This app provides ability to provision AGNI issued EAP-TLS client certificates to managed devices through Jamf.

Client Certificate Enrollment: Enabled

Use the following SCEP challenge for creating SCEP profile in Jamf.

SCEP Challenge: 729d90f8-8812-4475-85a6-dbc137e81eef

Use the following SCEP server URL for creating a SCEP profile in Jamf.

SCEP Server URL: https://qa.agnieng.net/enrollment/scep/E45feecf2-88ca-413a-ac64-1cd299ff259c/scep-serv

Application Logs

Figure: Installing Jamf Concourse Application

3. Enter Jamf in the **Name** field.
4. Click the **Install** button to complete the installation process.
5. Enable the **Client Certificate Enrollment** option.
6. Copy the generated SCEP Challenge and SCEP server URL, and enter in Jamf administration portal to create the SCEP profile.

The Jamf application gets displayed as an installed application in the Concourse page.

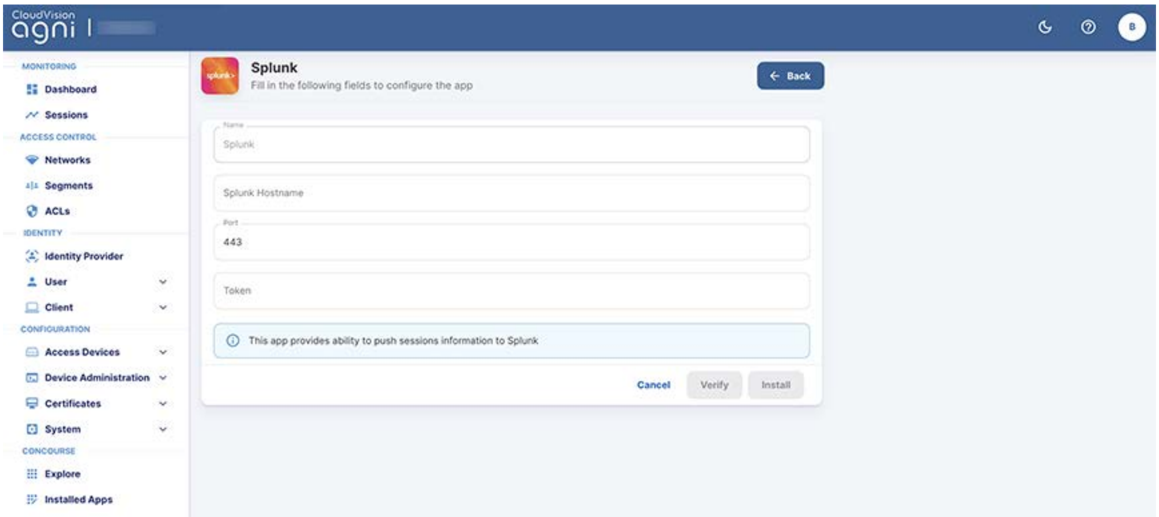
Splunk Integration

Splunk is a SIEM concourse application. Enabling Splunk integration with AGNI facilitates in retrieving the session log updates for the users authenticating in the network through AGNI. The update includes the user-ID, IP address, client device, and session details of the incoming authentication requests.

Pre-requisites: The integration requires Splunk SIEM credentials to be configured as part of the concourse application configuration. Refer to vendor documentation for details to configure these parameters.

You can integrate Splunk by installing the application as a Concourse App on the AGNI portal. To install Splunk:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Splunk** application (see image below)



Splunk
Fill in the following fields to configure the app

Name: Splunk
Splunk Hostname
Port: 443
Token

This app provides ability to push sessions information to Splunk

Figure: Installing Splunk Concourse Application

7. Enter the following parameters:
    e. Splunk in the **Name** field
    f. Splunk Hostname
    g. Port (default is 443)
    h. Token
8. Click the **Verify** button to validate the credentials.
9. Click the **Install** button to complete the installation process.

The Splunk application gets displayed as an installed application in the Concourse page.

Sumo Logic Integration

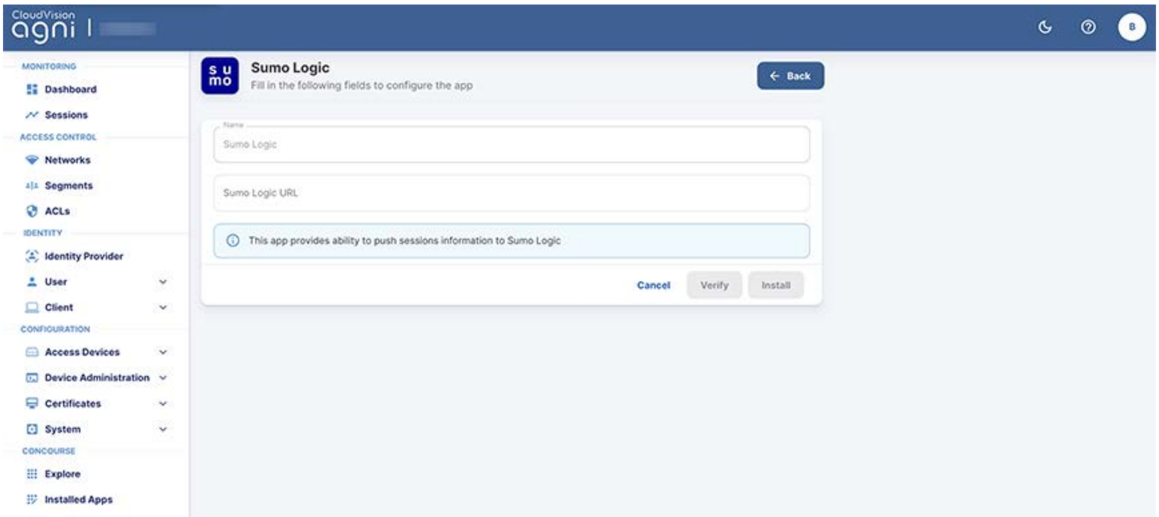
Sumo Logic is a SIEM concourse application. Enabling Sumo Logic integration facilitates in retrieving the session log updates for the users authenticating in the network through AGNI. The update includes the user-ID, IP address, client device, and session details of the incoming authentication requests.

Pre-requisites: The integration requires Sumo Logic SIEM URL to be configured as part of the concourse application configuration. Refer to vendor documentation for details on obtaining this parameter.

Integration is achieved through installing this concourse application to facilitate session log updates from AGNI.

You can integrate Sumo Logic by installing the application as a Concourse App on the AGNI portal. To install Sumo Logic:

1. Navigate to **Concourse** -> **Explore**
2. Install the **Sumo Logic** application (see image below)



Sumo Logic

Fill in the following fields to configure the app

Name: Sumo Logic

Sumo Logic URL

This app provides ability to push sessions information to Sumo Logic

Figure: Installing Sumo Logic Concourse Application

3. Enter Sumo Logic in the **Name** field.
4. Enter Sumo Logic URL.
5. Click the **Verify** button to validate the credentials.
6. Click the **Install** button to complete the installation process.

The Sumo Logic application gets displayed as an installed application in the Concourse page.

Configuring the Various Entities in AGNI

This section includes the detailed configuration aspects for the following entities:

- Device Configurations
- Certificate Configurations
- Identity Provider configuration
- Network Configurations
- Segment Configurations
- User Configurations
- Client Configurations

Configuring the Devices

Network Access Devices (NADs) connect with AGNI via RadSec and the devices are added to AGNI from the **Configuration** –> **Access Devices** → **Devices** page of the portal. You can add the devices to AGNI by:

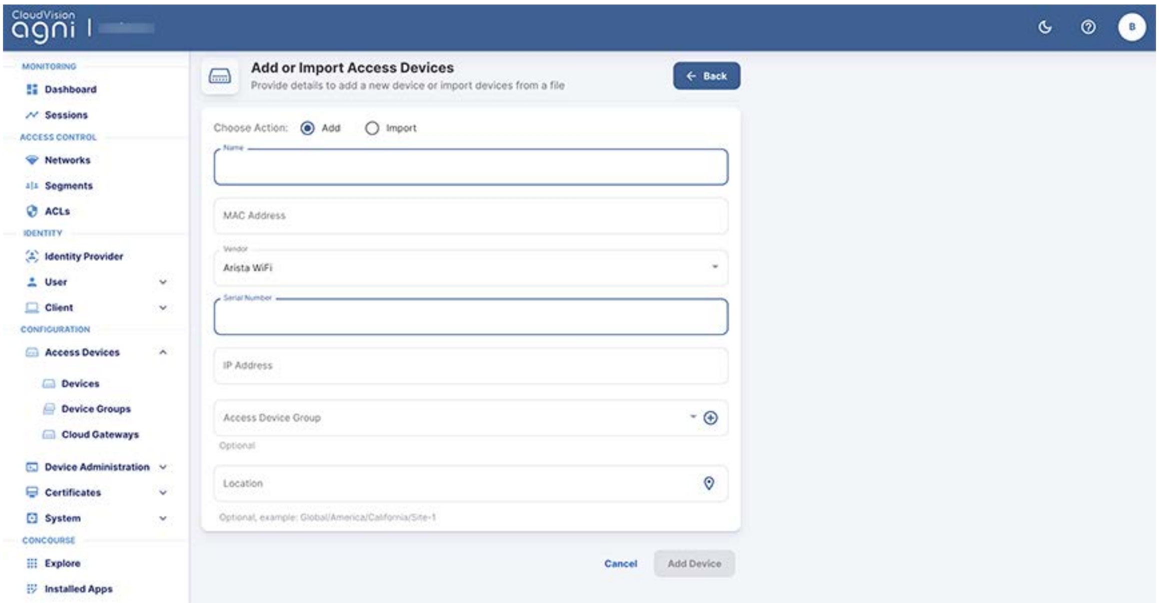
- Manually adding the devices
- Importing the devices using APIs
- Devices managed by Arista CloudVision can be imported automatically into the system by installing Arista CloudVision or Arista CV-CUE concourse application. For details on the concourse plugin installation, see the Third-party Integrations section.

Adding an Access Device

This option enables you to manually add network access devices into the system. AGNI, being a multi-vendor solution supports working with several third-party vendors, which support RadSec protocol. The vendor list includes:

- Arista WiFi
- Arista Switch
- Aruba
- Cisco
- Generic

The *Generic* option is used to add any other vendor that supports RadSec and complies to the protocol.



Add or Import Access Devices

Provide details to add a new device or import devices from a file

Choose Action: ● Add ○ Import

Name

MAC Address

Vendor: Arista WiFi

Serial Number

IP Address

Access Device Group

Optional

Location

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

Figure: Adding a Device

Importing Devices in Bulk to AGNI

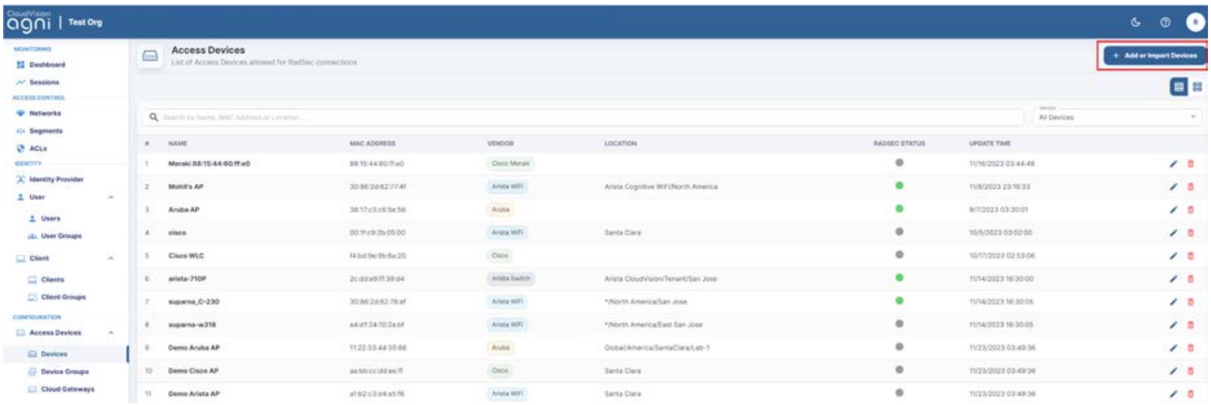
This section describes the steps to import Network Access Devices (NAD) in bulk to AGNI. The network access devices are added under the **Access Devices** tab.

The bulk import option of NAD devices also enables you to add the device's location, serial number, and IP Address. You must log in to AGNI as a network administrator and access the dashboard to import NAD devices in bulk.

Importing Devices to AGNI

To bulk import devices to AGNI:

1. Log in to AGNI and Navigate to **Access Devices**-> **Devices**. Click the **Add or Import Devices** option (see image below).



Access Devices
List of Access Devices allowed for RadSec connections

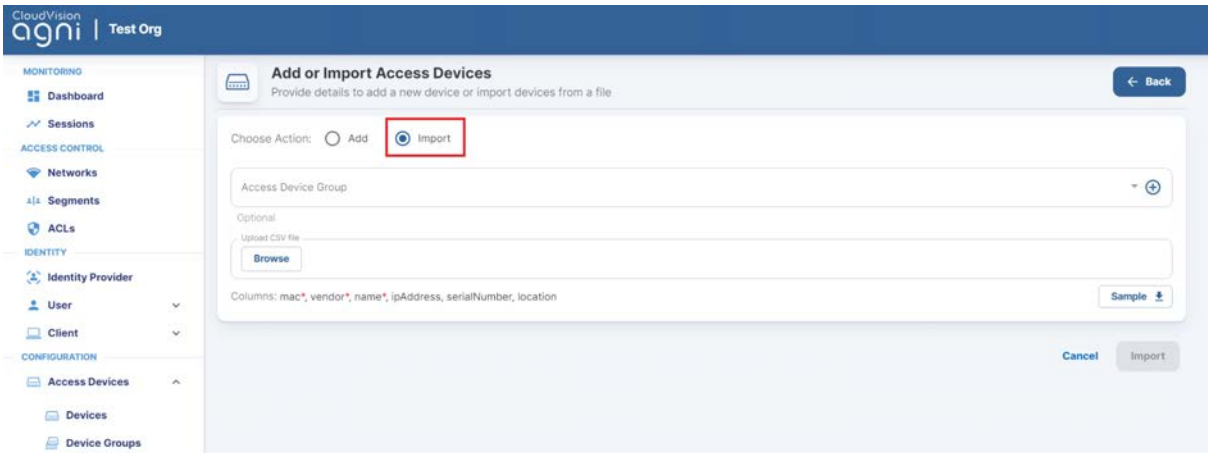
Search by Name, MAC Address or Location...

Vendor: All Devices

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS	UPDATE TIME
1	Meraki 88:15:44:60:ff:e0	88:15:44:60:ff:e0	Cisco Meraki		●	11/16/2023 03:44:48
2	Mohit's AP	30:86:2d:62:77:4f	Arista WiFi	Arista Cognitive WiFi/North America	●	11/8/2023 23:16:33
3	Aruba AP	38:17:c3:c6:5e:56	Aruba		●	9/7/2023 03:30:01
4	cisco	00:1f:c9:2b:05:00	Arista WiFi	Santa Clara	●	10/5/2023 03:02:00
5	Cisco WLC	14:bd:9e:9b:6a:20	Cisco		●	10/17/2023 02:53:06
6	arista-710P	2c:dd:e9:11:39:d4	Arista Switch	Arista CloudVision/Tenant/San Jose	●	11/14/2023 16:30:00
7	suparna_C-230	30:86:2d:62:78:ef	Arista WiFi	*/North America/San Jose	●	11/14/2023 16:30:05
8	suparna-w318	e4:d1:24:10:2a:bf	Arista WiFi	*/North America/East San Jose	●	11/14/2023 16:30:05
9	Demo Aruba AP	11:22:33:44:55:66	Aruba	Global/America/SantaClara/Lab-1	●	11/23/2023 03:49:36
10	Demo Cisco AP	aa:bb:cc:dd:ee:ff	Cisco	Santa Clara	●	11/23/2023 03:49:36
11	Demo Arista AP	a1:b2:c3:d4:e5:f6	Arista WiFi	Santa Clara	●	11/23/2023 03:49:36

Figure: Importing Devices

2. Select the **Import** option to import devices using the .csv file format.



Add or Import Access Devices
Provide details to add a new device or import devices from a file

Choose Action: ○ Add ● Import

Access Device Group
Optional

Upload CSV file

Columns: mac*, vendor*, name*, ipAddress, serialNumber, location

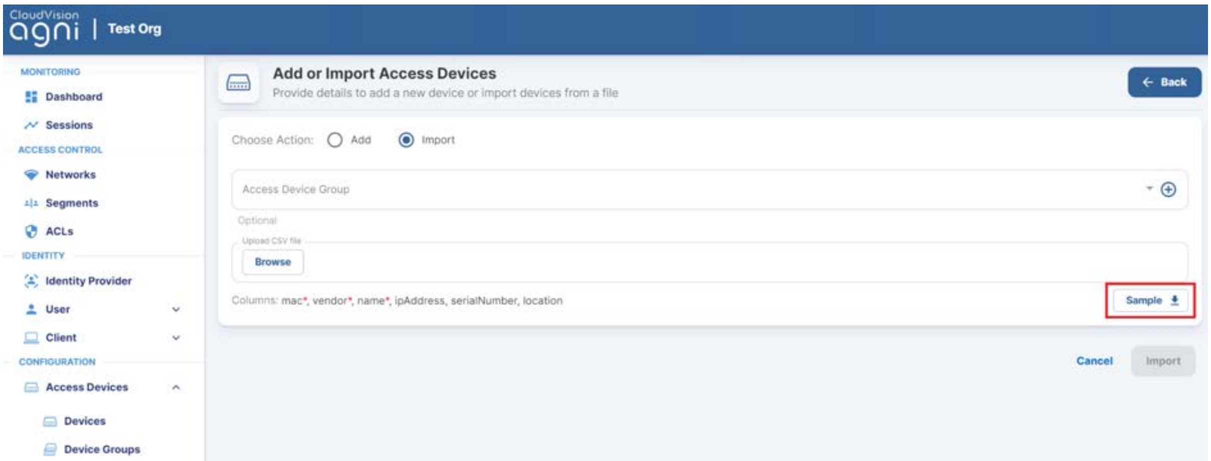
Figure: Add or Import Devices

As a network admin, you can download a sample .csv file and create the desired .csv file in the required format. The .csv file includes the following columns:

- MAC Address (mandatory)
- Vendor (Mandatory)

- Name (Mandatory)
- IP Address (Optional)
- Serial Number (Optional)
- Location (Optional)

To download a sample .csv file, click the **Sample** button (see image below).



Choose Action: ○ Add ● Import

Access Device Group

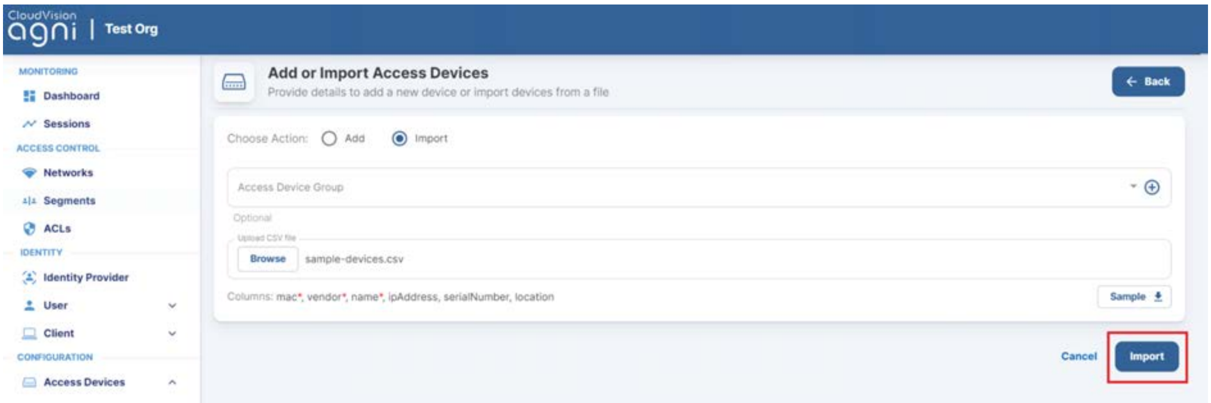
Optional

Upload CSV file

Columns: mac*, vendor*, name*, ipAddress, serialNumber, location

Figure: Add or Import Devices-2

3. Click the **Browse** button and select the .csv file that needs to be uploaded. The **Import** option gets enabled after the .csv file is uploaded (see image below).



Choose Action: ○ Add ● Import

Access Device Group

Optional

Upload CSV file: sample-devices.csv

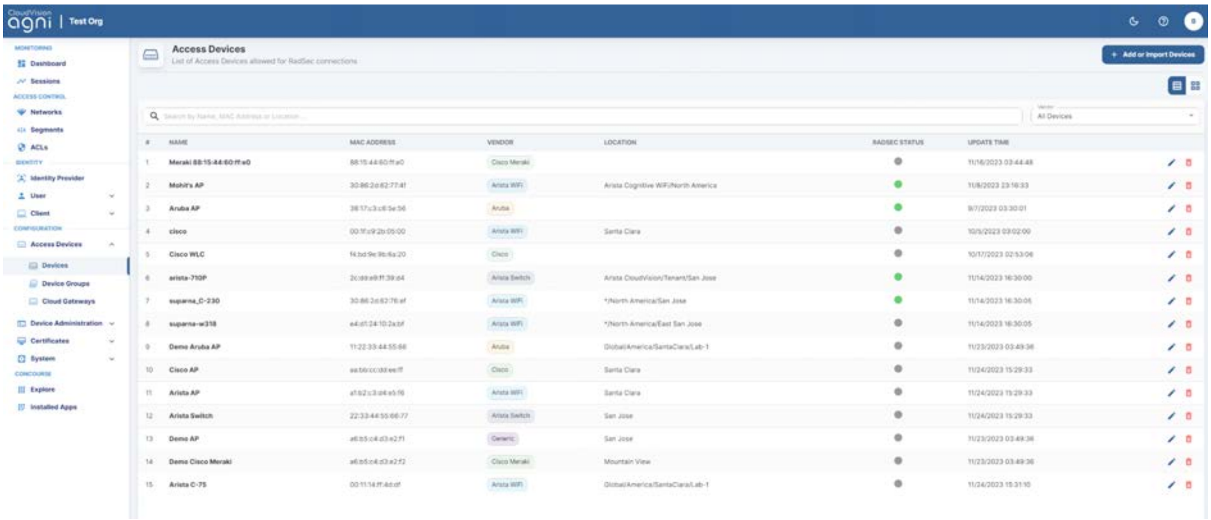
Columns: mac*, vendor*, name*, ipAddress, serialNumber, location

Figure: Add or Import Devices-3

You can also assign a device group while importing the Network Access devices. Once the bulk device import is complete, all the devices get associated with the selected device group.

4. Click **Import** to import all the devices to AGNI. Once the devices are successfully imported, they are displayed under the **Access Devices**-> **Devices** tab (see image below).

   Note: The AGNI portal displays an error message if the bulk device import is unsuccessful.



Access Devices

List of Access Devices allowed for RadSec connections

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS	UPDATE TIME
1	Meraki 88:15:44:60:ff:e0	88:15:44:60:ff:e0	Cisco Meraki		●	11/16/2023 03:44:48
2	Mohit's AP	30:86:2d:62:77:41	Arista WiFi	Arista Cognitive WiFi/North America	🟢	11/8/2023 23:16:33
3	Aruba AP	38:17:c3:c8:5e:56	Aruba		🟢	9/7/2023 03:30:01
4	cisco	00:1f:c9:2b:05:00	Arista WiFi	Santa Clara	●	10/5/2023 03:02:00
5	Cisco WLC	f4:bd:9e:9b:6a:20	Cisco		●	10/17/2023 02:53:06
6	arista-710P	2c:dd:e9:f1:39:d4	Arista Switch	Arista CloudVision/Tenant/San Jose	🟢	11/14/2023 16:30:00
7	suparna_C-230	30:86:2d:62:76:ef	Arista WiFi	*/North America/San Jose	🟢	11/14/2023 16:30:05
8	suparna-w318	e4:d1:24:10:2a:bf	Arista WiFi	*/North America/East San Jose	●	11/14/2023 16:30:05
9	Demo Aruba AP	11:22:33:44:55:66	Aruba	Global/America/SantaClara/Lab-1	●	11/23/2023 03:49:36
10	Cisco AP	aa:bb:cc:dd:ee:ff	Cisco	Santa Clara	●	11/24/2023 15:29:33
11	Arista AP	a1:b2:c3:d4:e5:f6	Arista WiFi	Santa Clara	●	11/24/2023 15:29:33
12	Arista Switch	22:33:44:55:66:77	Arista Switch	San Jose	●	11/24/2023 15:29:33
13	Demo AP	a6:b5:c4:d3:e2:f1	Generic	San Jose	●	11/23/2023 03:49:36
14	Demo Cisco Meraki	a6:b5:c4:d3:e2:f2	Cisco Meraki	Mountain View	●	11/23/2023 03:49:36
15	Arista C-75	00:11:14:ff:4d:df	Arista WiFi	Global/America/SantaClara/Lab-1	●	11/24/2023 15:31:10

Figure: Access Devices

Note: Serial Number is a mandatory field for adding Cisco-Meraki devices using .csv file format.

Configuring TACACS+ with AGNI

This section describes the procedure to configure TACACS+ in AGNI. To configure TACACS+ with AGNI, the admin should first configure the Arista Cloud Gateway (ACG) solution in the network. This Arista Cloud Gateway further integrates with AGNI over secure web sockets. The Arista Cloud Gateway solution provides greater security in accessing the public internet.

As illustrated in the image below, Arista Cloud Gateway enables the TACACS+ proxy implementation to terminate the TACACS+ protocol on-premise and transport the TACACS+ information as HTTPS payload to AGNI cloud.

The proxy/gateway is deployed as a software image extension (SWIX extension) on the Arista EOS platform. The network devices should be configured to use the proxy as the TACACS+ server.

End users can access device administration features through the AGNI self-service portal as explained in below sections.

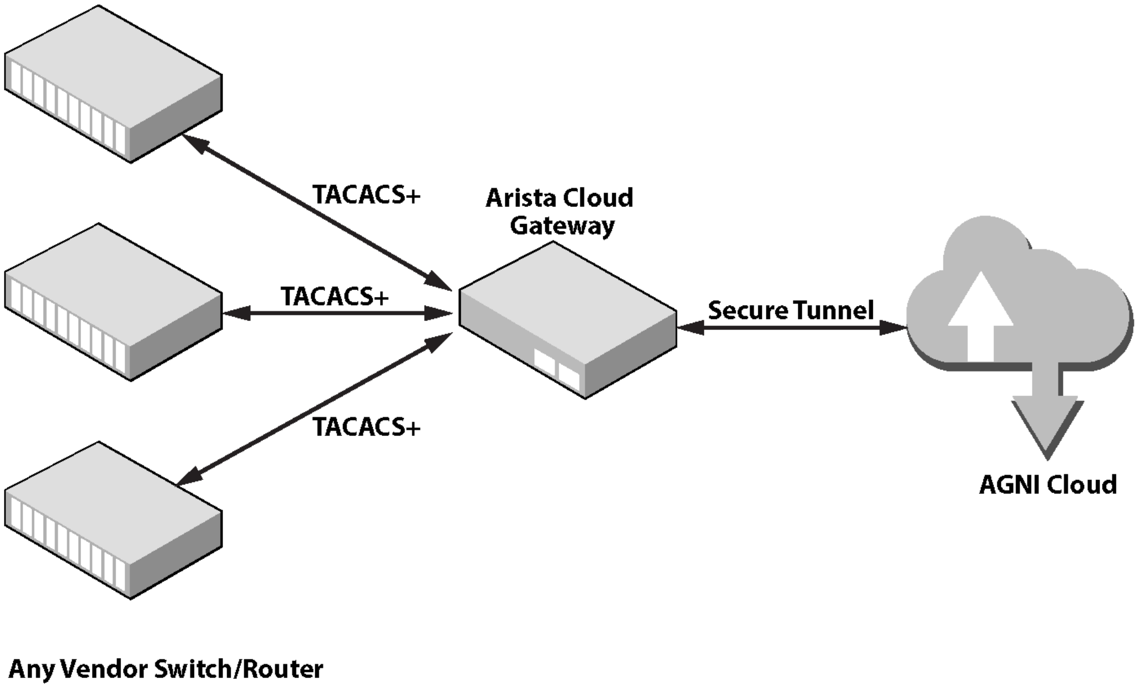


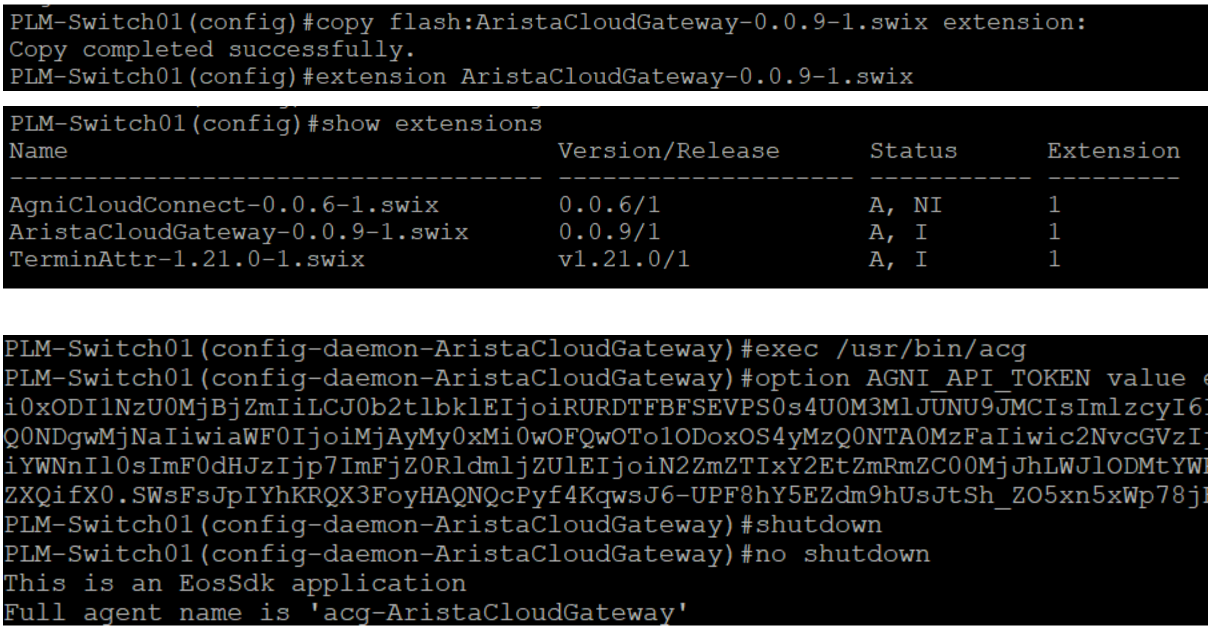
Figure: Arista Cloud Gateway Solution

Configuring Arista Cloud Gateway on Arista Switches

To install Arista Cloud Gateway on EOS switches, follow the below CLI configurations:

```
Copy the Arista Cloud Connect file to the system flash: scp
.\AristaCloudConnect-.swix admin@192.168.1.10:/mnt/flash

copy flash:AristaCloudGateway-.swix extension:

extension AristaCloudGateway-.swix

show extensions

no daemon AristaCloudGateway

daemon AristaCloudGateway
 exec /usr/bin/acg
option AGNI_API_TOKEN value <token from AGNI>
no shutdown
```

Below snapshots display how SWIX extension gets installed on an Arista switch:



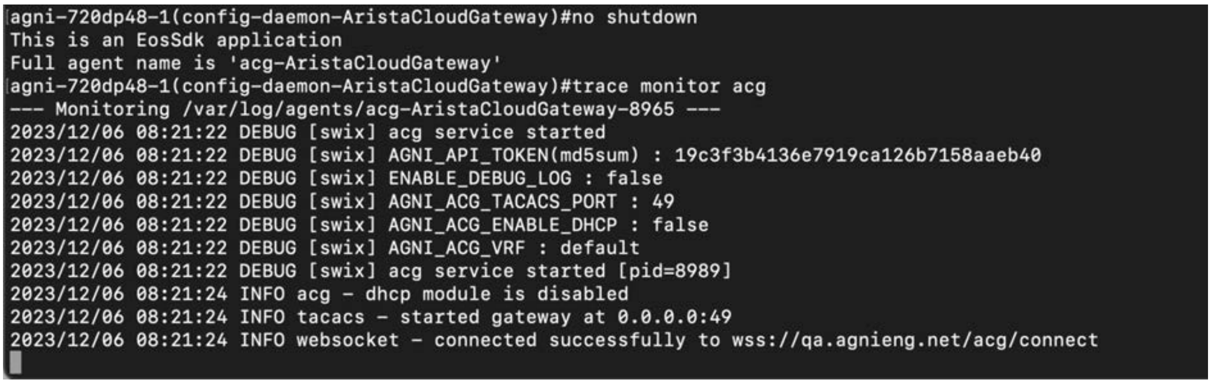
```
PLM-Switch01(config)#copy flash:AristaCloudGateway-0.0.9-1.swix extension:
Copy completed successfully.
PLM-Switch01(config)#extension AristaCloudGateway-0.0.9-1.swix
```

```
PLM-Switch01(config)#show extensions
Name                                  Version/Release      Status      Extension
------------------------------------- -------------------- ----------- ---------
AgniCloudConnect-0.0.6-1.swix         0.0.6/1              A, NI       1
AristaCloudGateway-0.0.9-1.swix       0.0.9/1              A, I        1
TerminAttr-1.21.0-1.swix              v1.21.0/1            A, I        1
```

```
PLM-Switch01(config-daemon-AristaCloudGateway)#exec /usr/bin/acg
PLM-Switch01(config-daemon-AristaCloudGateway)#option AGNI_API_TOKEN value
i0xODI1NzU0MjBjZmIiLCJ0b2tlbklEIjoiRURDTFBFSEVPS0s4U0M3MlJUNU9JMCIsImlzcyI6
Q0NDgwMjNaIiwiaWF0IjoiMjAyMy0xMi0wOFQwOTo1ODoxOS4yMzQ0NTA0MzFaIiwic2NvcGVzI
iYWNnIl0sImF0dHJzIjp7ImFjZ0RldmljZUlEIjoiN2ZmZTIxY2EtZmRmZC00MjJhLWJlODMtYW
ZXQifX0.SWsFsJpIYhKRQX3FoyHAQNQcPyf4KqwsJ6-UPF8hY5EZdm9hUsJtSh_ZO5xn5xWp78j
PLM-Switch01(config-daemon-AristaCloudGateway)#shutdown
PLM-Switch01(config-daemon-AristaCloudGateway)#no shutdown
This is an EosSdk application
Full agent name is 'acg-AristaCloudGateway'
```

Figure: Installing Arista Cloud Gateway on EOS Switch

Below snapshot shows the logs depicting that the daemon is listening on port 49:



```
agni-720dp48-1(config-daemon-AristaCloudGateway)#no shutdown
This is an EosSdk application
Full agent name is 'acg-AristaCloudGateway'
agni-720dp48-1(config-daemon-AristaCloudGateway)#trace monitor acg
--- Monitoring /var/log/agents/acg-AristaCloudGateway-8965 ---
2023/12/06 08:21:22 DEBUG [swix] acg service started
2023/12/06 08:21:22 DEBUG [swix] AGNI_API_TOKEN(md5sum) : 19c3f3b4136e7919ca126b7158aaeb40
2023/12/06 08:21:22 DEBUG [swix] ENABLE_DEBUG_LOG : false
2023/12/06 08:21:22 DEBUG [swix] AGNI_ACG_TACACS_PORT : 49
2023/12/06 08:21:22 DEBUG [swix] AGNI_ACG_ENABLE_DHCP : false
2023/12/06 08:21:22 DEBUG [swix] AGNI_ACG_VRF : default
2023/12/06 08:21:22 DEBUG [swix] acg service started [pid=8989]
2023/12/06 08:21:24 INFO acg - dhcp module is disabled
2023/12/06 08:21:24 INFO tacacs - started gateway at 0.0.0.0:49
2023/12/06 08:21:24 INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect
```

Figure: Arista Cloud Gateway Daemon Listening on Port 49

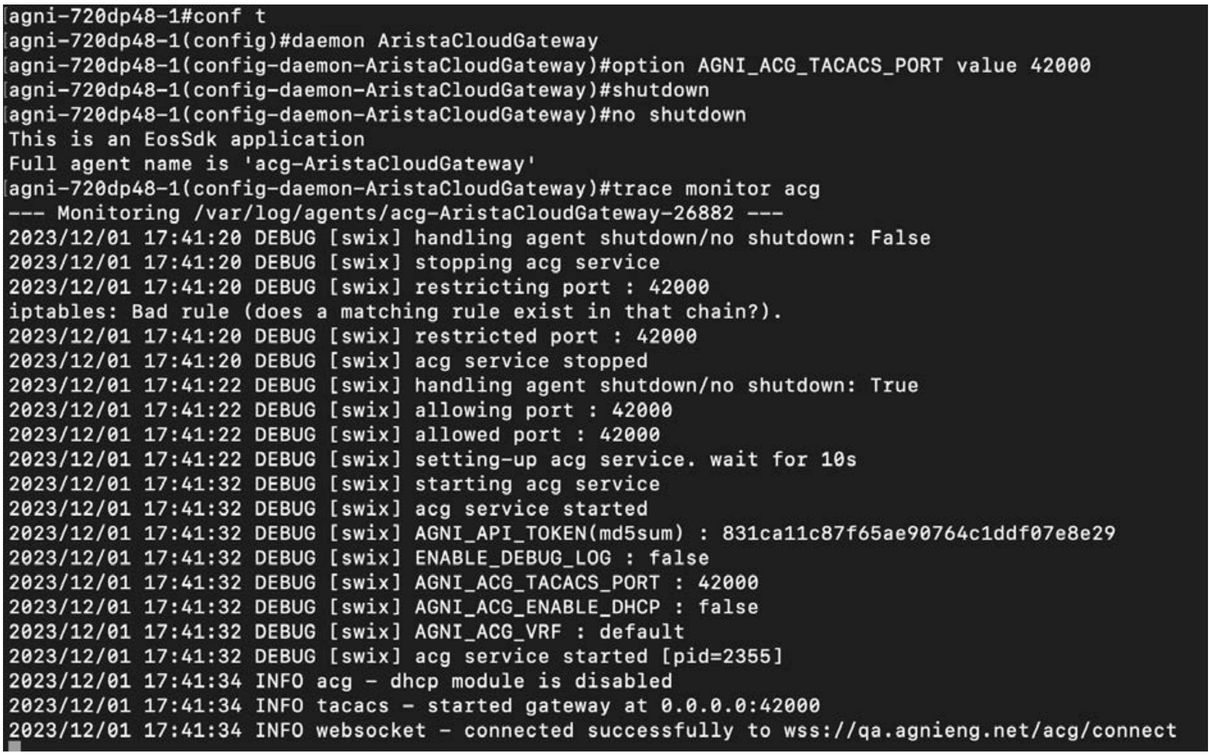
Note: By default, when you execute the above commands, Arista Cloud Gateway daemon listens on TACACS+ port 49. To run TACACS+ on a non-standard port other than 49, use the CLI:

```
option AGNI_ACG_TACACS_PORT value <port_no>
```

You can also change the default VRF option by using the command:

```
AGNI_ACG_VRF : change VRF. optional,default "default"
```

The below snapshot shows how to run Tacacs+ on a non-standard port on the Arista switch:



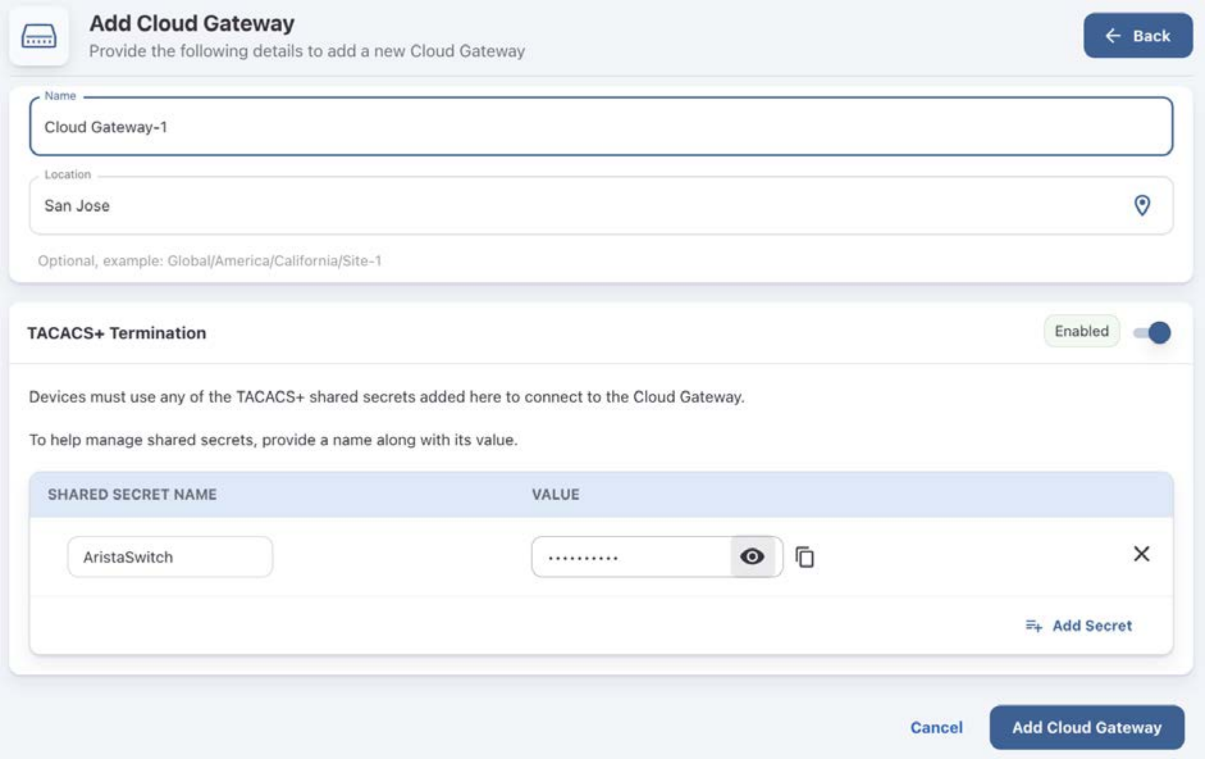
```
[agni-720dp48-1#conf t
[agni-720dp48-1(config)#daemon AristaCloudGateway
[agni-720dp48-1(config-daemon-AristaCloudGateway)#option AGNI_ACG_TACACS_PORT value 42000
[agni-720dp48-1(config-daemon-AristaCloudGateway)#shutdown
[agni-720dp48-1(config-daemon-AristaCloudGateway)#no shutdown
This is an EosSdk application
Full agent name is 'acg-AristaCloudGateway'
[agni-720dp48-1(config-daemon-AristaCloudGateway)#trace monitor acg
--- Monitoring /var/log/agents/acg-AristaCloudGateway-26882 ---
2023/12/01 17:41:20 DEBUG [swix] handling agent shutdown/no shutdown: False
2023/12/01 17:41:20 DEBUG [swix] stopping acg service
2023/12/01 17:41:20 DEBUG [swix] restricting port : 42000
iptables: Bad rule (does a matching rule exist in that chain?).
2023/12/01 17:41:20 DEBUG [swix] restricted port : 42000
2023/12/01 17:41:20 DEBUG [swix] acg service stopped
2023/12/01 17:41:22 DEBUG [swix] handling agent shutdown/no shutdown: True
2023/12/01 17:41:22 DEBUG [swix] allowing port : 42000
2023/12/01 17:41:22 DEBUG [swix] allowed port : 42000
2023/12/01 17:41:22 DEBUG [swix] setting-up acg service. wait for 10s
2023/12/01 17:41:32 DEBUG [swix] starting acg service
2023/12/01 17:41:32 DEBUG [swix] acg service started
2023/12/01 17:41:32 DEBUG [swix] AGNI_API_TOKEN(md5sum) : 831ca11c87f65ae90764c1ddf07e8e29
2023/12/01 17:41:32 DEBUG [swix] ENABLE_DEBUG_LOG : false
2023/12/01 17:41:32 DEBUG [swix] AGNI_ACG_TACACS_PORT : 42000
2023/12/01 17:41:32 DEBUG [swix] AGNI_ACG_ENABLE_DHCP : false
2023/12/01 17:41:32 DEBUG [swix] AGNI_ACG_VRF : default
2023/12/01 17:41:32 DEBUG [swix] acg service started [pid=2355]
2023/12/01 17:41:34 INFO acg - dhcp module is disabled
2023/12/01 17:41:34 INFO tacacs - started gateway at 0.0.0.0:42000
2023/12/01 17:41:34 INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect
```

Figure: Running TACACS+ on non-STandard Port

Configuring Arista Cloud Gateway on AGNI

To configure Arista Cloud Gateway on AGNI:

- Navigate to **Configuration→Access Devices–>Cloud Gateways.**
- Click **Add Cloud Gateway** to add a new cloud gateway to AGNI.



Add Cloud Gateway

Provide the following details to add a new Cloud Gateway

Name: Cloud Gateway-1

Location: San Jose

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

TACACS+ Termination

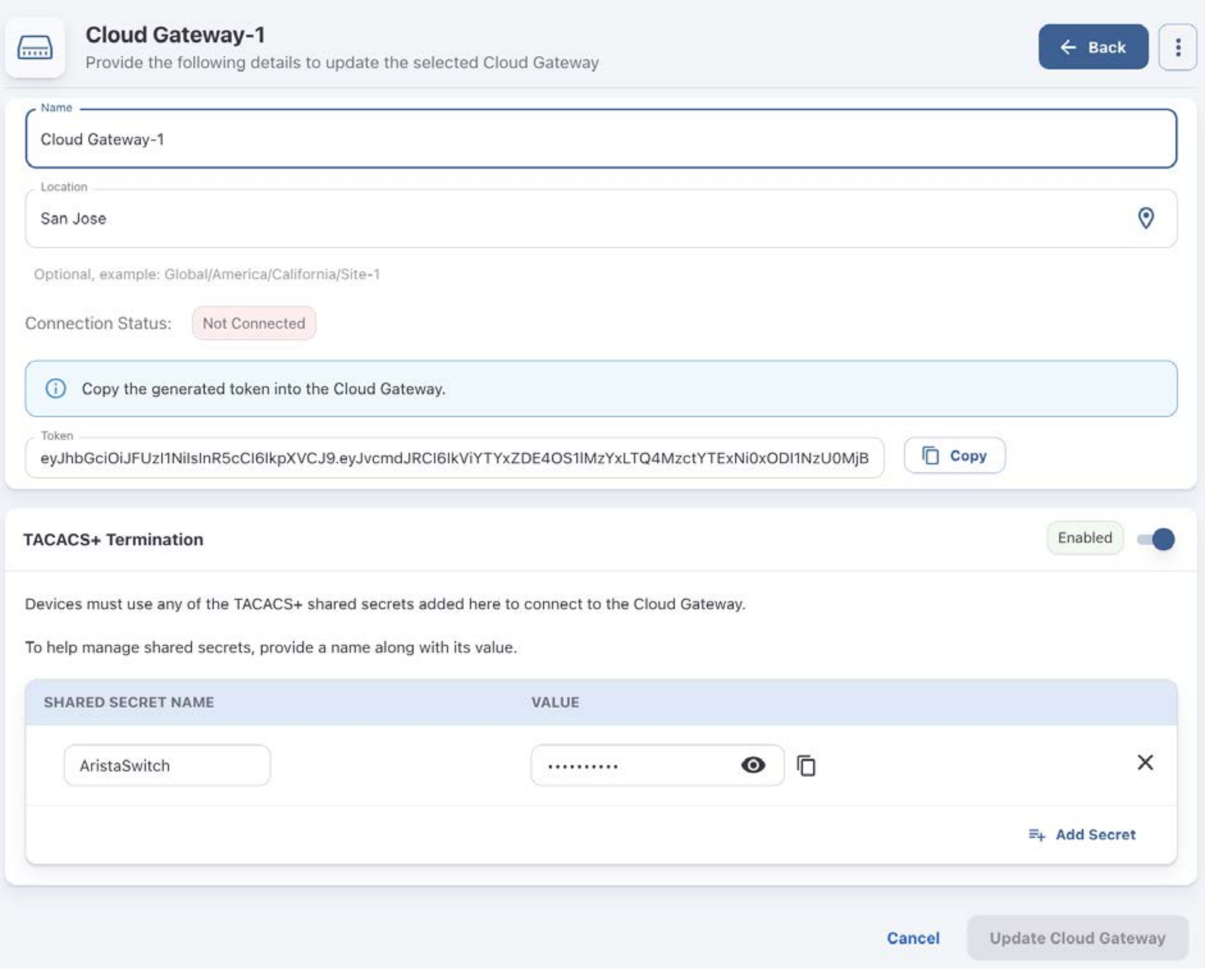
Devices must use any of the TACACS+ shared secrets added here to connect to the Cloud Gateway.

To help manage shared secrets, provide a name along with its value.

SHARED SECRET NAME	VALUE
AristaSwitch	••••••••••

Figure: Adding a New Cloud Gateway

- Click ***Add Cloud Gateway*** and a Token is generated. You can copy this token and can be used on Arista Cloud Gateway running on Arista Switch or the Docker instance to establish a HTTPS connection with AGNI.
- Click **Update Cloud Gateway**.



Cloud Gateway-1

Provide the following details to update the selected Cloud Gateway

Name: Cloud Gateway-1

Location: San Jose

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

Connection Status: Not Connected

Copy the generated token into the Cloud Gateway.

Token: eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IkViYTYxZDE4OS1lMzYxLTQ4MzctYTExNi0xODI1NzU0MjB

TACACS+ Termination Enabled

Devices must use any of the TACACS+ shared secrets added here to connect to the Cloud Gateway.

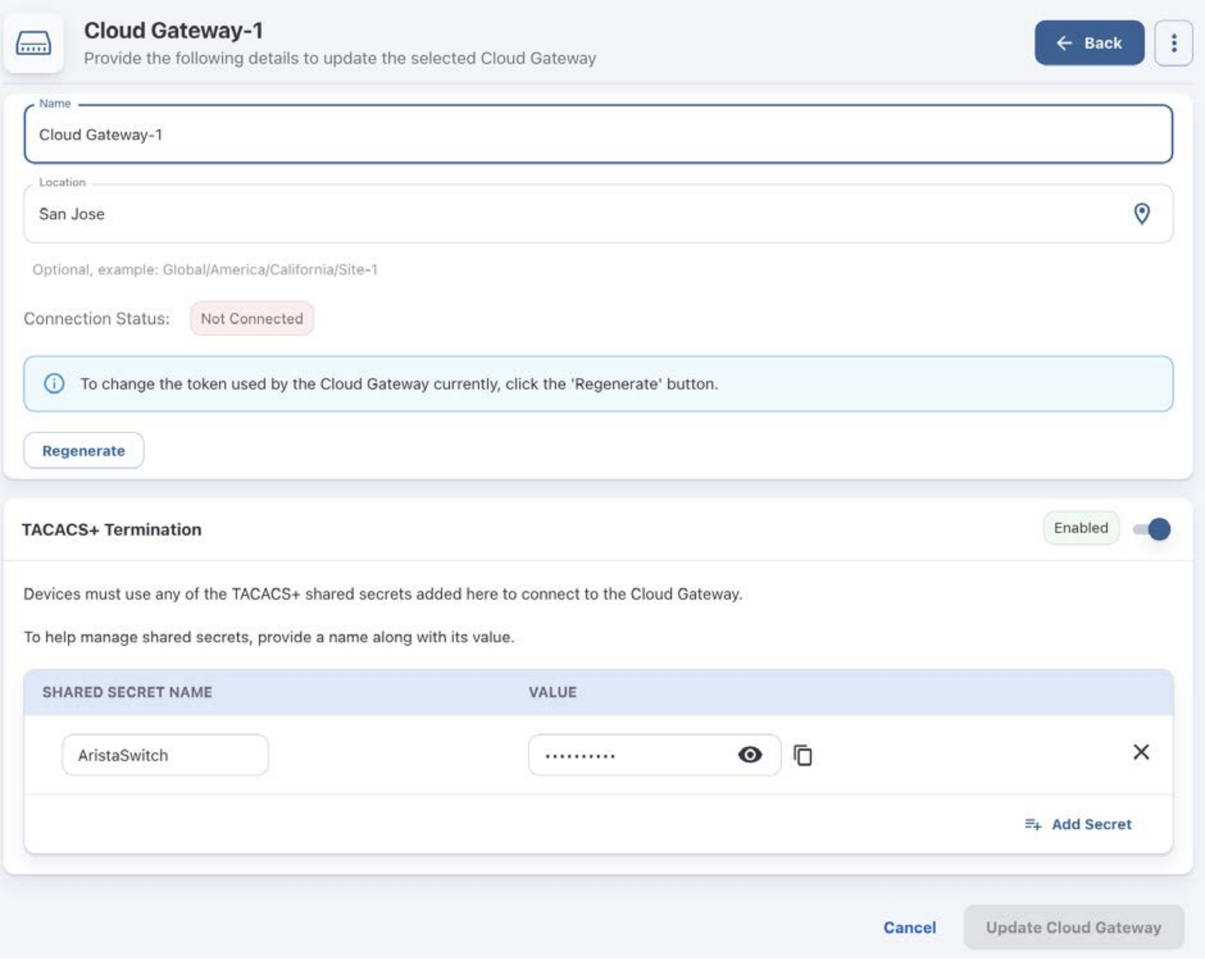
To help manage shared secrets, provide a name along with its value.

SHARED SECRET NAME	VALUE
AristaSwitch	••••••••••

Figure: Updating the Cloud Gateway

Note: For security reason, the generated token is visible only for the first time in AGNI portal. Ensure to copy and save the token when it is generated.

To generate a new Token, click the **Regenerate** button (see image below):



Cloud Gateway-1

Provide the following details to update the selected Cloud Gateway

Name: Cloud Gateway-1

Location: San Jose

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

Connection Status: Not Connected

To change the token used by the Cloud Gateway currently, click the 'Regenerate' button.

TACACS+ Termination: Enabled

Devices must use any of the TACACS+ shared secrets added here to connect to the Cloud Gateway.

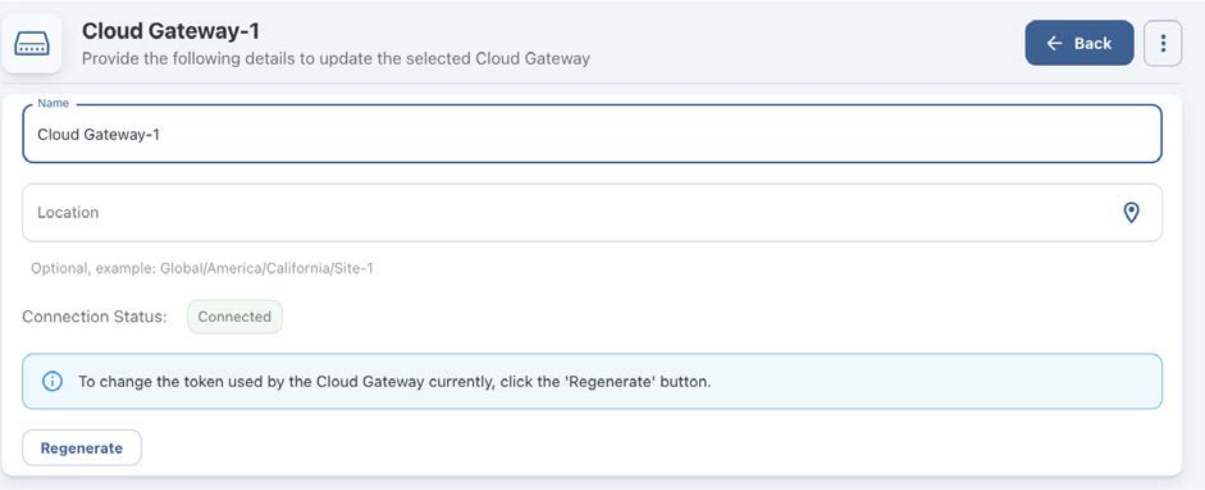
To help manage shared secrets, provide a name along with its value.

SHARED SECRET NAME	VALUE
AristaSwitch	•••••••••••

Figure: Regenerate Token

Once the Token generated by AGNI is used on Arista Cloud Gateway, the status of Cloud Gateway on AGNI reflects the connection status. Green status indicates a successful connection.

Similarly on Arista Cloud Gateway, "***trace monitor acg***" command displays the connection status in the logs.



Cloud Gateway-1

Provide the following details to update the selected Cloud Gateway

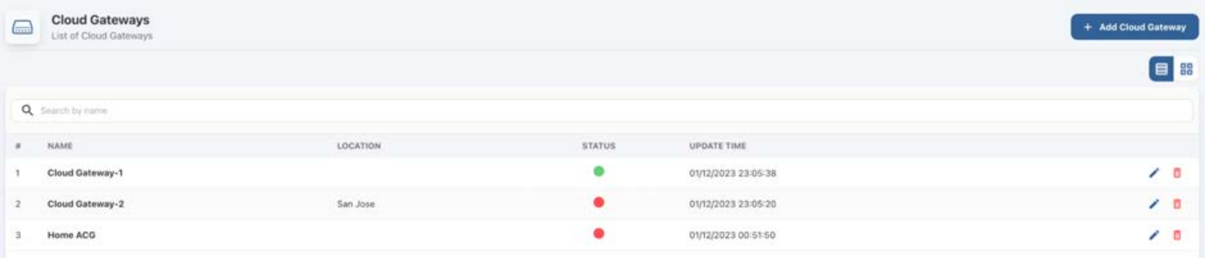
Name: Cloud Gateway-1

Location

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

Connection Status: Connected

To change the token used by the Cloud Gateway currently, click the 'Regenerate' button.



Cloud Gateways

List of Cloud Gateways

#	NAME	LOCATION	STATUS	UPDATE TIME
1	Cloud Gateway-1		🟢	01/12/2023 23:05:38
2	Cloud Gateway-2	San Jose	🔴	01/12/2023 23:05:20
3	Home ACG		🔴	01/12/2023 00:51:50

Figure: Regenerate Token Process

Configuring TACACS+ on Arista Switches

Below are the commands to configure TACACS+ on an Arista switch acting as a TACACS client:

```
conf terminal
tacacs-server policy unknown-mandatory-attribute ignore
tacacs-server host <IP_ACG> key <shared_secret>
```

Note: Shared_secret should be the same shared secret provided while adding the Arista Cloud Connect on AGNI.

```
aaa group server tacacs+ agni-tacacs
server <IP_ACG>
```

Note: In the above command, <IP_ACG> is the IP address of Arista Cloud Gateway, which is acting as a TACACS+ Proxy.

```
aaa authentication login default local group agni-tacacs
aaa authorization exec default local group agni-tacacs
aaa authorization commands all default local group agni-tacacs
```

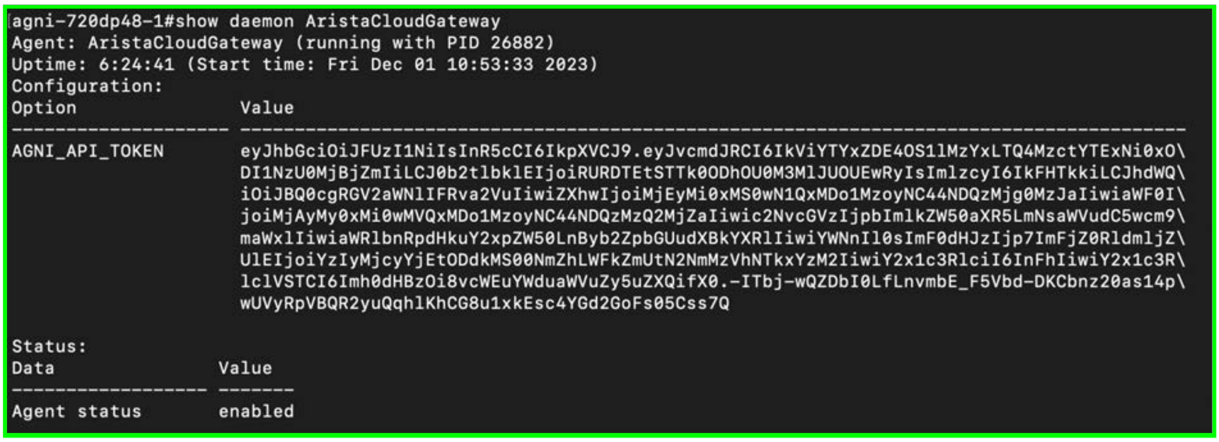
Debug commands on Arista Cloud Gateway

Below are sample debug commands that can be useful for troubleshooting purposes:

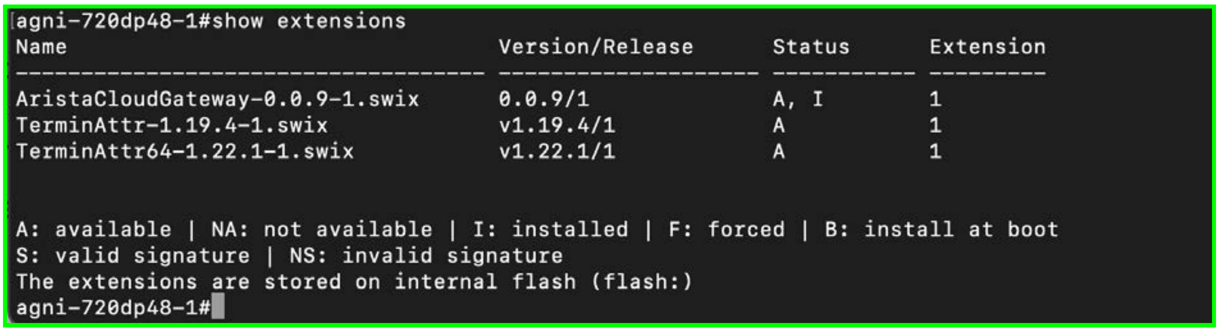
```
agni-720dp48-1(config-daemon-AristaCloudGateway)#trace monitor acg
```

```
--- Monitoring /var/log/agents/acg-AristaCloudGateway-26882 ---
2023/12/01 16:53:47 INFO websocket - connected successfully to
wss://qa.agnieng.net/acg/connect
2023/12/01 17:13:35 DEBUG [swix] handling agent shutdown/no shutdown:
False
2023/12/01 17:13:35 DEBUG [swix] stopping acg service
2023/12/01 17:13:35 DEBUG [swix] restricting port : 49
2023/12/01 17:13:35 DEBUG [swix] restricted port : 49
2023/12/01 17:13:35 DEBUG [swix] acg service stopped
2023/12/01 17:14:12 DEBUG [swix] handling agent shutdown/no shutdown:
True
2023/12/01 17:14:12 DEBUG [swix] allowing port : 49
2023/12/01 17:14:12 DEBUG [swix] allowed port : 49
2023/12/01 17:14:12 DEBUG [swix] setting-up acg service. wait for 10s
2023/12/01 17:14:22 DEBUG [swix] starting acg service
2023/12/01 17:14:22 DEBUG [swix] acg service started
2023/12/01 17:14:22 DEBUG [swix] AGNI_API_TOKEN(md5sum) :
831ca11c87f65ae90764c1ddf07e8e29
2023/12/01 17:14:22 DEBUG [swix] ENABLE_DEBUG_LOG : false
2023/12/01 17:14:22 DEBUG [swix] AGNI_ACG_TACACS_PORT : 49
2023/12/01 17:14:22 DEBUG [swix] AGNI_ACG_ENABLE_DHCP : false
2023/12/01 17:14:22 DEBUG [swix] AGNI_ACG_VRF : default
2023/12/01 17:14:22 DEBUG [swix] acg service started [pid=32154]
2023/12/01 17:14:23 INFO acg - dhcp module is disabled
2023/12/01 17:14:23 INFO tacacs - started gateway at 0.0.0.0:49
2023/12/01 17:14:23 INFO websocket - connected successfully to
wss://qa.agnieng.net/acg/connect
```

Note: Above command output shows that Arista Cloud gateway has successfully connected with AGNI and is listening on TCP port 49 for TACACS+ requests. See output details in images below:



```
agni-720dp48-1#show daemon AristaCloudGateway
Agent: AristaCloudGateway (running with PID 26882)
Uptime: 6:24:41 (Start time: Fri Dec 01 10:53:33 2023)
Configuration:
Option               Value
-------------------- ---------------------------------------------------------------------------------------
AGNI_API_TOKEN       eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IkViYTYxZDE4OS1lMzYxLTQ4MzctYTExNi0xO\
                     DI1NzU0MjBjZmIiLCJ0b2tlbklEIjoiRURDTEtSTTk0ODhOU0M3MlJUOUEwRyIsImlzcyI6IkFHTkkiLCJhdWQ\
                     iOiJBQ0cgRGV2aWNlIFRva2VuIiwiZXhwIjoiMjEyMi0xMS0wN1QxMDo1MzoyNC44NDQzMjg0MzJaIiwiaWF0I\
                     joiMjAyMy0xMi0wMVQxMDo1MzoyNC44NDQzMzQ2MjZaIiwic2NvcGVzIjpbImlkZW50aXR5LmNsaWVudC5wcm9\
                     maWxlIiwiaWRlbnRpdHkuY2xpZW50LnByb2ZpbGUudXBkYXRlIiwiYWNnIl0sImF0dHJzIjp7ImFjZ0RldmljZ\
                     UlEIjoiYzIyMjcyYjEtODdkMS00NmZhLWFkZmUtN2NmMzVhNTkxYzM2IiwiY2x1c3RlciI6InFhIiwiY2x1c3R\
                     lclVSTCI6Imh0dHBzOi8vcWEuYWduaWVuZy5uZXQifX0.-ITbj-wQZDbI0LfLnvmbE_F5Vbd-DKCbnz20as14p\
                     wUVyRpVBQR2yuQqhlKhCG8u1xkEsc4YGd2GoFs05Css7Q

Status:
Data               Value
------------------ -------
Agent status       enabled
```



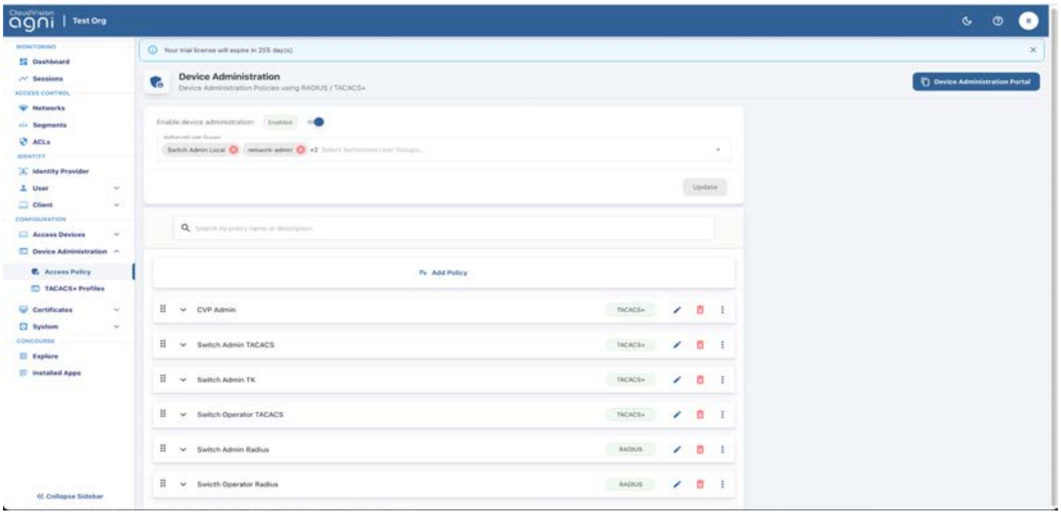
```
[agni-720dp48-1#show extensions
 Name                                   Version/Release      Status       Extension
 -------------------------------------- -------------------- ------------ ---------
 AristaCloudGateway-0.0.9-1.swix        0.0.9/1              A, I         1
 TerminAttr-1.19.4-1.swix               v1.19.4/1            A            1
 TerminAttr64-1.22.1-1.swix             v1.22.1/1            A            1


 A: available | NA: not available | I: installed | F: forced | B: install at boot
 S: valid signature | NS: invalid signature
 The extensions are stored on internal flash (flash:)
 agni-720dp48-1#
```

Figure: Command Output

Device Administration on AGNI

Device Administration toggle should be enabled on AGNI and should provide specified group access. Multiple Access policies can be added for the same. To enable Device Administartion:

- Navigate to **Device Administartion** -> **Access Policy.**
- Select Enable device administartion **Enabled** button (see image blow).



Your trial license will expire in 255 day(s).

Device Administration

Device Administration Policies using RADIUS / TACACS+

Enable device administration: Enabled

Authorized User Groups: Switch Admin Local, network-admin +2

Search by policy name or description

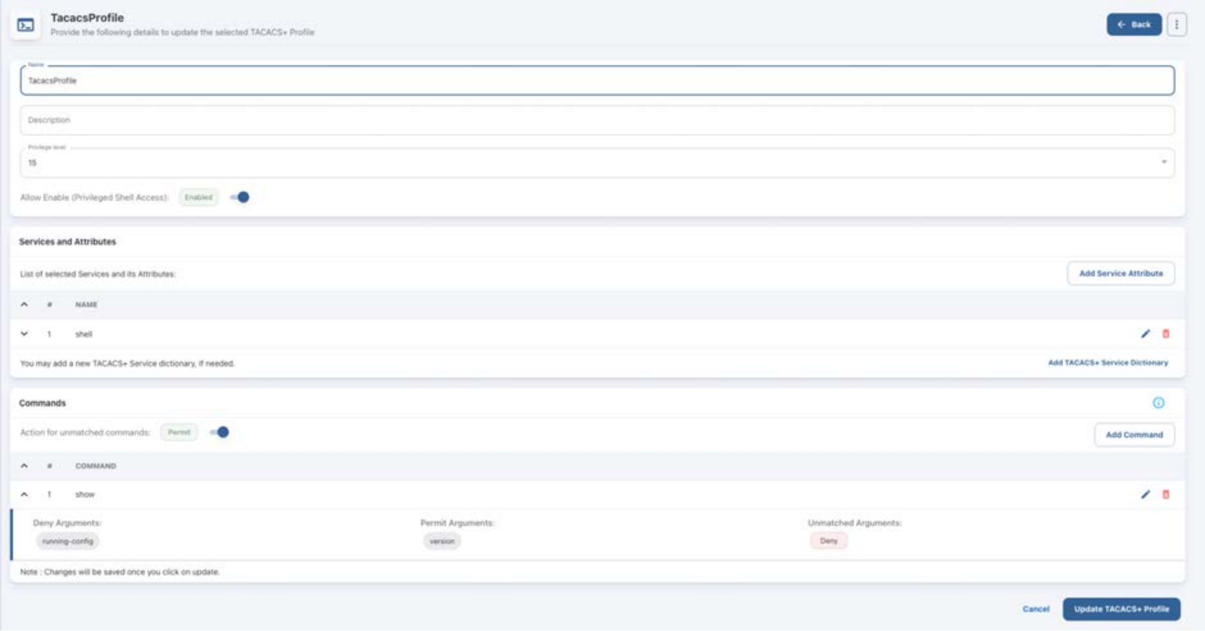
CVP Admin	TACACS+
Switch Admin TACACS	TACACS+
Switch Admin TK	TACACS+
Switch Operator TACACS	TACACS+
Switch Admin Radius	RADIUS
Swicth Operator Radius	RADIUS

Figure: Device Administration Enabled

Configuring TACACS+ on AGNI

You can configure Tacacs+ on AGNI by creating TACACS+ Profile and applying the Profile through the Access Policy.

You can create TACACS+ Profiles by navigating to **Device Administration→TACACS+ Profiles**.



TacacsProfile

Provide the following details to update the selected TACACS+ Profile

Name: TacacsProfile

Description

Privilege level: 15

Allow Enable (Privileged Shell Access): Enabled

Services and Attributes

List of selected Services and its Attributes:

#	NAME
1	shell

You may add a new TACACS+ Service dictionary, if needed.

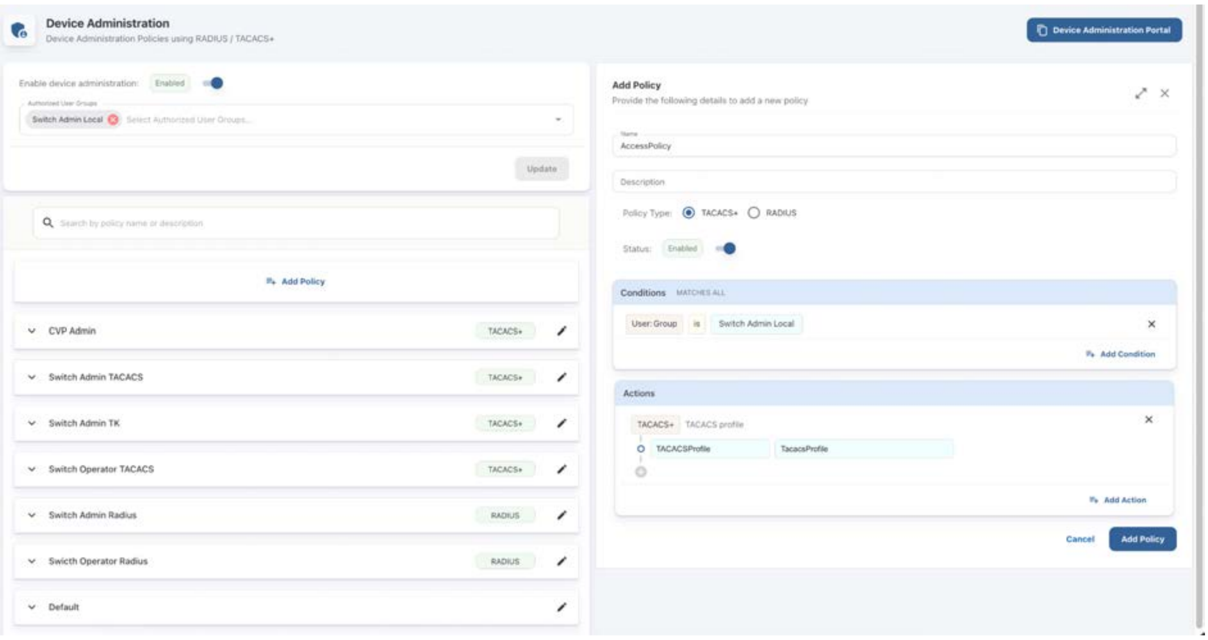
Commands

Action for unmatched commands: Permit

#	COMMAND
1	show

Deny Arguments:	Permit Arguments:	Unmatched Arguments:
running-config	version	Deny

Note : Changes will be saved once you click on update.



Device Administration

Device Administration Policies using RADIUS / TACACS+

Enable device administration: Enabled

Authorized User Groups: Switch Admin Local

Select Authorized User Groups...

Search by policy name or description

CVP Admin	TACACS+
Switch Admin TACACS	TACACS+
Switch Admin TK	TACACS+
Switch Operator TACACS	TACACS+
Switch Admin Radius	RADIUS
Swicth Operator Radius	RADIUS
Default	

Add Policy

Provide the following details to add a new policy

Name: AccessPolicy

Description

Policy Type: ● TACACS+ ○ RADIUS

Status: Enabled

Conditions MATCHES ALL

User: Group is Switch Admin Local

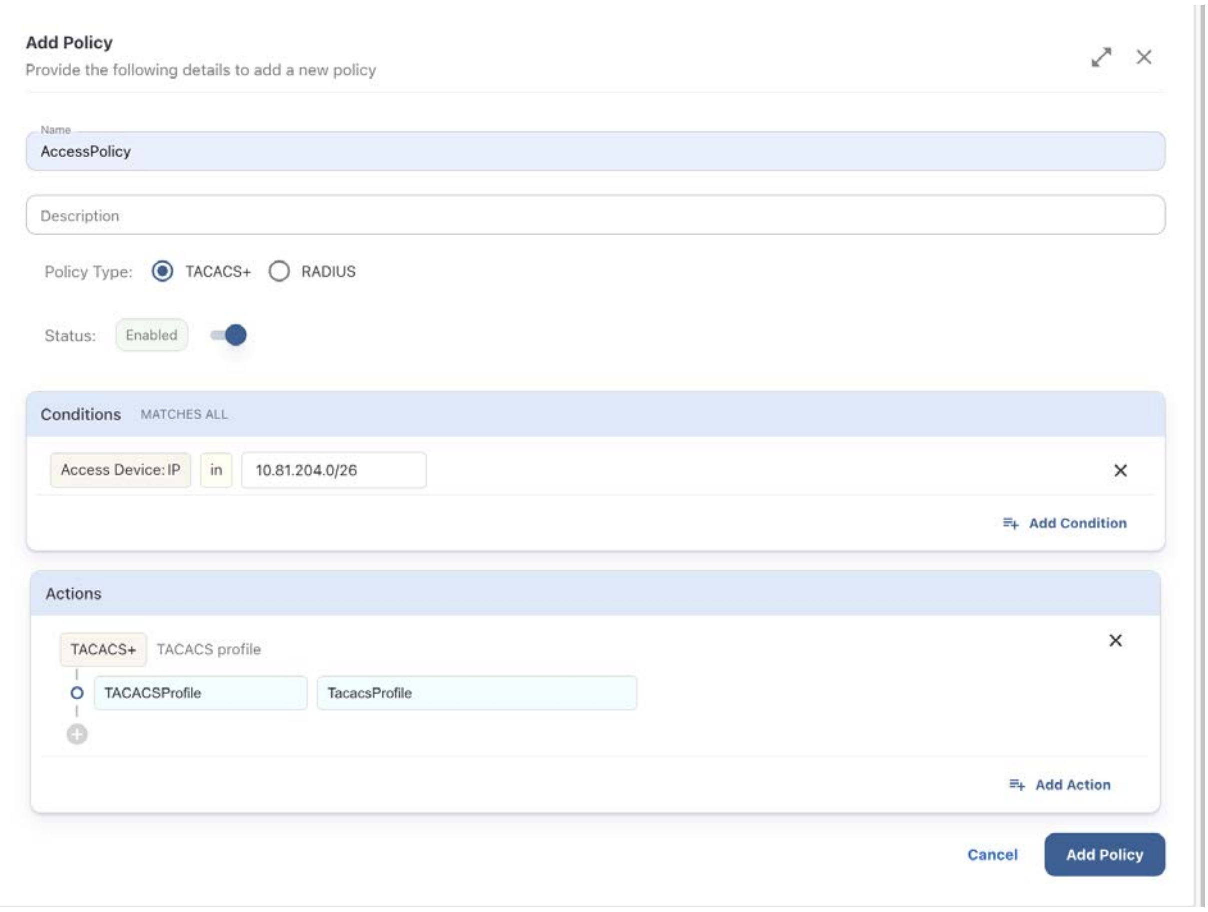
Actions

TACACS+ TACACS profile

TACACSProfile TacacsProfile

Figure: Creating TACACS+ Profiles

Conditions for the Access Policy are based upon User, Access Device, or CloudGateway (see image below):



Add Policy

Provide the following details to add a new policy

Name: AccessPolicy

Description

Policy Type: ● TACACS+ ○ RADIUS

Status: Enabled

Conditions MATCHES ALL

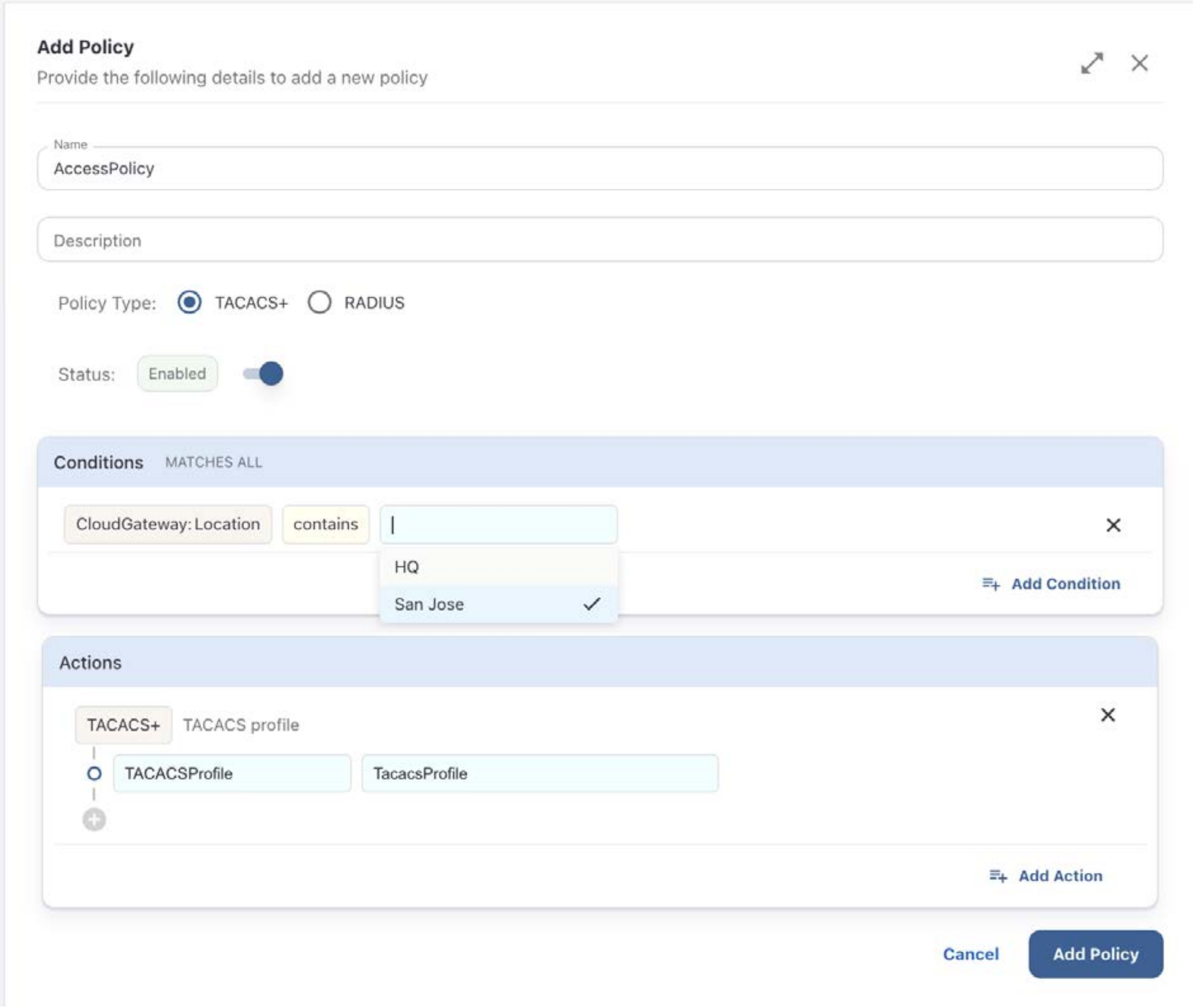
Access Device: IP in 10.81.204.0/26

Actions

TACACS+ TACACS profile

TACACSProfile TacacsProfile

Figure: Creating TACACS+ Prolicy Details



Add Policy

Provide the following details to add a new policy

Name: AccessPolicy

Description

Policy Type: ● TACACS+ ○ RADIUS

Status: Enabled

Conditions MATCHES ALL

CloudGateway: Location | contains |

HQ

San Jose ✓

Add Condition

Actions

TACACS+ TACACS profile

TACACSProfile | TacacsProfile

Add Action

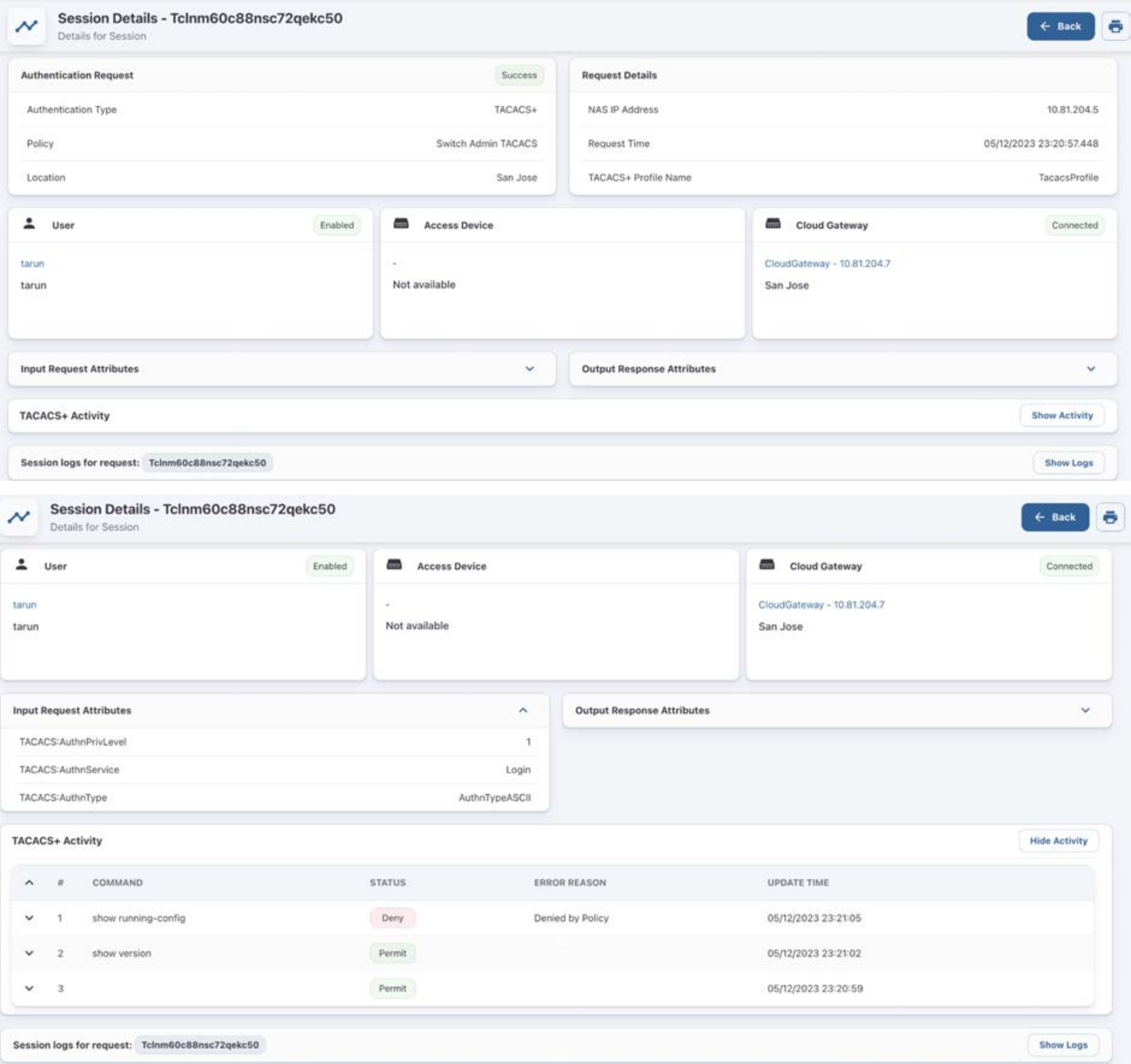
Cancel

Add Policy

Figure: Creating TACACS+ Prolicy Details-Conditions

Monitoring TACACS+ on AGNI

You can view the TACACS+ session details by navigating to **Monitoring** → **Sessions** → Show Details (eye icon):



Authentication Request	Success
Authentication Type	TACACS+
Policy	Switch Admin TACACS
Location	San Jose

Request Details	
NAS IP Address	10.81.204.5
Request Time	05/12/2023 23:20:57.448
TACACS+ Profile Name	TacacsProfile

tarun
tarun

-
Not available

CloudGateway - 10.81.204.7
San Jose

Session logs for request: Tclnm60c88nsc72qekc50

tarun
tarun

-
Not available

CloudGateway - 10.81.204.7
San Jose

Input Request Attributes	
TACACS:AuthnPrivLevel	1
TACACS:AuthnService	Login
TACACS:AuthnType	AuthnTypeASCII

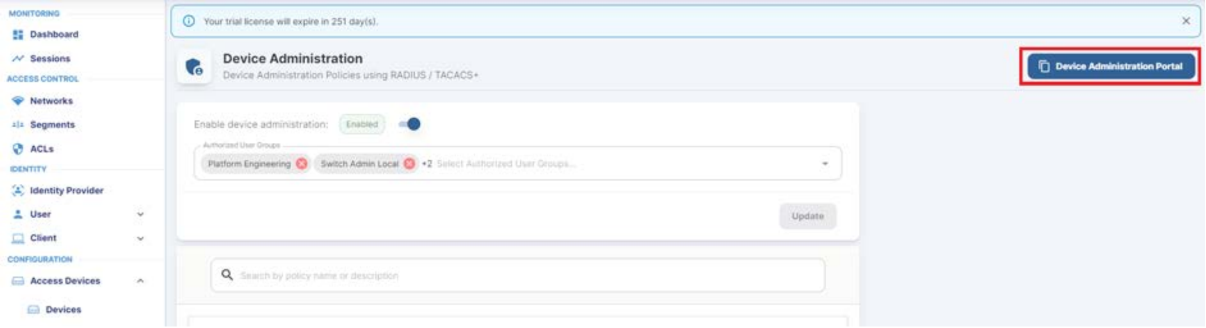
#	COMMAND	STATUS	ERROR REASON	UPDATE TIME
1	show running-config	Deny	Denied by Policy	05/12/2023 23:21:05
2	show version	Permit		05/12/2023 23:21:02
3		Permit		05/12/2023 23:20:59

Session logs for request: Tclnm60c88nsc72qekc50

Figure: TACACS+ Session Details

Self Service Portal on AGNI

To access the Self Service Portal admin needs to navigate to ***Device Administration-> Access Policy***. Click on **Device Administration Portal**



Your trial license will expire in 251 day(s).

Device Administration
Device Administration Policies using RADIUS / TACACS+

Enable device administration: Enabled

Authorized User Groups: Platform Engineering, Switch Admin Local, +2 Select Authorized User Groups...

Search by policy name or description

Figure: Self Service Portal

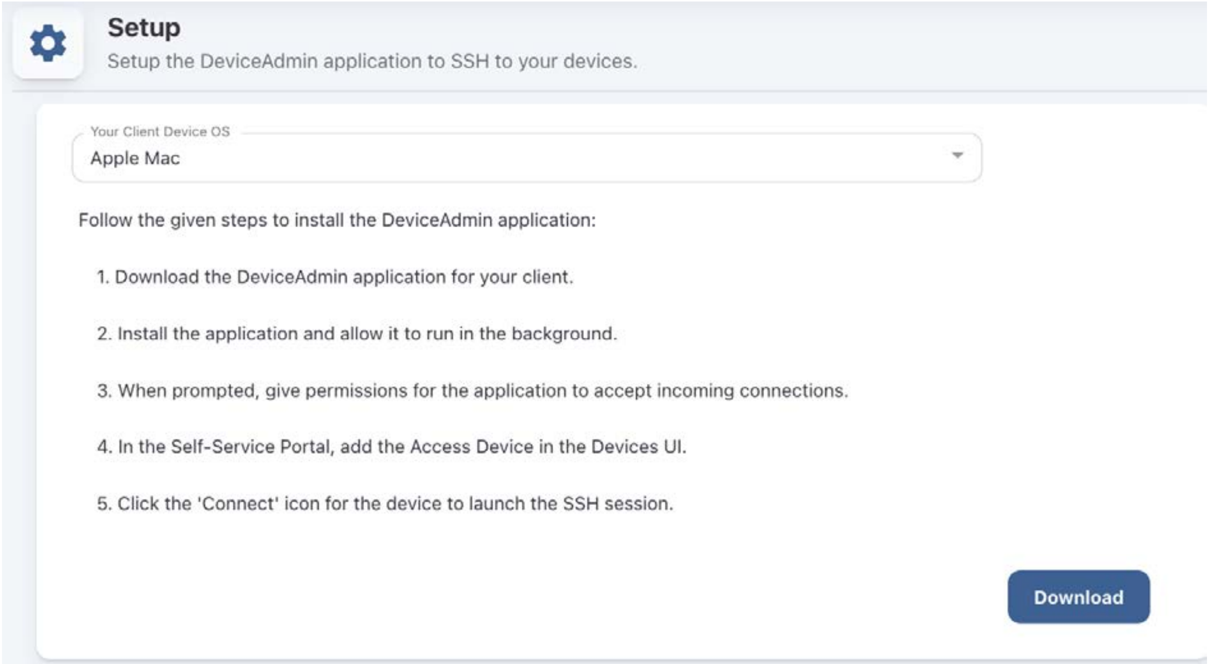
Device administration functionality is accessible to users belonging to authorized user groups from the AGNI self service portal.The self service portal provides a browser based *shell to SSH to devices* that are to be managed. End users can add a list of devices they frequently access for device management in the self service portal by specifying below details.

- **Name -** This is a friendly name for the device
- **IP address -** IP address of the target device
- **Port -** The SSH port of the target device

The self service portal supports importing of network devices in CSV format. Users should first download and run the AGNI app on their local laptop. The app is supported on MacOS and Windows platforms and you can download from the self service portal.

By logging in to the Self Service Portal, you can install the App (see image below) based on the operating system of your computer as it is a session launched from the browser.

.



Setup

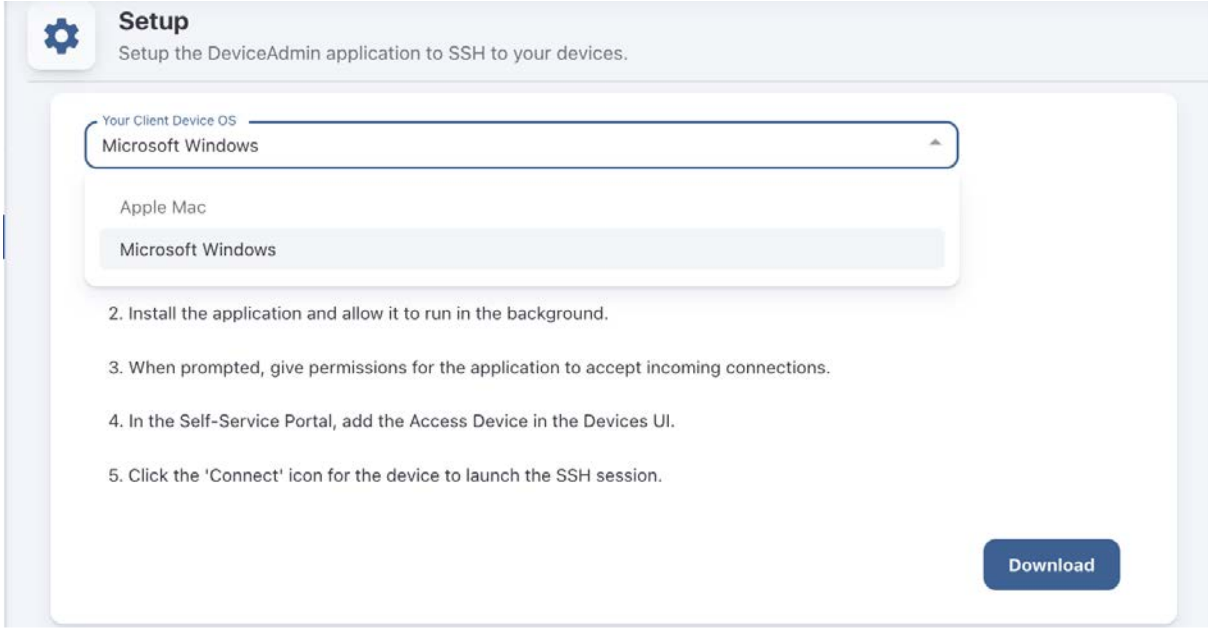
Setup the DeviceAdmin application to SSH to your devices.

Your Client Device OS: Apple Mac

Follow the given steps to install the DeviceAdmin application:

1. Download the DeviceAdmin application for your client.
2. Install the application and allow it to run in the background.
3. When prompted, give permissions for the application to accept incoming connections.
4. In the Self-Service Portal, add the Access Device in the Devices UI.
5. Click the 'Connect' icon for the device to launch the SSH session.

Figure: Self Service Portal for Mac OS



Setup

Setup the DeviceAdmin application to SSH to your devices.

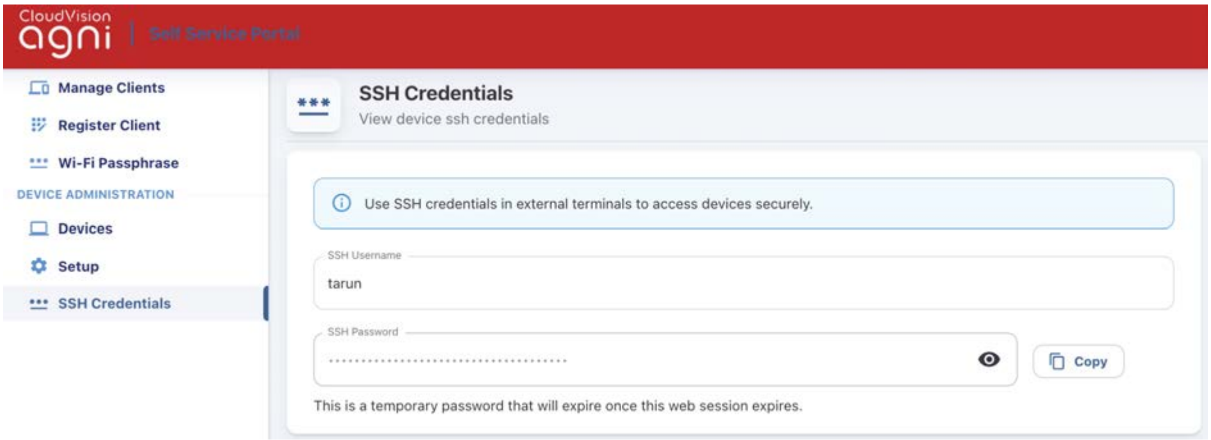
Your Client Device OS: Microsoft Windows

2. Install the application and allow it to run in the background.
3. When prompted, give permissions for the application to accept incoming connections.
4. In the Self-Service Portal, add the Access Device in the Devices UI.
5. Click the 'Connect' icon for the device to launch the SSH session.

Figure: Self Service Portal for Windows

Once the AGNI app is installed on the laptop, you can add the NAD’s under Devices. Also, you can use the **Import** option to import clients to AGNI in the form of a csv file.

Note: The system admin can initiate SSH session from local SSH clients installed on the laptop like *PUTTY*, *SecureCRT* or any other terminal by navigating to SSH credentials and getting the Session password, which is available only for the time the user is logged in.



SSH Credentials

View device ssh credentials

Use SSH credentials in external terminals to access devices securely.

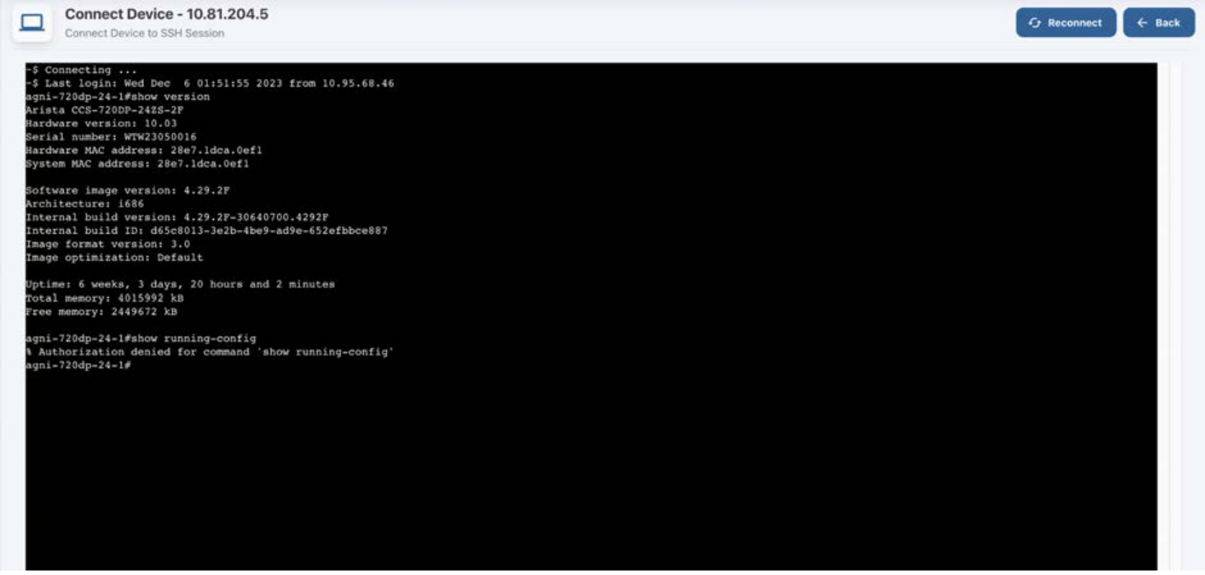
SSH Username: tarun

SSH Password: ••••••••••••••••••••••••••••••••••••••

This is a temporary password that will expire once this web session expires.

Figure: SSH Credentials

Below image displays the TACACS+ authorization allowed (first show output) and authorization denied (second show output).



Connect Device - 10.81.204.5

Connect Device to SSH Session

```
-$ Connecting ...
-$ Last login: Wed Dec  6 01:51:55 2023 from 10.95.68.46
agni-720dp-24-1#show version
Arista CCS-720DP-24ZS-2F
Hardware version: 10.03
Serial number: WTW23050016
Hardware MAC address: 28e7.1dca.0ef1
System MAC address: 28e7.1dca.0ef1

Software image version: 4.29.2F
Architecture: i686
Internal build version: 4.29.2F-30640700.4292F
Internal build ID: d65c8013-3e2b-4be9-ad9e-652efbbce887
Image format version: 3.0
Image optimization: Default

Uptime: 6 weeks, 3 days, 20 hours and 2 minutes
Total memory: 4015992 kB
Free memory: 2449672 kB

agni-720dp-24-1#show running-config
% Authorization denied for command 'show running-config'
agni-720dp-24-1#
```

Figure: TACACS+ Authorization Allowed and Denied Output

Configuring Cloud Gateway to Integrate AGNI with On-Premises Setup

This article describes how an on-premises container service, which is the Cloud Gateway, can send IP and other DHCP information to AGNI. To successfully send the IP and DHCP information to AGNI, install a DHCP relay container in your docker environment, preferably on a Linux platform.

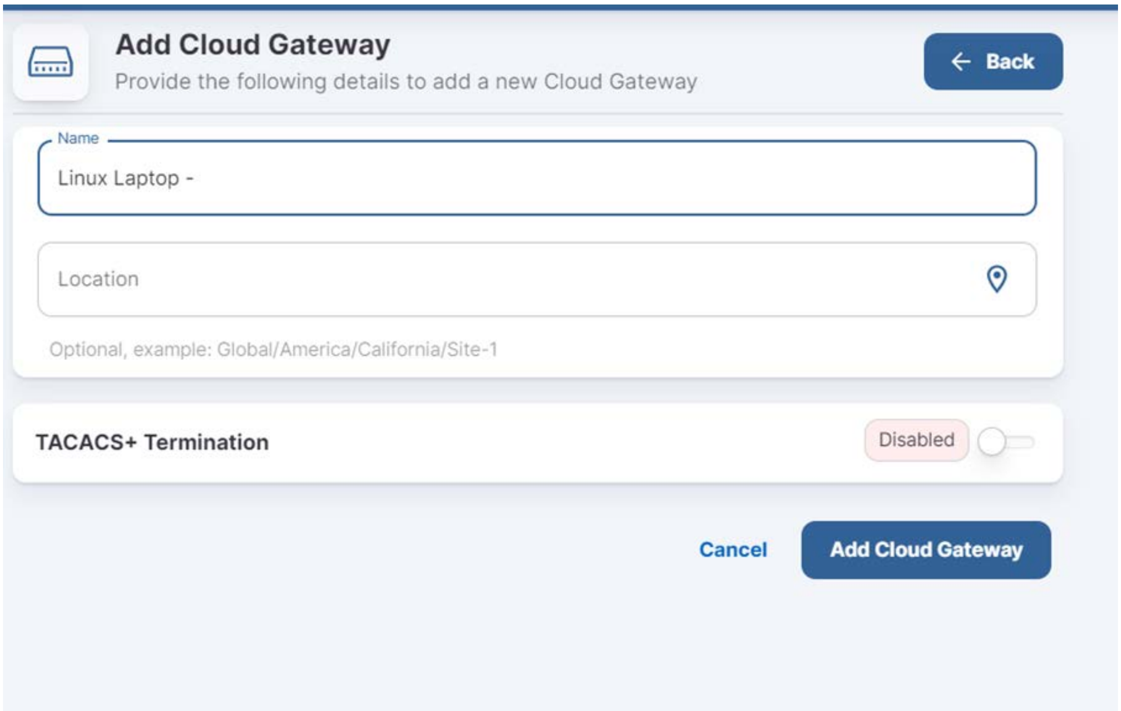
The Cloud Gateway must meet the following requirements:

- It must have Internet access to communicate with AGNI.
- It must be able to communicate with the network infrastructure for relaying the client's IP to AGNI.
- The container listens on port 67 to get the DHCP information from clients and send it to AGNI. The container establishes a secure web socket connection with AGNI over HTTPS.

To establish a connection between AGNI and the Cloud Gateway, administrators need to configure AGNI and the docker.

Configuring Cloud Gateway in AGNI

1. Navigate to **Configuration > Access Devices > Cloud Gateway**.
2. Click **Add** to add a new Cloud Gateway.



Add Cloud Gateway

Provide the following details to add a new Cloud Gateway

Name: Linux Laptop -

Location

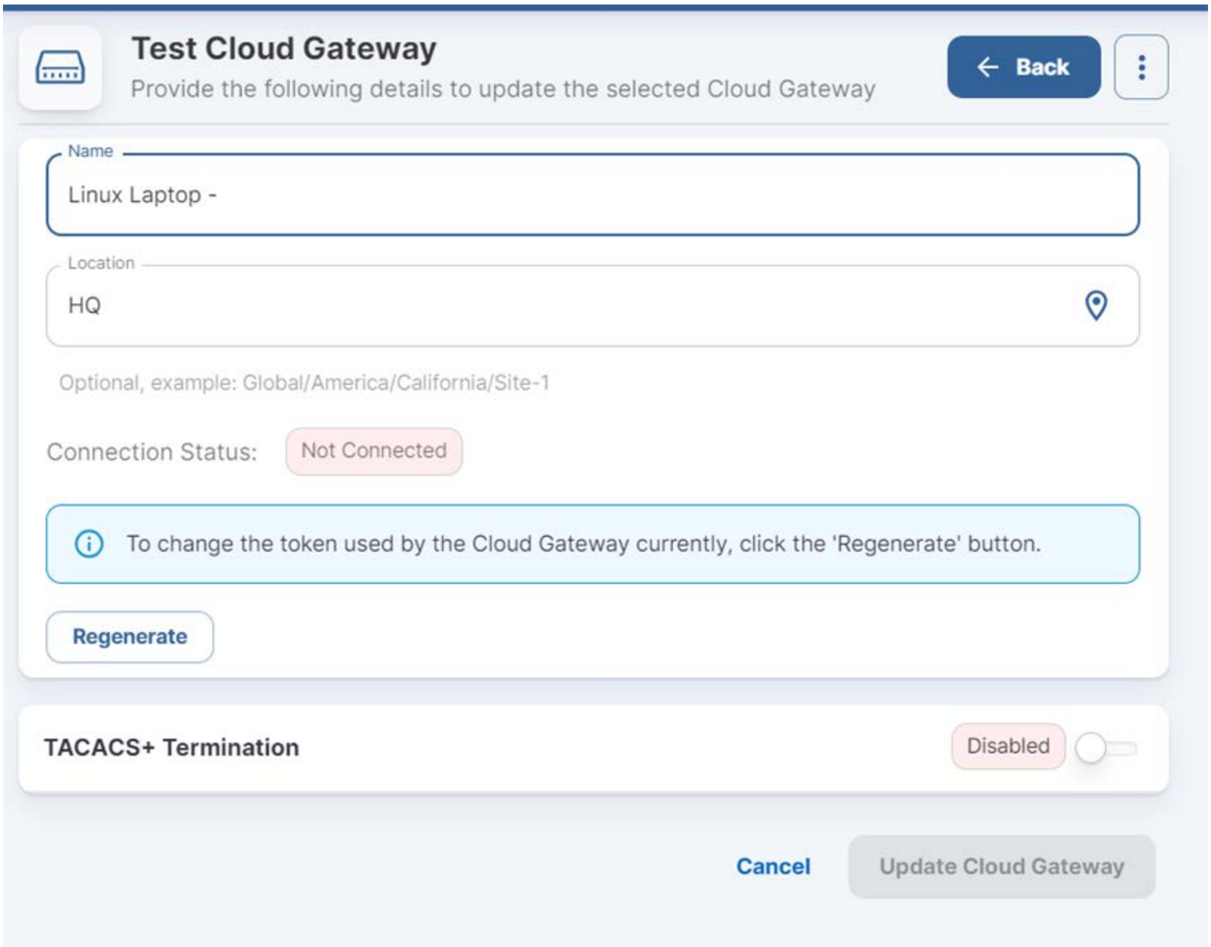
Optional, example: Global/America/California/Site-1

TACACS+ Termination: Disabled

Figure: Adding Cloud Gateway

3. Provide a name for the gateway and click ***Add Cloud Gateway.***
   A token is generated.
4. Copy the token. You need the token to bootstrap the Cloud Gateway in order to establish a secure connection with the AGNI cloud server.
   Note: For security reasons, the generated token is displayed only once on the UI. Ensure to copy and save the token.

logs.



Test Cloud Gateway

Provide the following details to update the selected Cloud Gateway

Name: Linux Laptop -

Location: HQ

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

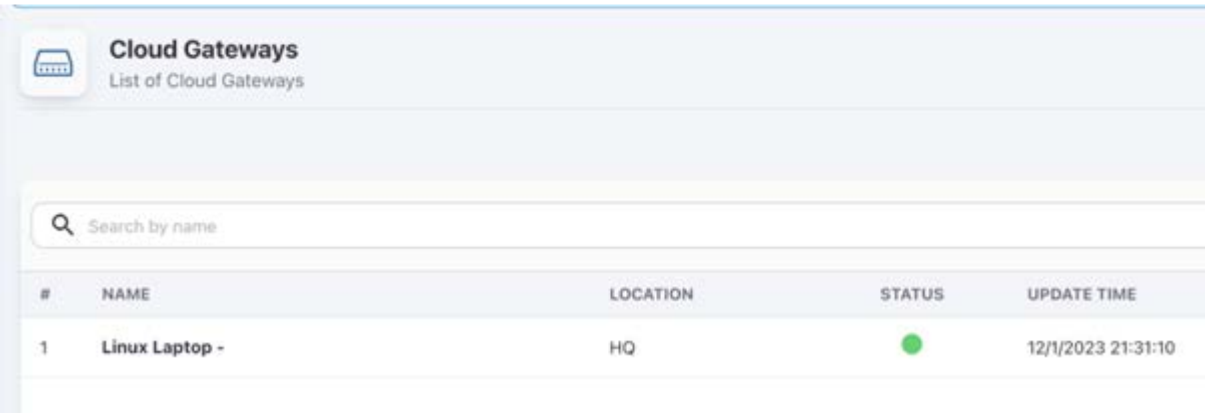
Connection Status: Not Connected

To change the token used by the Cloud Gateway currently, click the 'Regenerate' button.

TACACS+ Termination: Disabled

Figure: Adding Cloud Gateway -2

5. To generate a new Token, click the **Regenerate** button.
   Once the Cloud Gateway is established, the connection status of the gateway changes to Green.



Cloud Gateways

List of Cloud Gateways

Search by name

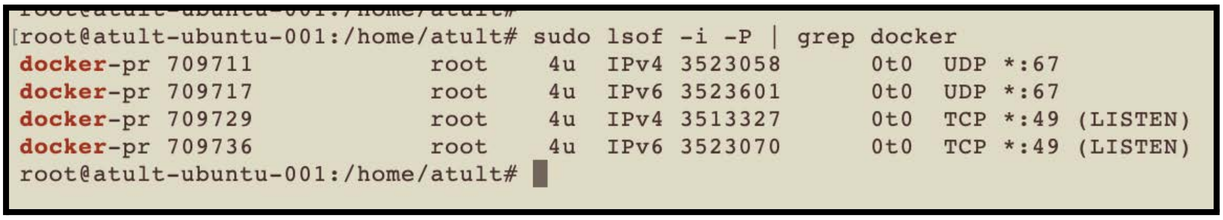
#	NAME	LOCATION	STATUS	UPDATE TIME
1	Linux Laptop -	HQ	●	12/1/2023 21:31:10

Figure: Adding Cloud Gateway -3

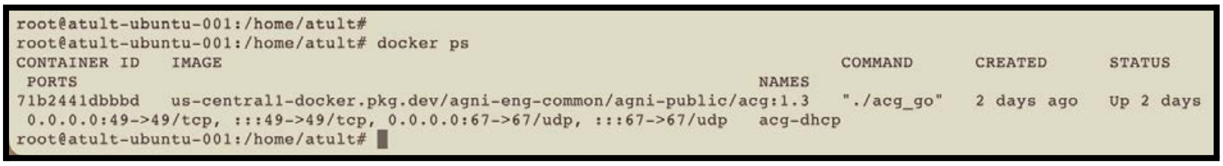
On the Cloud Gateway, the **trace monitor acg** command shows the connected status in the logs.

Installing Cloud Gateway

1. Choose a client system (for example, Mac OS) where you want to install the Cloud Gateway.
2. Install Docker Desktop on the client system. Follow the installation steps from the docker website:
   https://www.docker.com/products/docker-desktop
3. Start the Docker container
   ```
   nohup docker run --rm --name acg-dhcp
     -p 67:67/udp -p 49:49 --env AGNI_ACG_ENABLE_DHCP=true --env
   ENABLE_DEBUG_LOG=true --env AGNI_API_TOKEN=<your token here>
   us-central1-docker.pkg.dev/agni-eng-common/agni-public/acc:1.
   3 &
   ```
4. Validate **Port 67** is running on the client machine where you have installed Docker.



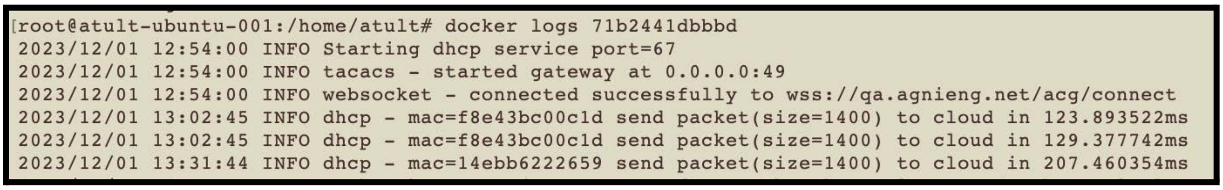
```
root@atult-ubuntu-001:/home/atult# sudo lsof -i -P | grep docker
docker-pr 709711            root    4u  IPv4 3523058      0t0  UDP *:67
docker-pr 709717            root    4u  IPv6 3523601      0t0  UDP *:67
docker-pr 709729            root    4u  IPv4 3513327      0t0  TCP *:49 (LISTEN)
docker-pr 709736            root    4u  IPv6 3523070      0t0  TCP *:49 (LISTEN)
root@atult-ubuntu-001:/home/atult# 
```



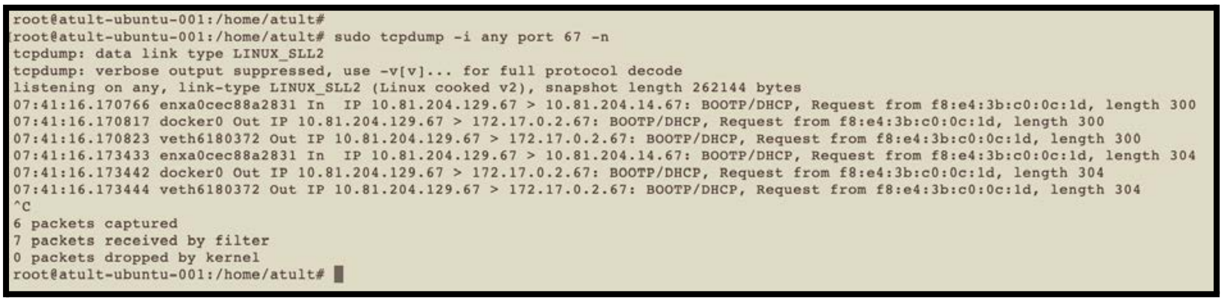
```
root@atult-ubuntu-001:/home/atult#
root@atult-ubuntu-001:/home/atult# docker ps
CONTAINER ID   IMAGE                                                    COMMAND      CREATED      STATUS
 PORTS                                                              NAMES
71b2441dbbbd   us-central1-docker.pkg.dev/agni-eng-common/agni-public/acg:1.3   "./acg_go"   2 days ago   Up 2 days
 0.0.0.0:49->49/tcp, :::49->49/tcp, 0.0.0.0:67->67/udp, :::67->67/udp   acg-dhcp
root@atult-ubuntu-001:/home/atult# 
```

Debugging Workflow

Validate that DHCP Packets are received on Port 67 on the host machine



```
root@atult-ubuntu-001:/home/atult# docker logs 71b2441dbbbd
2023/12/01 12:54:00 INFO Starting dhcp service port=67
2023/12/01 12:54:00 INFO tacacs - started gateway at 0.0.0.0:49
2023/12/01 12:54:00 INFO websocket - connected successfully to wss://qa.agnieng.net/acg/connect
2023/12/01 13:02:45 INFO dhcp - mac=f8e43bc00c1d send packet(size=1400) to cloud in 123.893522ms
2023/12/01 13:02:45 INFO dhcp - mac=f8e43bc00c1d send packet(size=1400) to cloud in 129.377742ms
2023/12/01 13:31:44 INFO dhcp - mac=14ebb6222659 send packet(size=1400) to cloud in 207.460354ms
```



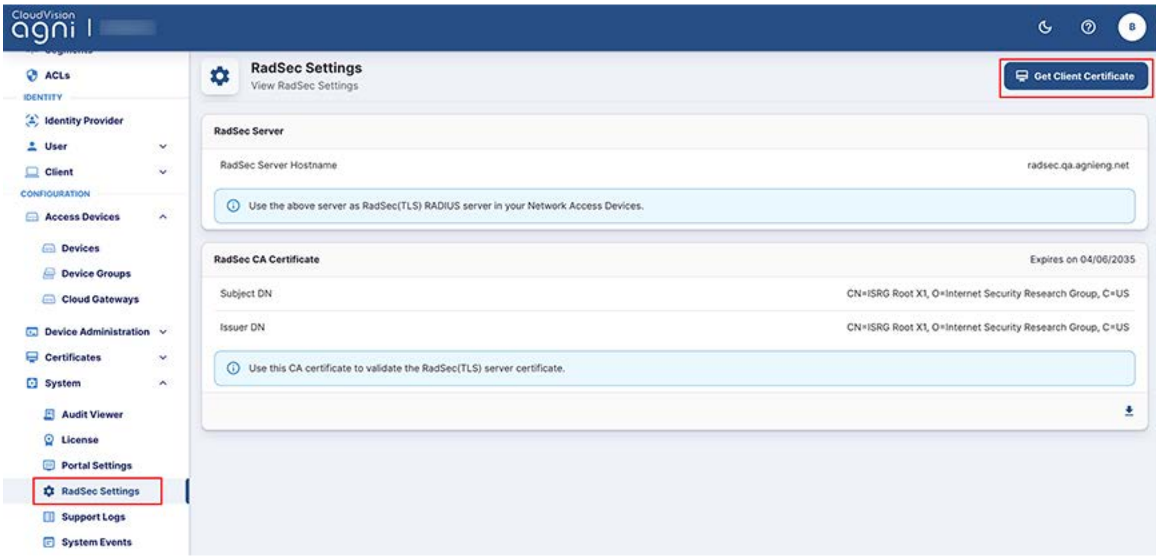
```
root@atult-ubuntu-001:/home/atult#
root@atult-ubuntu-001:/home/atult# sudo tcpdump -i any port 67 -n
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
07:41:16.170766 enxa0cec88a2831 In  IP 10.81.204.129.67 > 10.81.204.14.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.170817 docker0 Out IP 10.81.204.129.67 > 172.17.0.2.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.170823 veth6180372 Out IP 10.81.204.129.67 > 172.17.0.2.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 300
07:41:16.173433 enxa0cec88a2831 In  IP 10.81.204.129.67 > 10.81.204.14.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.173442 docker0 Out IP 10.81.204.129.67 > 172.17.0.2.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
07:41:16.173444 veth6180372 Out IP 10.81.204.129.67 > 172.17.0.2.67: BOOTP/DHCP, Request from f8:e4:3b:c0:0c:1d, length 304
^C
6 packets captured
7 packets received by filter
0 packets dropped by kernel
root@atult-ubuntu-001:/home/atult# 
```

Generating Client Certificates

AGNI establishes RadSec connection with the network devices. In most cases, the Trusted Platform Module (TPM) certificate of the network devices can be used to establish the RadSec connection. In cases where this is not possible, AGNI enables you to generate a self-signed certificate for the access devices and it can be used to establish a RadSec tunnel. You can also get network access device certificates externally and use it for RadSec communication.

You can generate the client certificates by following one of the below methods:

- Navigate to **System** -> **RadSec Settings** and click on **Get Client Certificate** (see image below).



RadSec Settings
View RadSec Settings

RadSec Server

RadSec Server Hostname radsec.qa.agnieng.net

Use the above server as RadSec(TLS) RADIUS server in your Network Access Devices.

RadSec CA Certificate Expires on 04/06/2035

Subject DN CN=ISRG Root X1, O=Internet Security Research Group, C=US

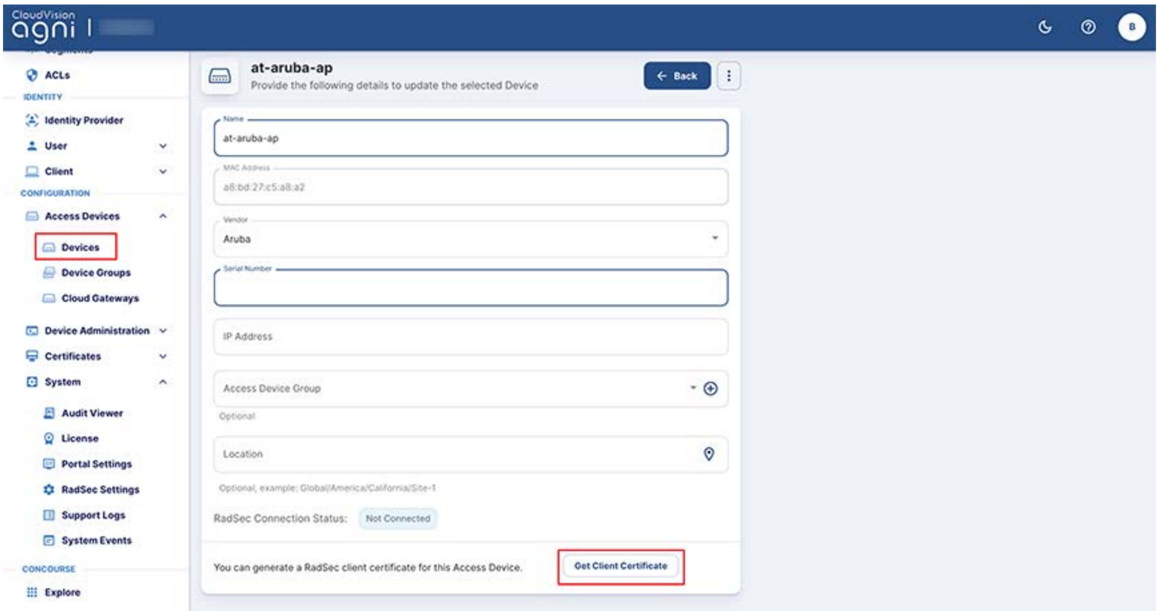
Issuer DN CN=ISRG Root X1, O=Internet Security Research Group, C=US

Use this CA certificate to validate the RadSec(TLS) server certificate.

Figure: RadSec Settings Certificate Generate Page

OR

- Navigate to **Configuration** -> **Access Devices** -> **Devices**. Click on any device. On the Device page, click **Get Client Certificate** (see image below)



at-aruba-ap

Provide the following details to update the selected Device

Name: at-aruba-ap

MAC Address: a8:bd:27:c5:a8:a2

Vendor: Aruba

Serial Number

IP Address

Access Device Group

Optional

Location

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

RadSec Connection Status: Not Connected

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

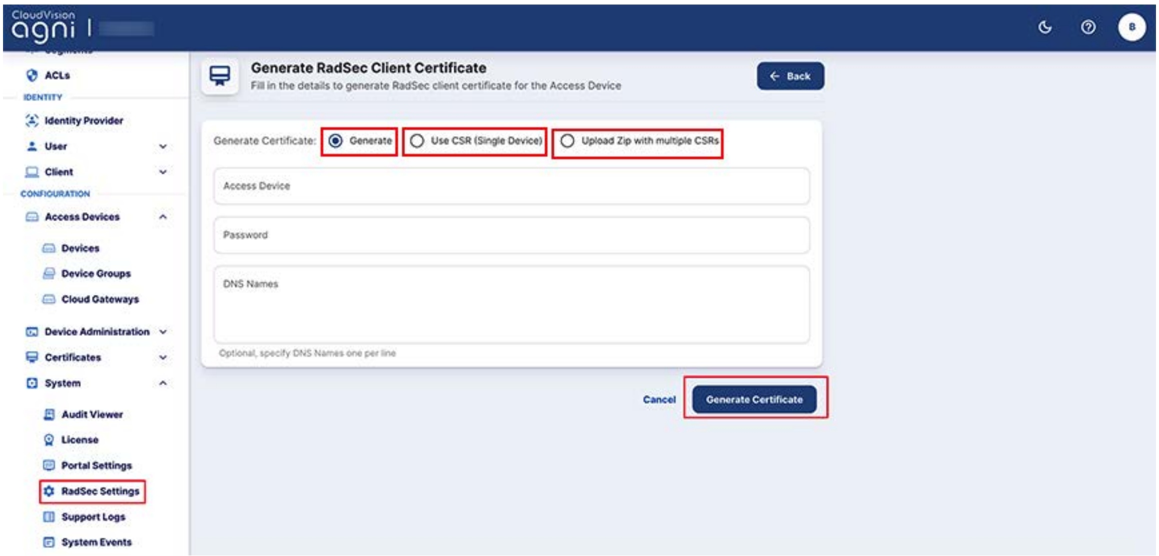
Figure: Device Settings Certificate Generate Page

You can generate the certificate in one of the three ways below (see Figure 20) :

- Click the **Generate** option for AGNI to automatically generate the certificate.
  The certificate generation process involves generating the device certificate and the corresponding private key. When you click on the **Generate Certificate** button, the system generates a *p12* file containing a self-signed certificate and private key for the network access device. The output is encrypted using a password provided by the administrator.

- Click the **Use CSR (Single Device)** option to generate a CSR certificate for a single device.
  This is done by uploading the Certificate Signing Request (CSR). In this case, the CSR is generated on the network access device (refer to vendor-specific documentation) and the output is provided in the interface here. The system signs the CSR and generates the certificate that can be uploaded to the network access device.

- Click Upload Zip with multiple CSRs to upload a zip file containing CSR certificates for several devices together.
  For Arista WiFi devices, you can generate bulk CSRs from Arista CV-CUE interface. Bulk CSRs can be uploaded as a zip file to generate the client certificates.



Generate RadSec Client Certificate

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

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

Access Device

Password

DNS Names

Optional, specify DNS Names one per line

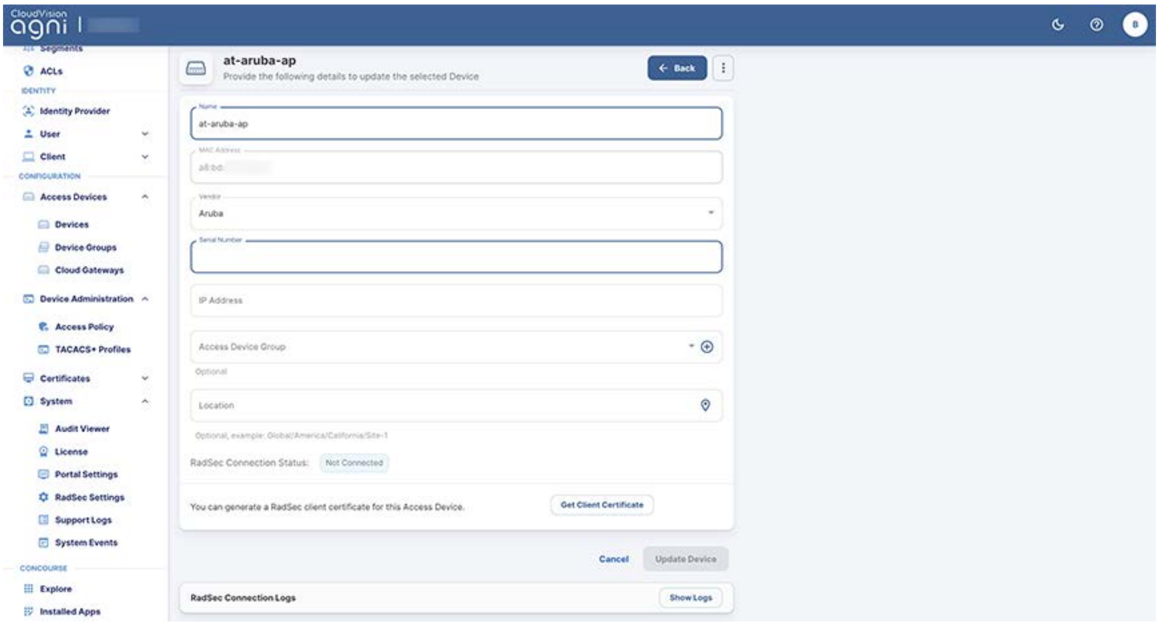
Figure: RadSec Client Certificate Generating Options

After selecting one of the Generate Certificate options, enter the following details:

- Name of the device
- MAC address of the devivce
- Select the Vendor
- Enter Serial Number of the device (mandatory for Cisco Meraki devices)
- DNS as domain name

You can upload the CSR or copy and paste the content in the UI.

The RadSec status is conveyed in the administration. The connection details can be verified by checking the device logs for each access device.



at-aruba-ap

Provide the following details to update the selected Device

Name: at-aruba-ap

MAC Address: a8:bd:[redacted]

Vendor: Aruba

Serial Number

IP Address

Access Device Group

Optional

Location

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

RadSec Connection Status: Not Connected

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

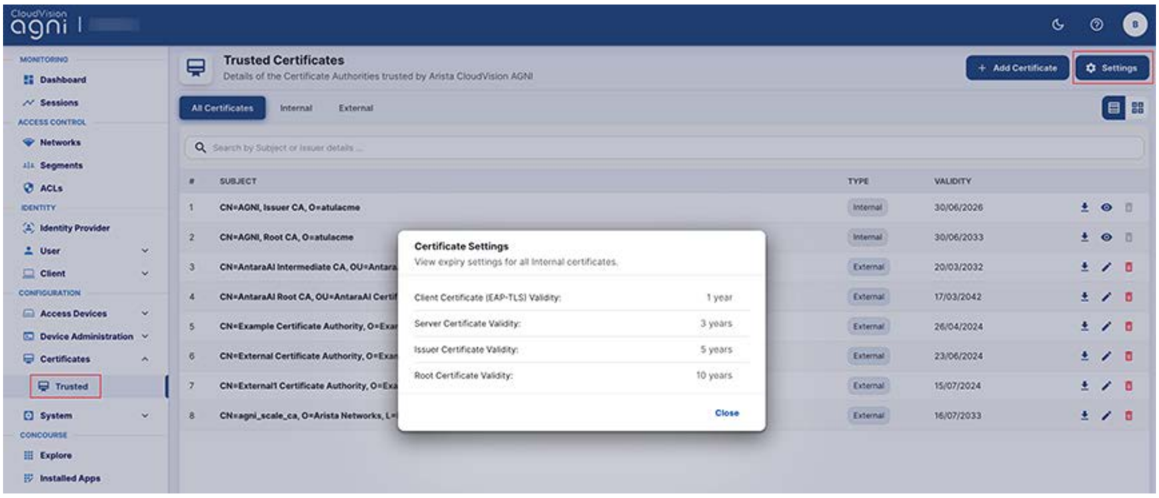
RadSec Connection Logs

Figure: Device Details

Viewing the Certificates

The native Public Key Infrastructure (PKI) built into the product enables the life cycle management of client certificates issued through its services.

The Trusted Certificates section in AGNI displays the Root and Issuer CAs of built-in PKI. You can download the certificate by navigating to **Configuration → Certificates → Trusted**. Then, click on **Settings** to view the details of AGNI certificates.



Trusted Certificates

Details of the Certificate Authorities trusted by Arista CloudVision AGNI

#	SUBJECT	TYPE	VALIDITY
1	CN=AGNI, Issuer CA, O=atulacme	Internal	30/06/2026
2	CN=AGNI, Root CA, O=atulacme	Internal	30/06/2033
3	CN=AntaraAI Intermediate CA, OU=Antara	External	20/03/2032
4	CN=AntaraAI Root CA, OU=AntaraAI Certif	External	17/03/2042
5	CN=Example Certificate Authority, O=Exar	External	26/04/2024
6	CN=External Certificate Authority, O=Exar	External	23/06/2024
7	CN=External1 Certificate Authority, O=Exa	External	15/07/2024
8	CN=agni_scale_ca, O=Arista Networks, L=	External	16/07/2033

Certificate Settings

View expiry settings for all internal certificates.

Client Certificate (EAP-TLS) Validity: 1 year

Server Certificate Validity: 3 years

Issuer Certificate Validity: 5 years

Root Certificate Validity: 10 years

Figure: Trusted Certificates

You can import external certificates into AGNI by clicking the **+Add Certificate** on the top right of the page. Importing the external *root*, *intermediate*, and *issuer certificates* enables AGNI to work with external PKIs.

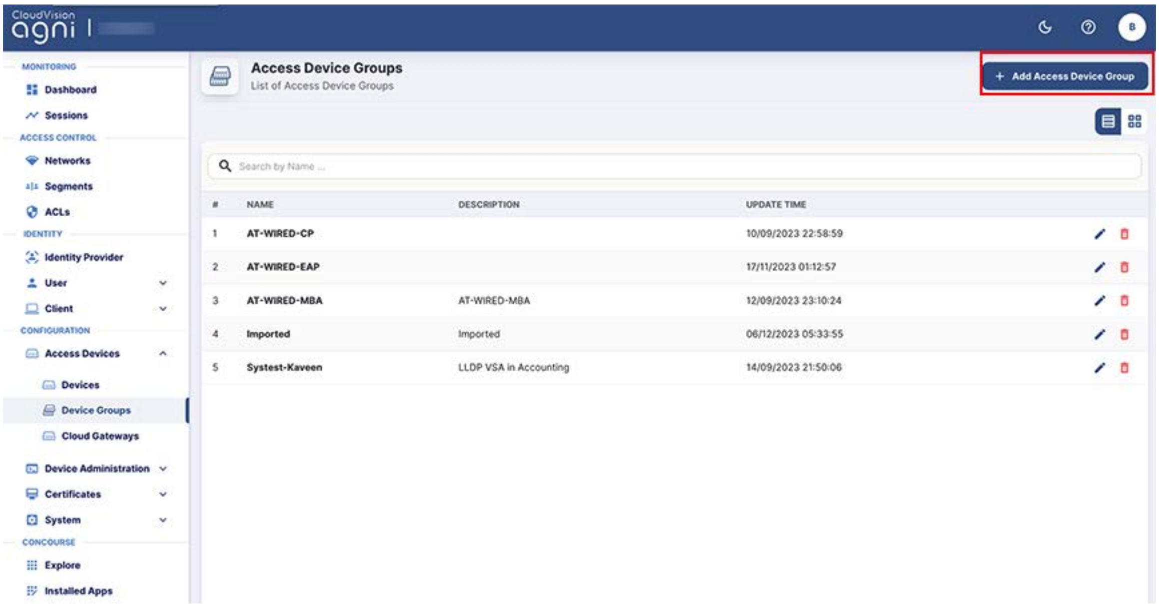
For external PKIs, the system supports certificate revocation checks either by querying the URL or statically checking against the revocation list.

Configuring Device Groups

You can configure Device Groups using the AGNI portal. Device Groups can be set up with one or more network devices for ease of management and policy administration. After setting up, the Device Groups are then available in the Segment conditions to enforce network access policies.

To add a Device Group:

1. Navigate to **Configuration** -> **Access Devices** -> **Device Groups**
2. Click + **Add Access Device Group** (see image below)



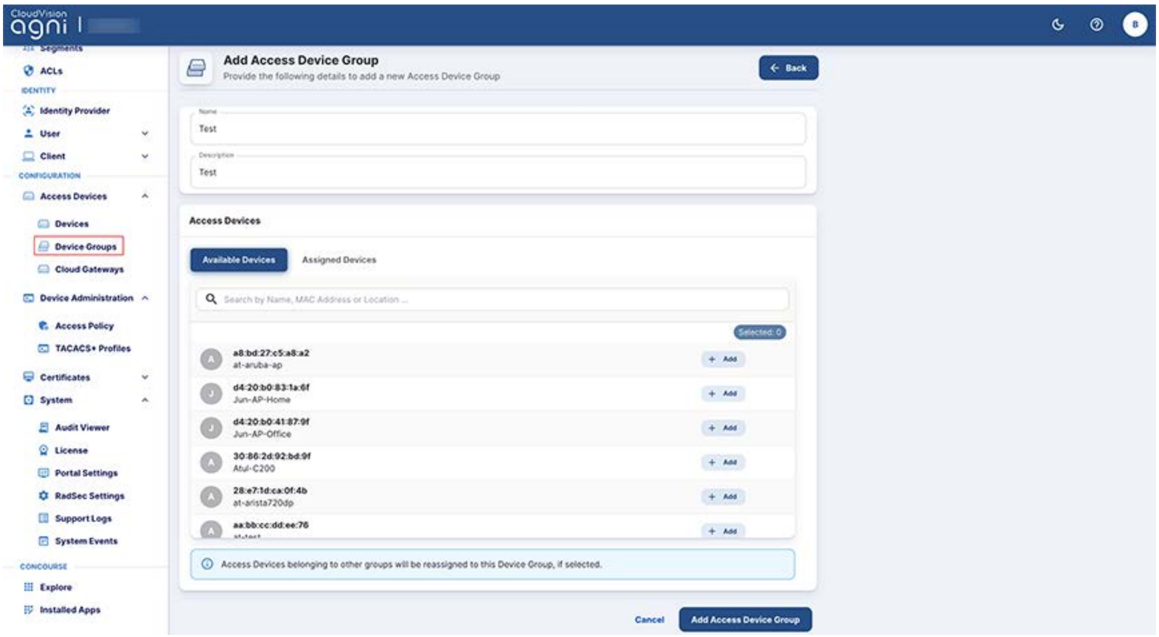
Access Device Groups

List of Access Device Groups

#	NAME	DESCRIPTION	UPDATE TIME
1	AT-WIRED-CP		10/09/2023 22:58:59
2	AT-WIRED-EAP		17/11/2023 01:12:57
3	AT-WIRED-MBA	AT-WIRED-MBA	12/09/2023 23:10:24
4	Imported	Imported	06/12/2023 05:33:55
5	Systest-Kaveen	LLDP VSA in Accounting	14/09/2023 21:50:06

Figure: Access Device Groups

3. On the Add Access Device Group page, enter a device name and click **Add Access Device Group** button. The device gets added to the Available Devices list (see image below).
   You can also add the devices from the Available Devices tab.



Add Access Device Group

Provide the following details to add a new Access Device Group

Name: Test

Description: Test

Access Devices

a8:bd:27:c5:a8:a2
at-aruba-ap

d4:20:b0:83:1a:6f
Jun-AP-Home

d4:20:b0:41:87:9f
Jun-AP-Office

30:86:2d:92:bd:9f
Atul-C200

28:e7:1d:ca:0f:4b
at-arista720dp

aa:bb:cc:dd:ee:76
at-test

Access Devices belonging to other groups will be reassigned to this Device Group, if selected.

Figure: Adding Access Device Groups

Configuring Identity Providers (IDPs)

AGNI interacts with IDPs through OIDC and OAuth2.0 protocols. AGNI supports the following IDPs:

- Microsoft 365 (Azure)
- Google Workspace
- OneLogin
- Okta
- Local

The AGNI integration with IDPs requires:

- Authentication of:
  - User onboarding workflows to onboard the client devices through UPSK, EAP-TLS, and Captive Portal
  - Admin login to the user interface
  - Admin login to the UPSK client portal
  - User login to the UPSK client portal
- Authorization - To gather user authorization attributes such as groups, account status, and user attributes from the identity providers.
  Authorization is an optional process and the IDP configuration for authorization is required only when the network access policies providing access to the users are based on the user authorization attributes.

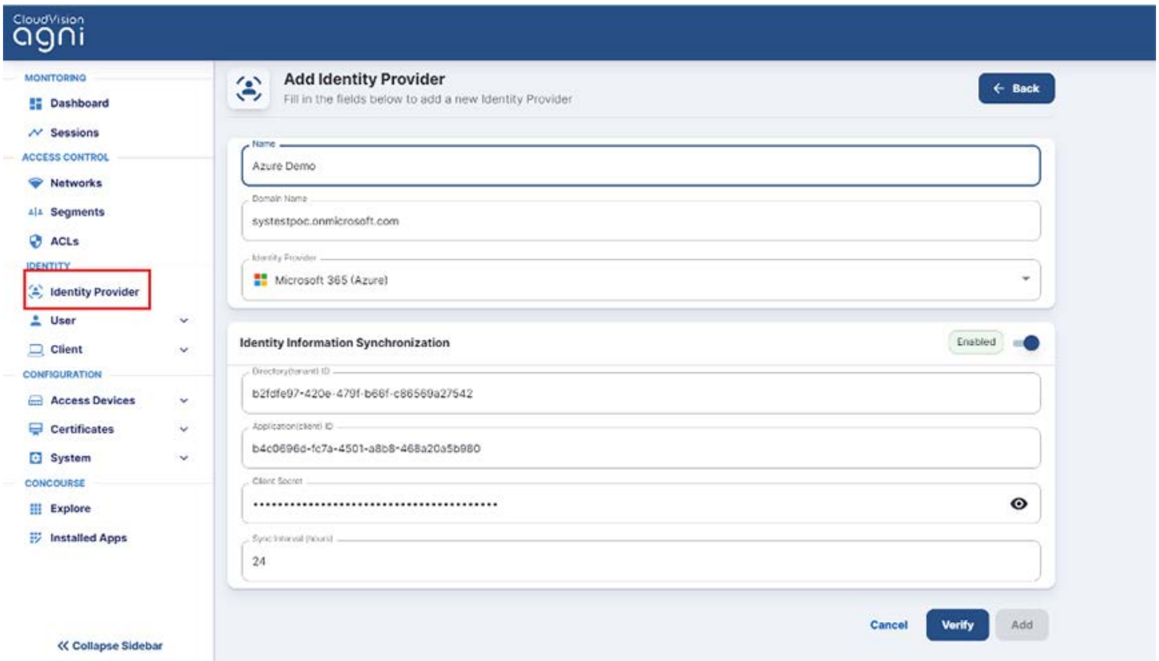
Microsoft 365 (Azure)

For authentication, AGNI uses the application endpoint registered with Microsoft Azure AD that handles all the authentication requirements. You do not have to make any other configuration changes to perform authentication.

About authorization, you can skip the below steps, if you are not performing any user authorization or if you are not using any of the identity provider attributes in network policies.

If you provide user authorization, follow the below steps:

1. Navigate to **Identity → Identity Provider.**
2. Click the **Edit** or **Add** button to edit an existing IDP or to add a new IDP.
3. Enter a name and Domain name in the respective fields.
4. Enable **Identity information Synchronization.**
5. Provide the identity provider details (Refer to Appendix section on how to configure the details in Microsoft Azure AD)
   a. Directory (tenant) ID
   b. Application (client) ID
   c. Client Secret
   d. Synch Interval (hours)
6. Click the **Verify** button. Once the operation is successful, the system fetches the list of groups from the IDP, which can be used in the policy creation.



Add Identity Provider

Fill in the fields below to add a new Identity Provider

Name: Azure Demo

Domain Name: systestpoc.onmicrosoft.com

Identity Provider: Microsoft 365 (Azure)

Identity Information Synchronization: Enabled

Directory(tenant) ID: b2fdfe97-420e-479f-b66f-c86569a27542

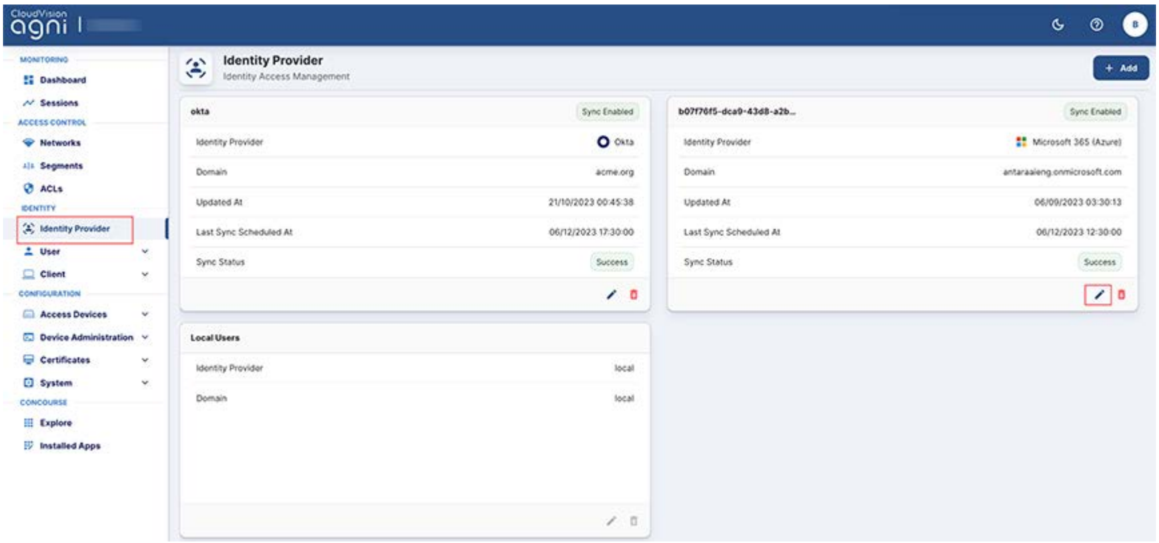
Application(client) ID: b4c0696d-fc7a-4501-a8b8-468a20a5b980

Client Secret: ••

Sync Interval (hours): 24

Figure: Adding Identity Provider

7. On the Identity Provider page, click the update icon (see image below).



Identity Provider

Identity Access Management

okta	Sync Enabled
Identity Provider	Okta
Domain	acme.org
Updated At	21/10/2023 00:45:38
Last Sync Scheduled At	06/12/2023 17:30:00
Sync Status	Success

b07f76f5-dca9-43d8-a2b...	Sync Enabled
Identity Provider	Microsoft 365 (Azure)
Domain	antaraaieng.onmicrosoft.com
Updated At	06/09/2023 03:30:13
Last Sync Scheduled At	06/12/2023 12:30:00
Sync Status	Success

Local Users	
Identity Provider	local
Domain	local

Figure: Edit or Update Identity Provider

8. Select the groups from the Available Groups (see image below). The selected groups are visible in the Synchronized Groups tab and can be used in the network access policies.

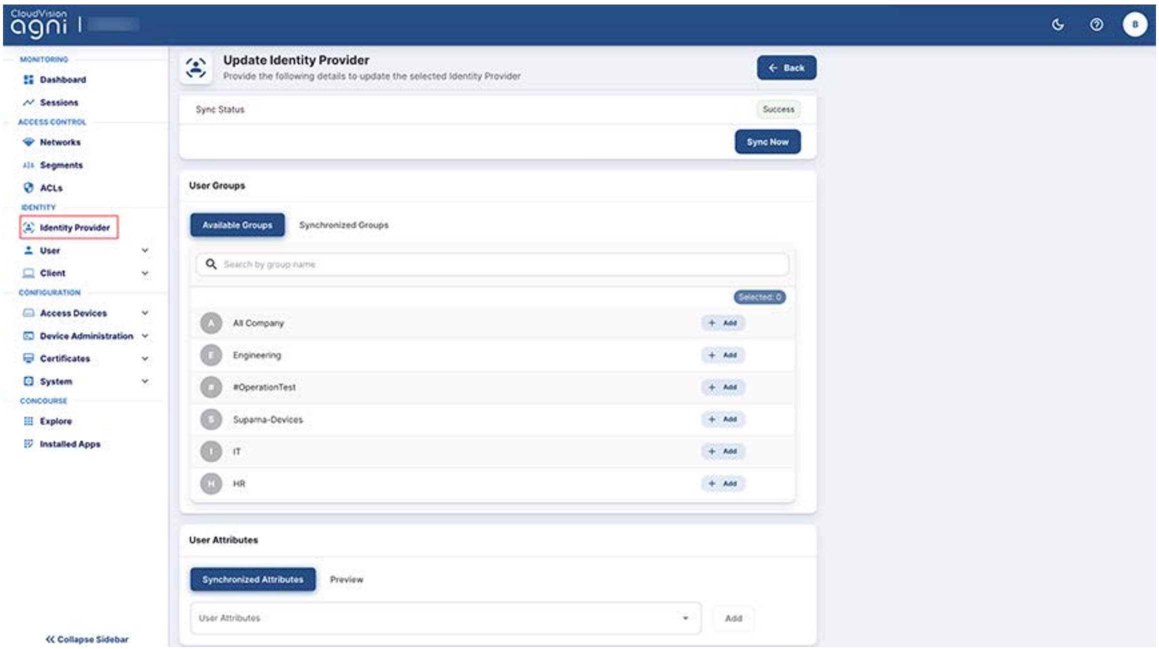


Figure: Identity Provider Available Groups

9. Click on the **Add** button to save the changes.

The details include:

- **Sync Interval** - This parameter dictates when the system must synchronize user attributes from the IDP. To perform an on-demand synchronization, click on the **Sync now** button. Alternatively, the system synchronizes once every Sync Interval duration that was specified.
- **User Attributes** - These are additional attributes that can be added to the IDP. The synchronization operation fetches the additional attributes specified and can be used in the segmentation policies.

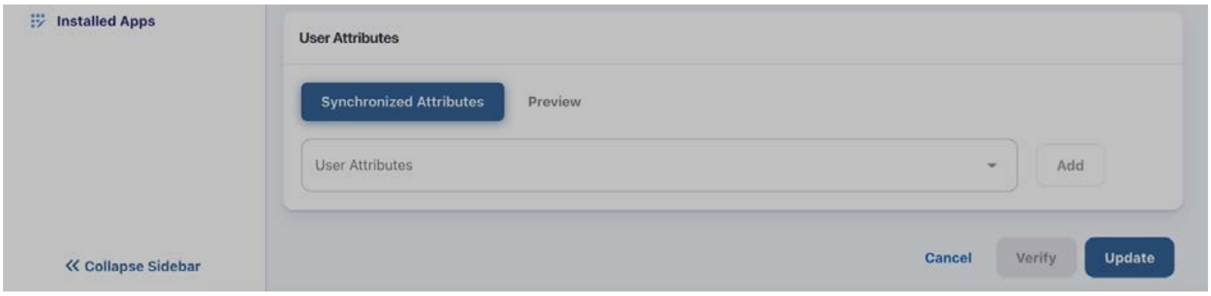
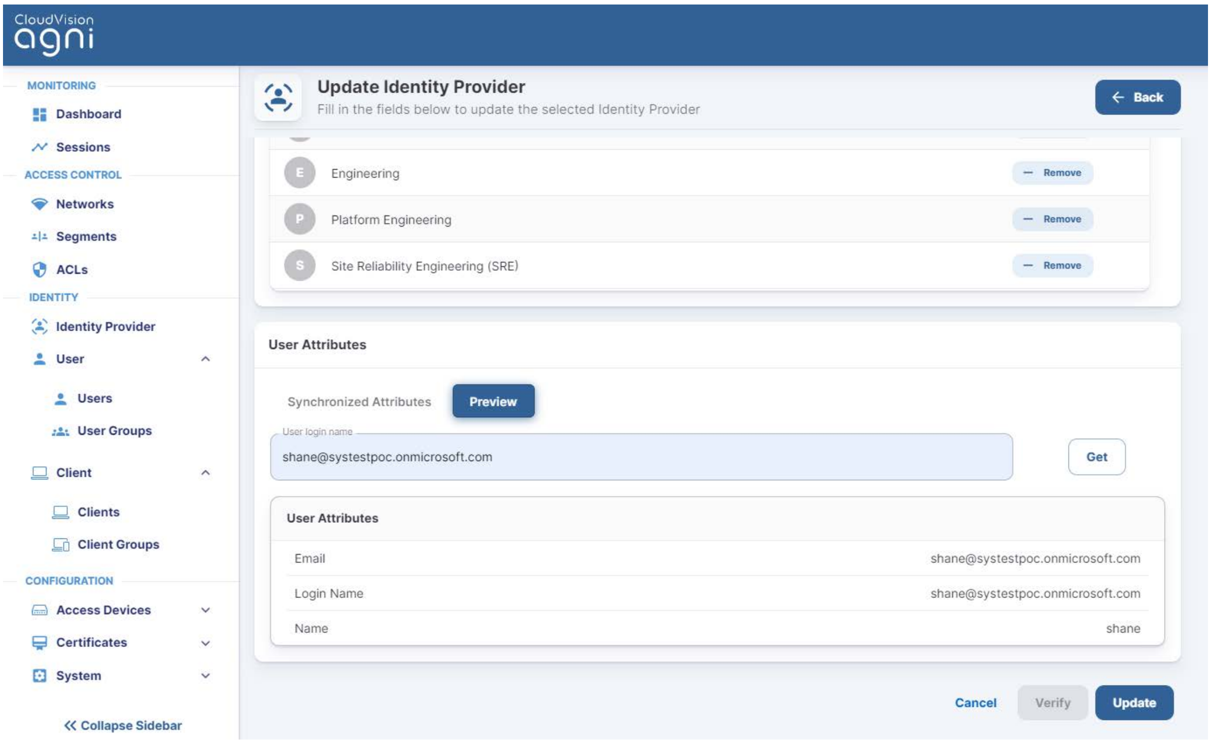


Figure: Identity Provider and User Attributes

- **Preview** – In the preview section, you can view the user and user attributes. This enables the ability to visualize user attributes from the IDP and use them in the segmentation policies.



Update Identity Provider

Fill in the fields below to update the selected Identity Provider

- E Engineering
- P Platform Engineering
- S Site Reliability Engineering (SRE)

User Attributes

User login name: shane@systestpoc.onmicrosoft.com

User Attributes	
Email	shane@systestpoc.onmicrosoft.com
Login Name	shane@systestpoc.onmicrosoft.com
Name	shane

Figure: Identity Provider and User Preview

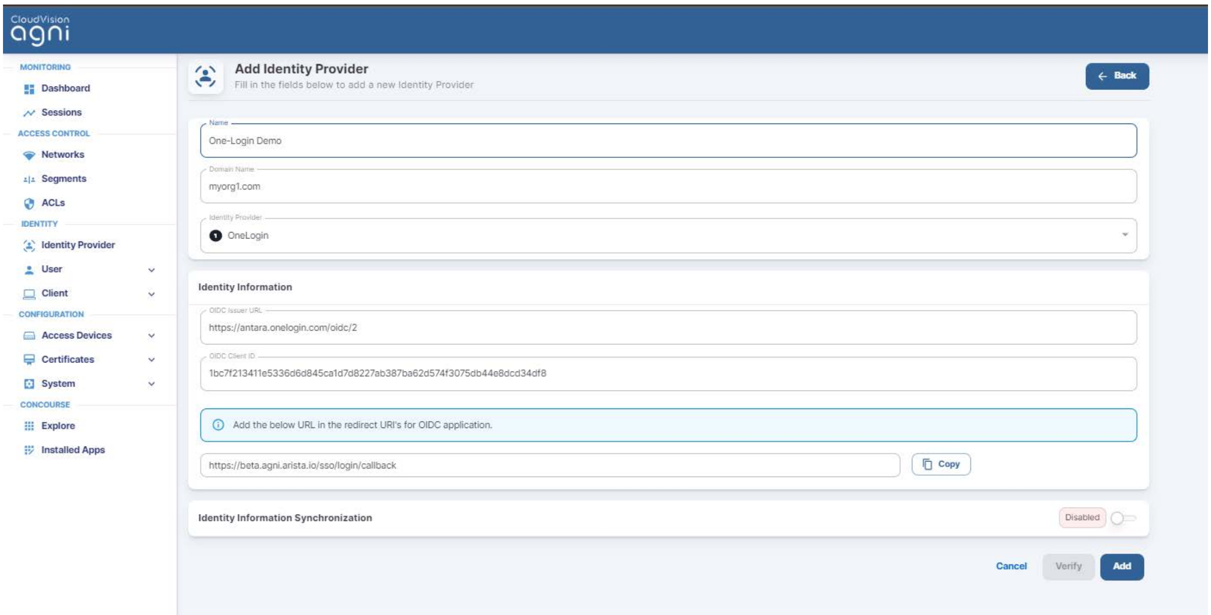
OneLogin

For Authentication, AGNI uses the OIDC protocol to authenticate the users into the IDP. You can set up OneLogin with an OIDC application and *save the Client ID and Issuer URL* for later use.

Authorization is performed by setting up API access under the Developers section in OneLogin administration. Create new API credentials in OneLogin for AGNI that have read permission for user fields, roles, and groups. Once set up, save the Client ID and Client Secret for later use.

Enter these values in AGNI by adding a new Identity Provider for OneLogin.

- Navigate to **Identity** → **Identity Provider**
- Click **Edit Identity Provider** (or **Add a new identity provider**)
- Enter the details for:
  - **Name** - Name of the identity provider
  - **Domain Name** - Domain name of the organization
- Provide details for - Identity Information. These details are used for authentication and can be found as described in the authentication section above.
  - **OIDC Issuer URL**
  - **OIDC Client ID**



Add Identity Provider

Fill in the fields below to add a new Identity Provider

Name: One-Login Demo

Domain Name: myorg1.com

Identity Provider: OneLogin

Identity Information

OIDC Issuer URL: https://antara.onelogin.com/oidc/2

OIDC Client ID: 1bc7f213411e5336d6d845ca1d7d8227ab387ba62d574f3075db44e8dcd34df8

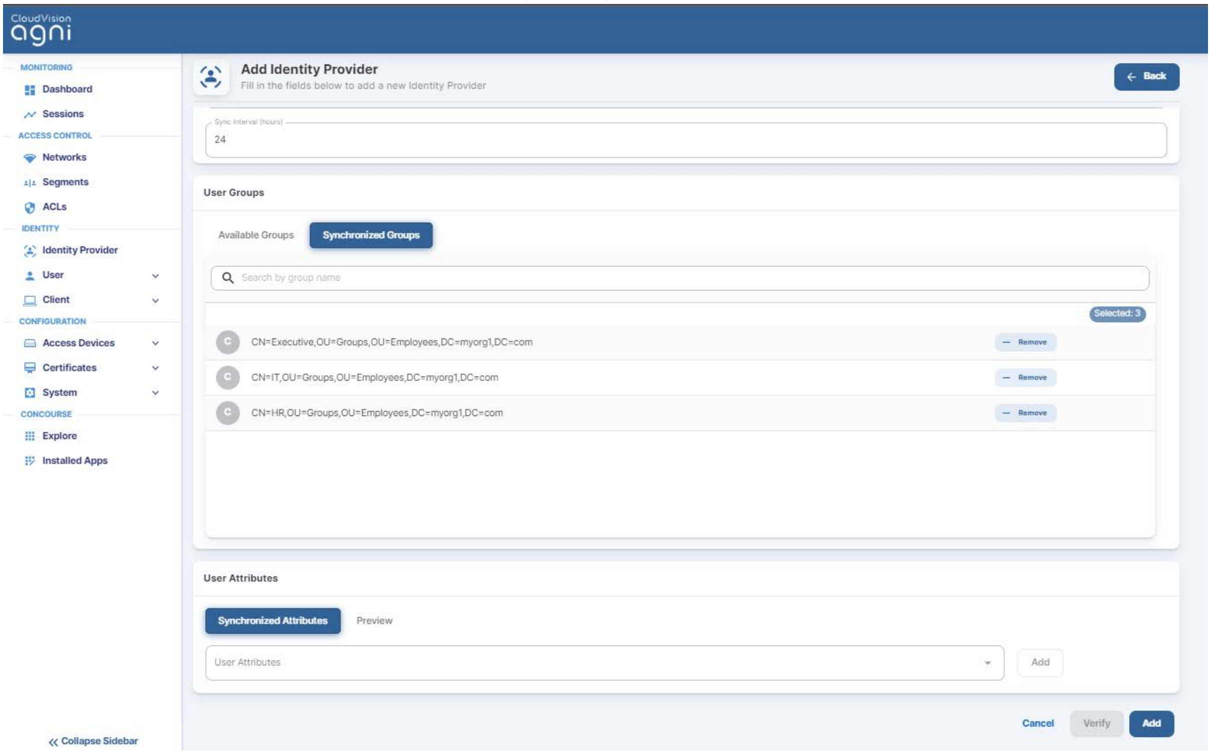
Add the below URL in the redirect URI's for OIDC application.

https://beta.agni.arista.io/sso/login/callback

Identity Information Synchronization

Figure: OneLogin and Identity Provider

- **Enable** Identity information Synchronization
- Provide the Identity Information Synchronization details (Refer to Appendix section on how to configure the details in OneLogin or the vendor documentation)
  - **API Client ID**
  - **API Client Secret**
- Click on the **Verify** button. Once the operation is successful, you can add the group information as it appears in OneLogin and use it in the authorization policies.
- Click on the **Add** or **Update** section to save the identity provider configuration.
- The details of **Sync Interval**, **User Attributes**, and **Preview** functions are similar to the IDP details in Microsoft 365 (Azure).



Add Identity Provider

Fill in the fields below to add a new Identity Provider

Sync Interval (hours): 24

User Groups

CN=Executive,OU=Groups,OU=Employees,DC=myorg1,DC=com

CN=IT,OU=Groups,OU=Employees,DC=myorg1,DC=com

CN=HR,OU=Groups,OU=Employees,DC=myorg1,DC=com

User Attributes

Figure: OneLogin Identity Provider Synchronization

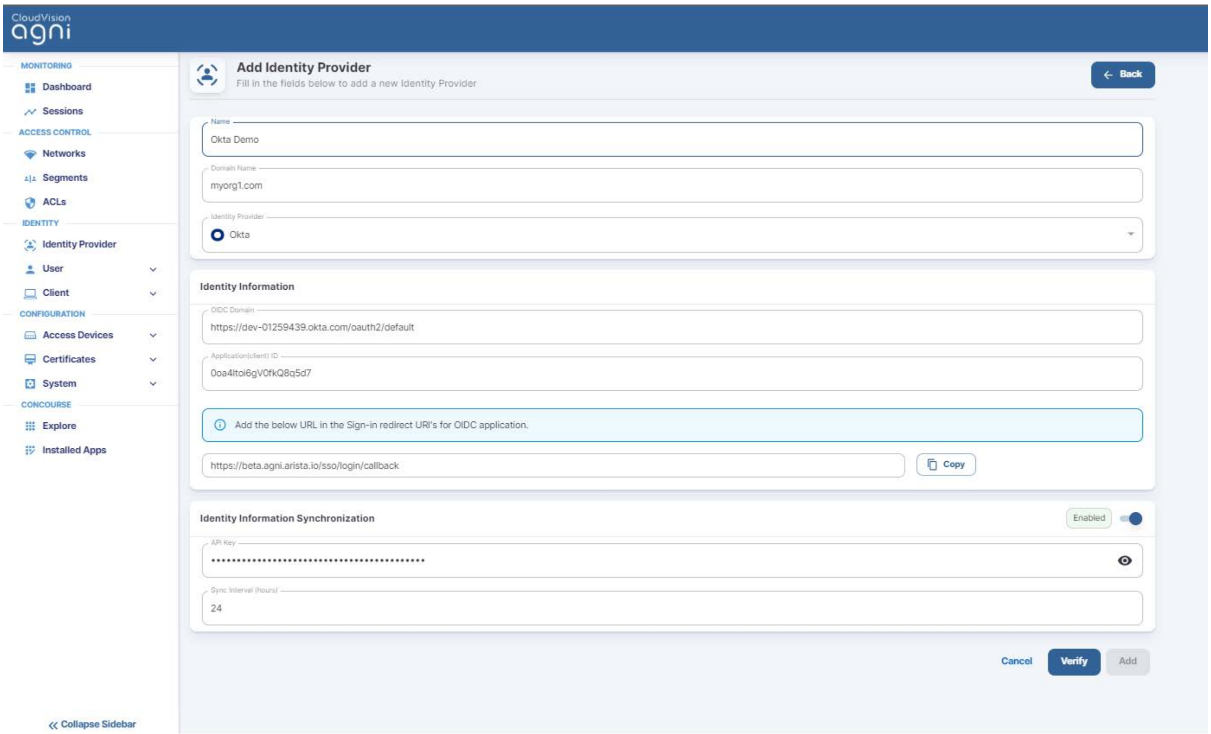
Okta

For authentication, AGNI uses OIDC protocol to authenticate the users into the IDP. You can set up Okta with an OIDC application and save the *Client ID and Issuer URL* for later use.

Authorization is performed through setting up API access under the Security section in Okta administration. Create a new **API Token** in Okta for AGNI.

Enter these values in AGNI by adding a new Identity Provider for Okta:

- Navigate to **Identity** → **Identity Provider**
- **Edit Identity Provider** (or **Add a new identity provider**)
- Provide the details for :
    - **Name** - Name of the identity provider
    - **Domain Name** - Domain name of the organization
- Provide details for - Identity Information. The details are used for authentication and is described in the authentication section above.
    - **OIDC Domain**
    - **Application (client) Client ID**



Add Identity Provider

Fill in the fields below to add a new Identity Provider

Name: Okta Demo

Domain Name: myorg1.com

Identity Provider: Okta

Identity Information

OIDC Domain: https://dev-01259439.okta.com/oauth2/default

Application(client) ID: 0oa4ltoi6gV0fkQ8q5d7

Add the below URL in the Sign-in redirect URI's for OIDC application.

https://beta.agni.arista.io/sso/login/callback

Identity Information Synchronization: Enabled

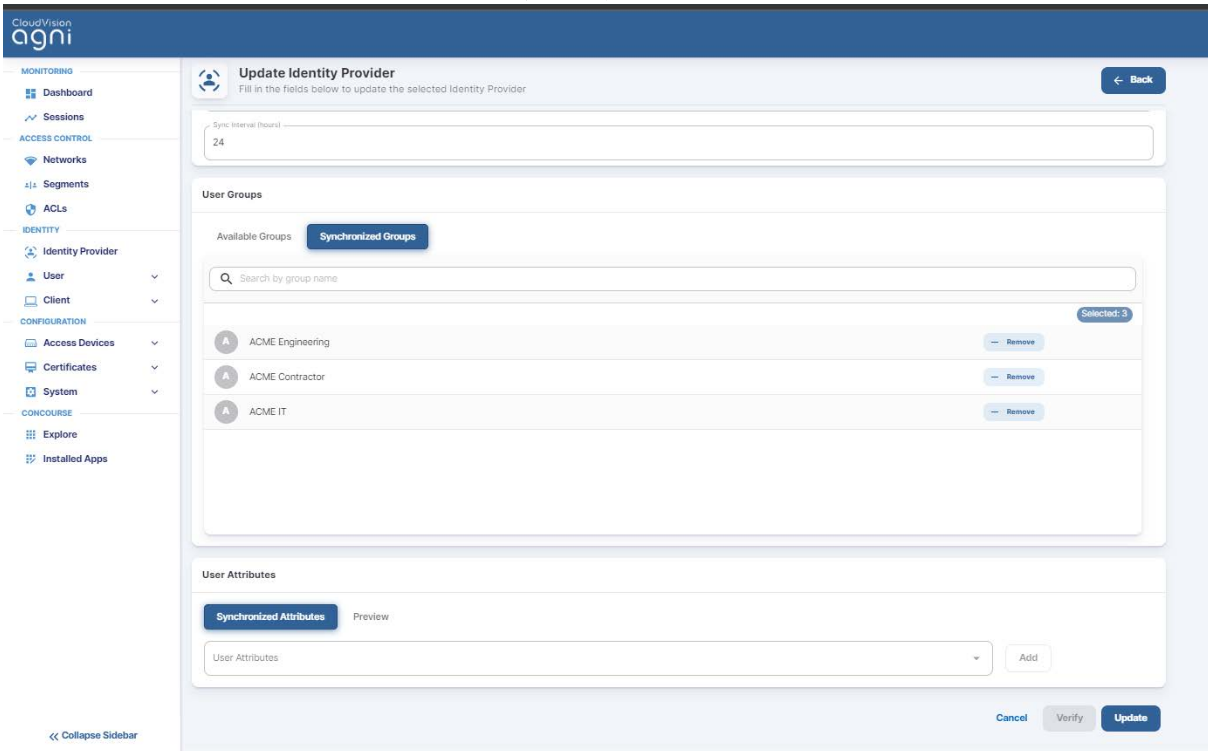
API Key: ••

Sync Interval (hours): 24

Figure: Okta Identity Provider Configuration

- **Enable** Identity information Synchronization.
- Provide the Identity Information Synchronization details (Refer to the Appendix section on how to configure the details in Okta or the vendor documentation)
    - **API Key**
- Click on the **Verify** button. Once the operation is successful, you can add the group information as it appears in Okta and use it in the authorization policies.
- Click on the **Add** or **Update** section to save the identity provider configuration.

- The details of **Sync Interval**, **User Attributes**, and **Preview** functions are similar to the IDP details in Microsoft 365 (Azure).



Update Identity Provider

Fill in the fields below to update the selected Identity Provider

Sync Interval (hours): 24

User Groups

Selected: 3

Synchronized Groups
ACME Engineering
ACME Contractor
ACME IT

User Attributes

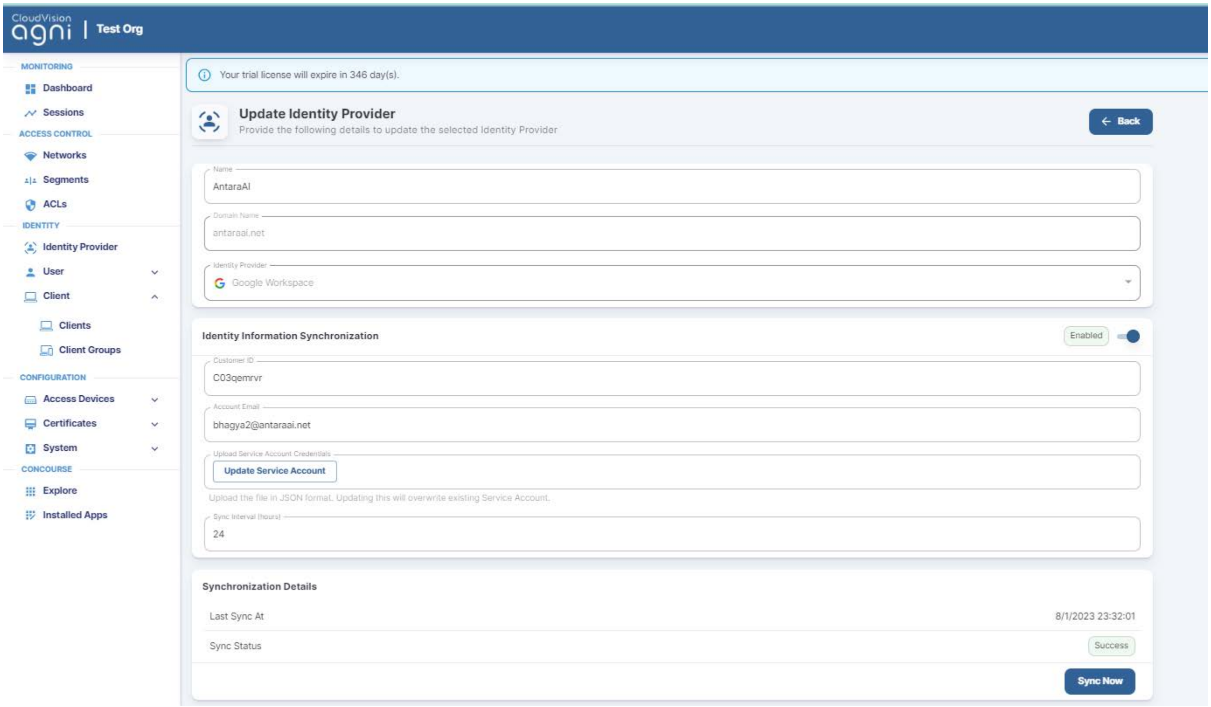
Figure: Okta Identity Provider Synchronization

Google Workspace

For Authentication, AGNI uses OAuth protocol to authenticate the users into the IDP. Authorization is performed by setting up API access under the Security section in Google Workspace administration. Create a new API JSON in Google Workspace for AGNI.

Enter these values in AGNI by adding a new Identity Provider for Google Workspace:

- Navigate to **Identity → Identity Provider**
- **Edit Identity Provider** (or **Add a new identity provider**)
- Provide the details for:
  - **Name** - Name of the identity provider
  - **Domain Name** - Domain name of the organization
- Provide details for - Identity Information.
- **Enable** Identity information Synchronization
- Provide the Identity Information Synchronization details
  - **Customer ID**
  - **Account Email**
  - **Upload Service Account credentials**
- Click on the **Verify** button. Once the operation is successful, you can add the group information as it appears in Google Workspace and use it in the authorization policies.
- Click on the **Add** or **Update** section to save the identity provider configuration.
- The details of Sync Interval, User Attributes, and Preview functions are similar to the IDP details in Microsoft 365 (Azure).



Your trial license will expire in 346 day(s).

Update Identity Provider

Provide the following details to update the selected Identity Provider

Name: AntaraAI

Domain Name: antaraai.net

Identity Provider: Google Workspace

Identity Information Synchronization: Enabled

Customer ID: C03qemrvr

Account Email: bhagya2@antaraai.net

Upload Service Account Credentials

Upload the file in JSON format. Updating this will overwrite existing Service Account.

Sync Interval (hours): 24

Synchronization Details

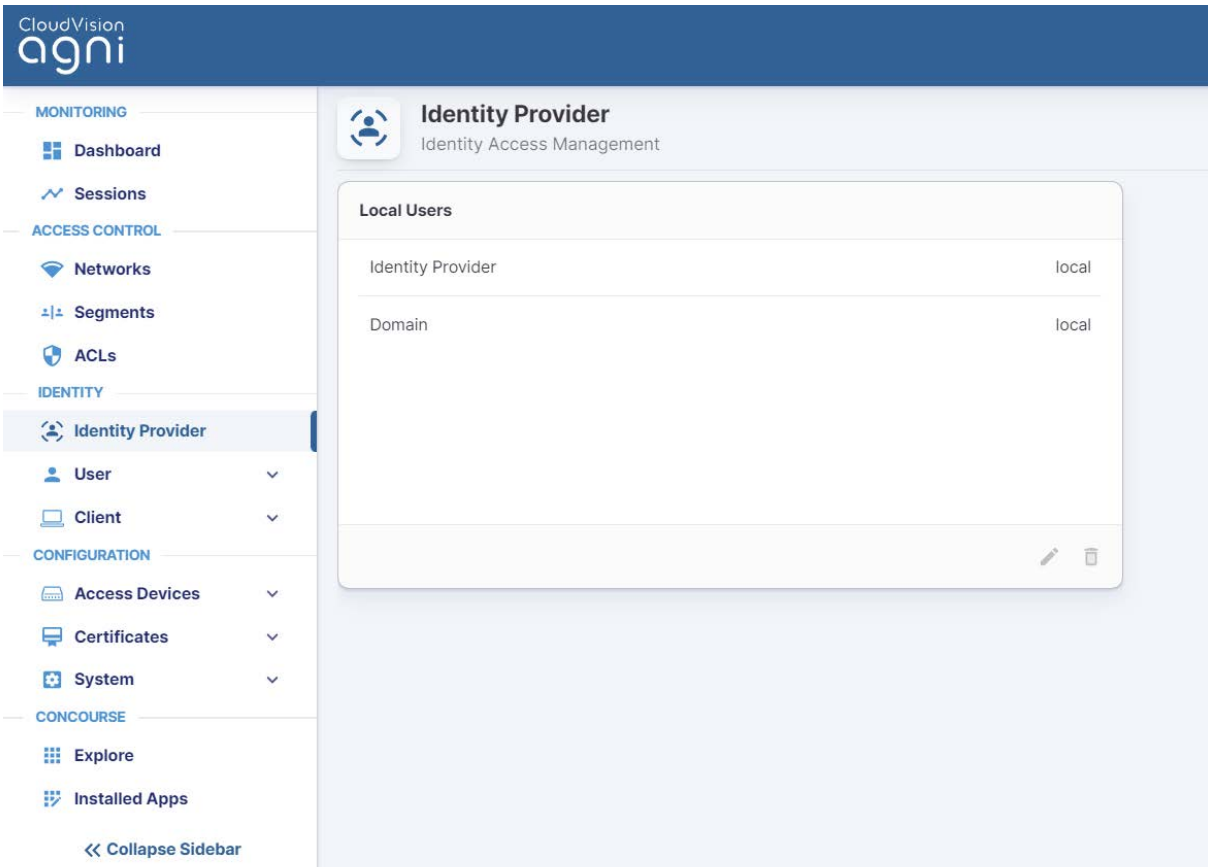
Last Sync At: 8/1/2023 23:32:01

Sync Status: Success

Figure: Google Workspace

Local

AGNI also supports the local identity provider. This enables the addition of local users into the system and validation of the product feature set. The local identity provider is enabled by default.



Local Users

Identity Provider	local
Domain	local

Figure: Local IDP Configurations

Networks

Networks represent the entry point for network access control. The Networks represent different ways a client can connect to your network environment. Various Network options are available based on the authentication needs.

802.1X

You can set up 802.1X Networks to provide AAA access to the clients with the highest level of security using EAP-TLS. AGNI supports EAP-TLS authentications from the clients using its native PKI or through the external PKI.

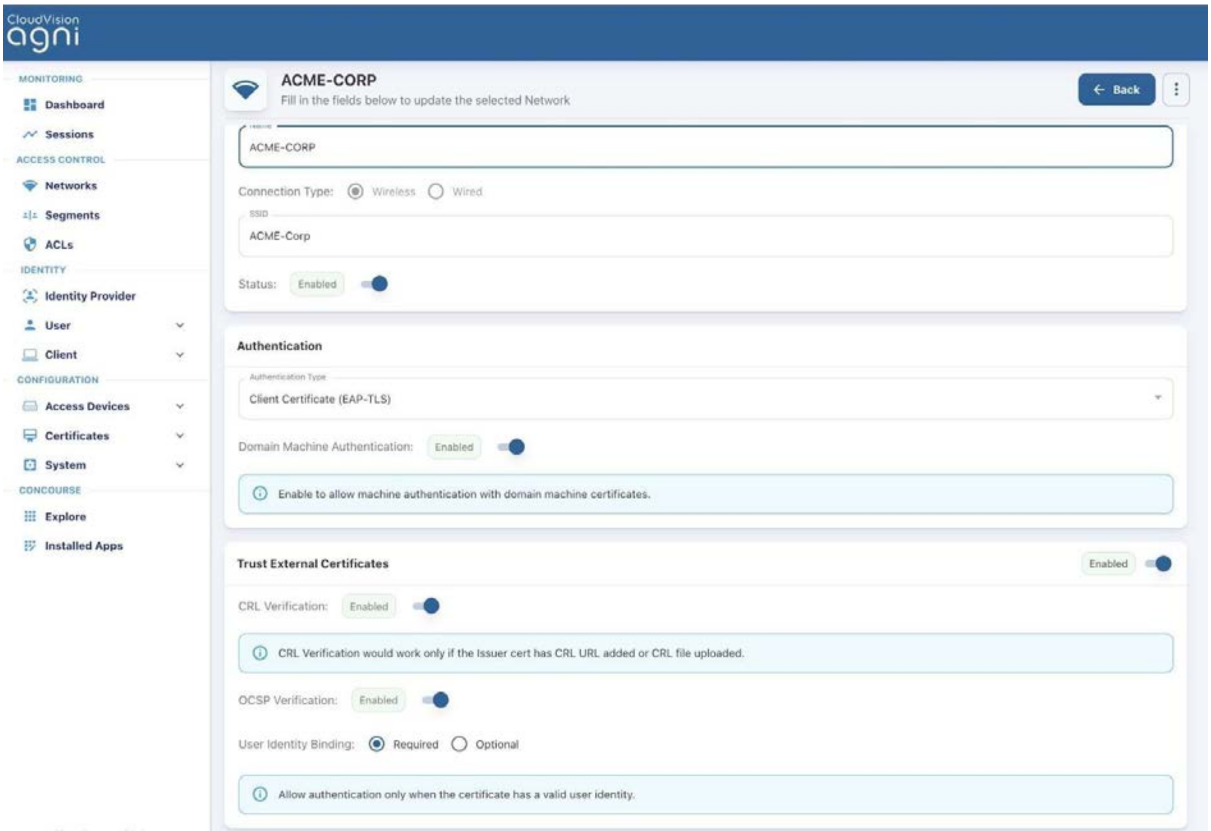
Prerequisites

- Wireless SSID should be configured on the APs to perform 802.1X authentication.
- Clients are onboarded with credentials and configured to perform 802.1X authentication either using native PKI or external PKI.
- For external PKIs, the PKI **root** and **issuer certificates** are imported into AGNI.

Configuring the Networks

To configure Networks:

1. Navigate to **Access Control → Networks**. Click on **Add Network**.



ACME-CORP

Fill in the fields below to update the selected Network

Name: ACME-CORP

Connection Type: ● Wireless ○ Wired

SSID: ACME-Corp

Status: Enabled

Authentication

Authentication Type: Client Certificate (EAP-TLS)

Domain Machine Authentication: Enabled

Enable to allow machine authentication with domain machine certificates.

Trust External Certificates: Enabled

CRL Verification: Enabled

CRL Verification would work only if the Issuer cert has CRL URL added or CRL file uploaded.

OCSP Verification: Enabled

User Identity Binding: ● Required ○ Optional

Allow authentication only when the certificate has a valid user identity.

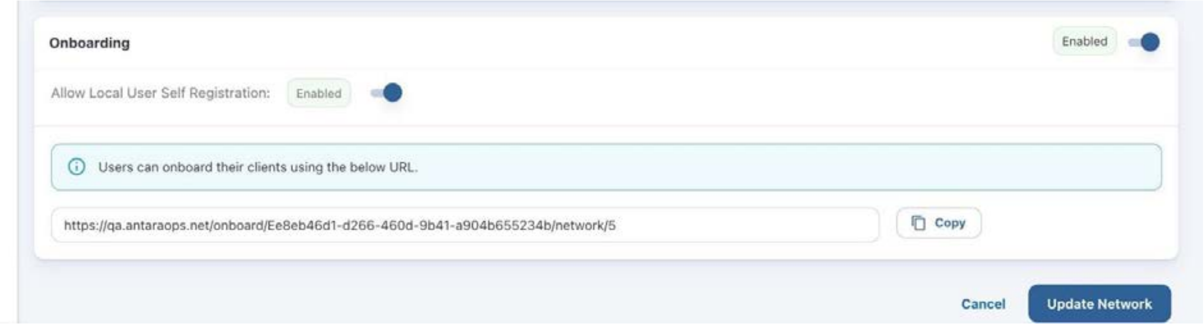
Figure: Wireless EAP-TLS Network

2. Enter the **Network Name** and choose **ConnectionType** as **Wireless**
3. Enter the **SSID** name. Ensure that the name matches the SSID configured in wireless APs.
4. **Status**
   a. **Enabled** - Enables this network to honor incoming requests.
   b. **Disabled** - Disables this network.
5. **Authentication** - Set the Type of authentication to the **Client Certificate**. This enables the system to honor EAP-TLS authentication requests.
6. **Domain Machine Authentication** - Enable this setting to process the domain machine authentication (via EAP-TLS) requests.
7. **Trusted External Certificates**

    a. If external PKI is being used and if you require AGNI to honor the external certificates, enable the setting with an option to check against **CRL** and **OCSP URLs** for certificate revocations.
    b. The setting assumes external PKI root and issuer certificates are imported into AGNI.
    c. User Identity Binding
        i. **Required** - When set, the certificate has a valid query-able user identity for request authorizations.
        ii. **Optional** - When set, the certificate contains any identity that is optionally bound or not bound to the user. For example, this option can be set to honor appliance authentication where the certificates are not bound to any user but set to machine identity.

8. Onboarding
    a. **Enable** this setting if using AGNI PKI
    b. Allow Local User Self Registration:
        i. **Disabled** - Disallows local users to self-register into the system as part of the user onboarding process.
        ii. **Authorized User Group** - This setting is optional. Choose the names of the User Groups, if you want to allow onboarding of the users belonging to these groups. When this setting is not provided the system honors onboarding requests from all the users of the organization.
        iii. Enabled - Users can self-register into the system as part of the user onboarding process.

9. Click on the **Add Network** button.
   This process creates the network. It also creates an **Onboarding URL**, which should be set as a captive portal URL in the WiFi configuration of your AP. Clients are redirected to this URL during the onboarding process.



Onboarding

Enabled

Allow Local User Self Registration: Enabled

Users can onboard their clients using the below URL.

https://qa.antaraops.net/onboard/Ee8eb46d1-d266-460d-9b41-a904b655234b/network/5

Figure: Wireless EAP-TLS Network User Onboarding

Network Settings

To manage the Network settings, you must configure UPSK Settings and EAP-TLS Settings as below.

Unique PSK (UPSK) Settings

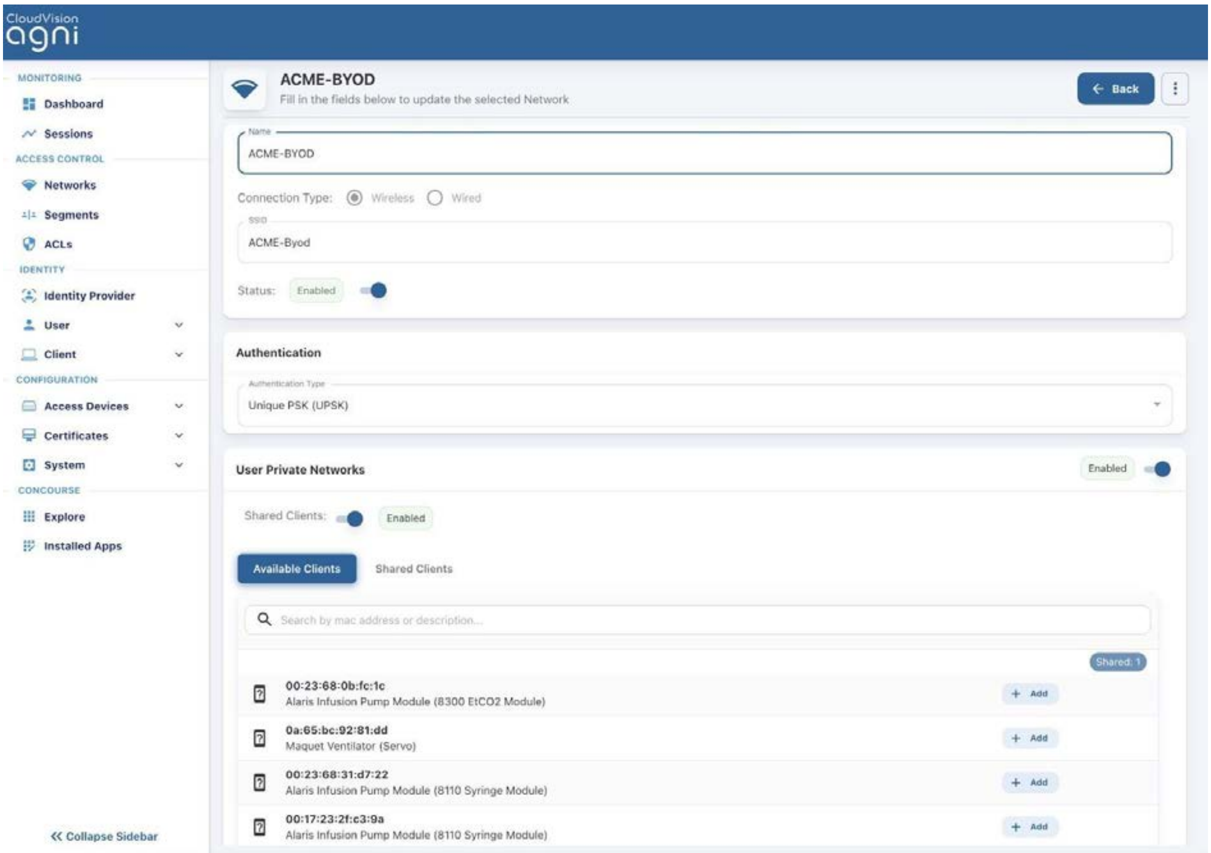
UPSK provides secure access to the network based on the unique PSK generated by the system. UPSKs are governed by the security principles that ensure that the passphrases are unique and secure. UPSKs can be generated by the end user through the user onboarding workflow or by administrators through the administration workflows. They can be generated on a per-device basis or per group of devices as required by the network.

Prerequisites

- Wireless SSID should be configured on the APs to perform UPSK authentication.
- Onboarding roles should be configured on the APs.
- Onboarding PSK passphrase should be configured on the SSID.
- Walled garden domain names are configured to allow access to the required domains (more details under the *Show Domains* section below).

Configuration

1. Navigate to **Access Control → Networks**. Click on the **Add Networks** button.



ACME-BYOD

Fill in the fields below to update the selected Network

Name: ACME-BYOD

Connection Type: ● Wireless ○ Wired

SSID: ACME-Byod

Status: Enabled

Authentication

Authentication Type: Unique PSK (UPSK)

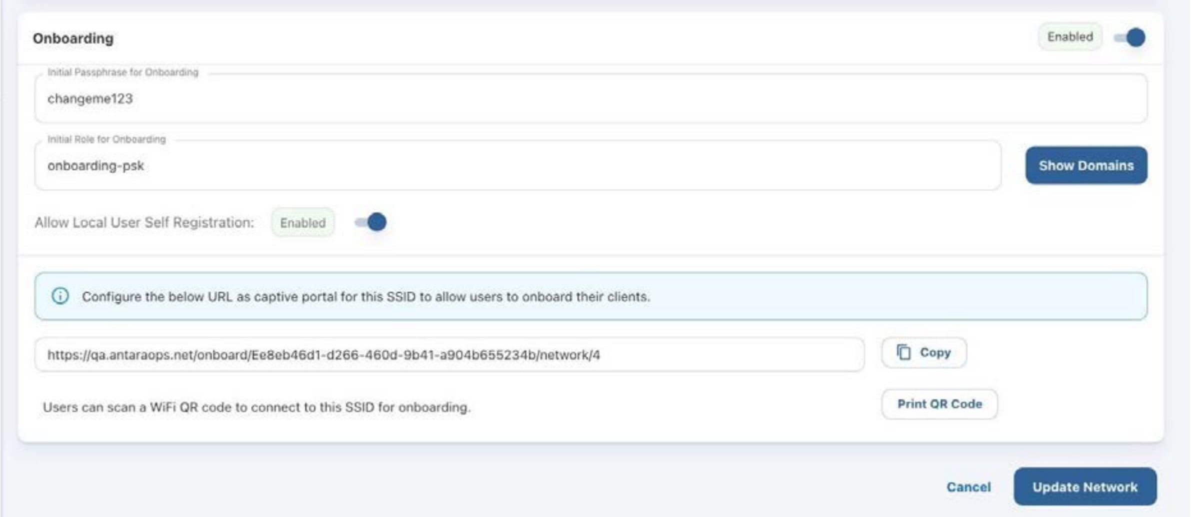
User Private Networks Enabled

Shared Clients: Enabled

00:23:68:0b:fc:1c Alaris Infusion Pump Module (8300 EtCO2 Module)	+ Add
0a:65:bc:92:81:dd Maquet Ventilator (Servo)	+ Add
00:23:68:31:d7:22 Alaris Infusion Pump Module (8110 Syringe Module)	+ Add
00:17:23:2f:c3:9a Alaris Infusion Pump Module (8110 Syringe Module)	+ Add

Figure: Wireless UPSK Network

2. Enter the **Network Name** and choose **ConnectionType** as **Wireless**.
3. Provide the **SSID** name. Ensure that the name matches the SSID configured in wireless APs.
4. **Status**:
    a. **Enabled** - Enables this network to honor incoming requests.
    b. **Disabled** - Disables this network.
5. **Authentication** – The type of authentication should be set to Unique PSK (UPSK). This enables the system to honor UPSK authentication requests.
6. **User Private Networks**:
    a. Enable this setting when interacting with Arista APs. This setting sends Arista VSAs for UPSK transactions.
    b. **Shared Clients** (Optional). Enable the setting and choose the list of clients this connection can share from the configuration. This is specific to Arista APs.
7. **Onboarding** - Enables the end user to self-register the devices.
    a. **Initial Passphrase for Onboarding** - Specify the initial passphrase that should be used by the clients to connect to the UPSK network. This passphrase should match with the one configured on the SSID of your APs.
    b. **Initial Role for Onboarding** - Specify the initial role to be associated with when the clients connect to the UPSK network. This role should be configured in the APs.
    c. **Show Domains** - Shows the list of walled garden domain names that need to be allow-listed in your network infrastructure (wired or wireless) to allow the onboarding process. Without this, the user authentication may be blocked by the network infrastructure.
    d. **Allow Local User Self Registration**:
        i. **Disabled** - Disallows local users to self-register into the system as part of the user onboarding process.
        ii. **Authorized User Group** - This setting is optional. Choose the names of the User Groups, if you want to allow onboarding to be permitted for the users belonging to these groups. When this setting is not provided the system honors onboarding requests from all the users of the organization.
        iii. **Enabled** - Users can self-register into the system as part of the user onboarding process.



Onboarding

Enabled

Initial Passphrase for Onboarding: changeme123

Initial Role for Onboarding: onboarding-psk

Allow Local User Self Registration: Enabled

Configure the below URL as captive portal for this SSID to allow users to onboard their clients.

https://qa.antaraops.net/onboard/Ee8eb46d1-d266-460d-9b41-a904b655234b/network/4

Users can scan a WiFi QR code to connect to this SSID for onboarding.

Figure: Wireless UPSK Network User Onboarding

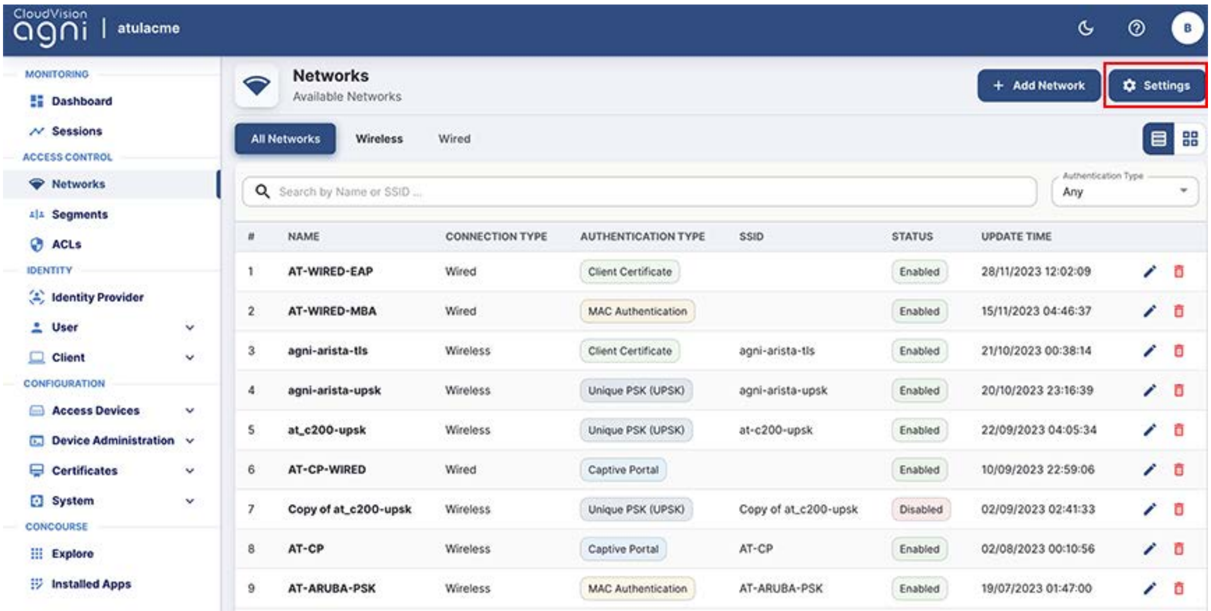
8. Click on the **Add Network** button. The process:
   - Creates the network
   - Creates an **Onboarding URL**, which should be set as a captive portal URL in the WiFi configuration of your AP. Clients are redirected to this URL for onboarding.
   - Creates a QR code that can be used to connect to the SSID and get redirected to the onboarding page as well.

Configuring the Device Count Limit for Authentication

This section describes the steps to configure the maximum device count limit for authentication using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) in AGNI.

To configure the EAP-TLS maximum count:

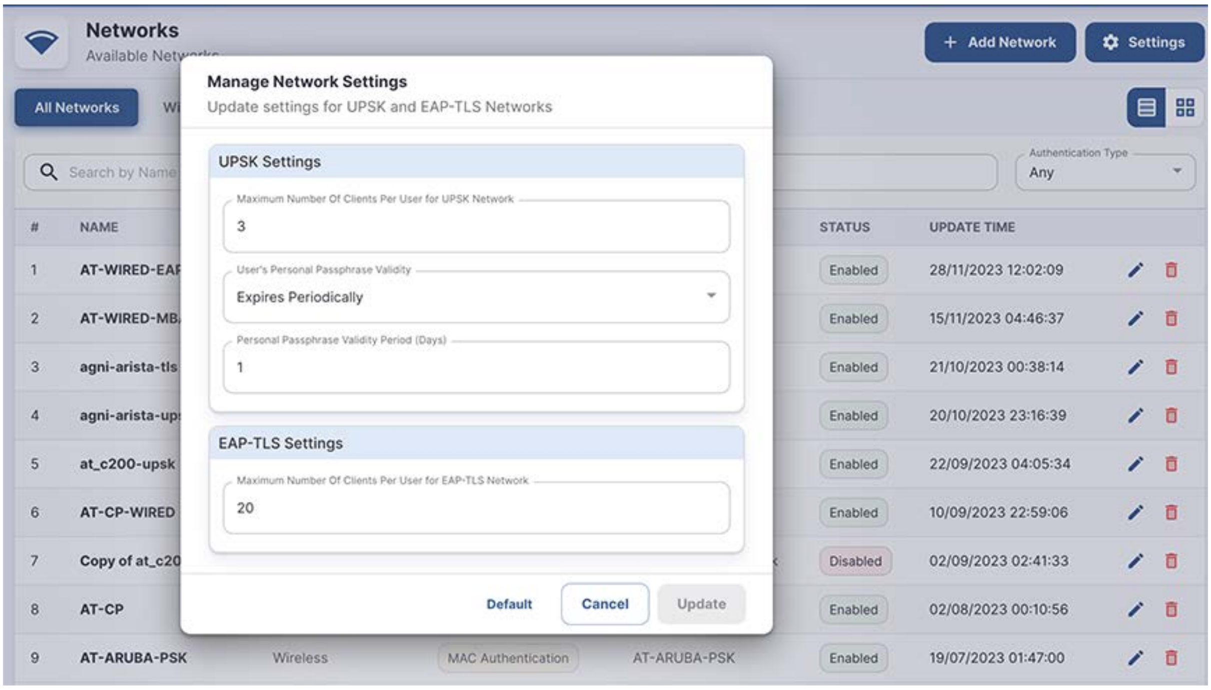
1. Log in to AGNI and navigate to **Access Control**-> **Networks**
2. Click **Settings** on the top right corner of the dashboard (see image below)



#	NAME	CONNECTION TYPE	AUTHENTICATION TYPE	SSID	STATUS	UPDATE TIME
1	AT-WIRED-EAP	Wired	Client Certificate		Enabled	28/11/2023 12:02:09
2	AT-WIRED-MBA	Wired	MAC Authentication		Enabled	15/11/2023 04:46:37
3	agni-arista-tls	Wireless	Client Certificate	agni-arista-tls	Enabled	21/10/2023 00:38:14
4	agni-arista-upsk	Wireless	Unique PSK (UPSK)	agni-arista-upsk	Enabled	20/10/2023 23:16:39
5	at_c200-upsk	Wireless	Unique PSK (UPSK)	at-c200-upsk	Enabled	22/09/2023 04:05:34
6	AT-CP-WIRED	Wired	Captive Portal		Enabled	10/09/2023 22:59:06
7	Copy of at_c200-upsk	Wireless	Unique PSK (UPSK)	Copy of at_c200-upsk	Disabled	02/09/2023 02:41:33
8	AT-CP	Wireless	Captive Portal	AT-CP	Enabled	02/08/2023 00:10:56
9	AT-ARUBA-PSK	Wireless	MAC Authentication	AT-ARUBA-PSK	Enabled	19/07/2023 01:47:00

Figure:Networks Page

The *Manage Network Settings* window is displayed as a pop-up screen.



Manage Network Settings
Update settings for UPSK and EAP-TLS Networks

UPSK Settings

Maximum Number Of Clients Per User for UPSK Network: 3

User's Personal Passphrase Validity: Expires Periodically

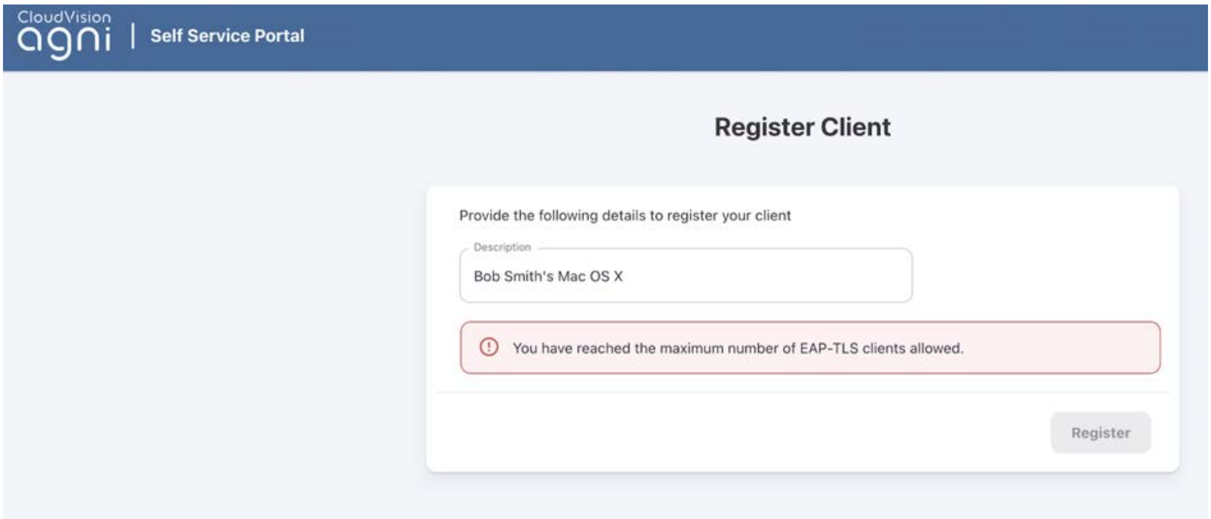
Personal Passphrase Validity Period (Days): 1

EAP-TLS Settings

Maximum Number Of Clients Per User for EAP-TLS Network: 20

Figure:Manage Network Settings

3. Enter a value between 1-20 to set the maximum number of clients per user for the EAP-TLS Network.
   The maximum number of clients you can add is 20. If you enter a value higher than 20, an error message is displayed as in the image below:



Register Client

Provide the following details to register your client

Description: Bob Smith's Mac OS X

You have reached the maximum number of EAP-TLS clients allowed.

Figure:Registering a Client

Note: The maximum limit of 20 applies only to the EAP-TLS network with AGNI public key infrastructure (PKI). This limit is not applicable when AGNI interacts with external PKI infrastructure.

Wireless Captive Portal

Captive Portal provides network access based on the authentication mechanism through the web browsers. The credentials are either validated locally (in case of local users) or via SSO (in case of external IDP integration).

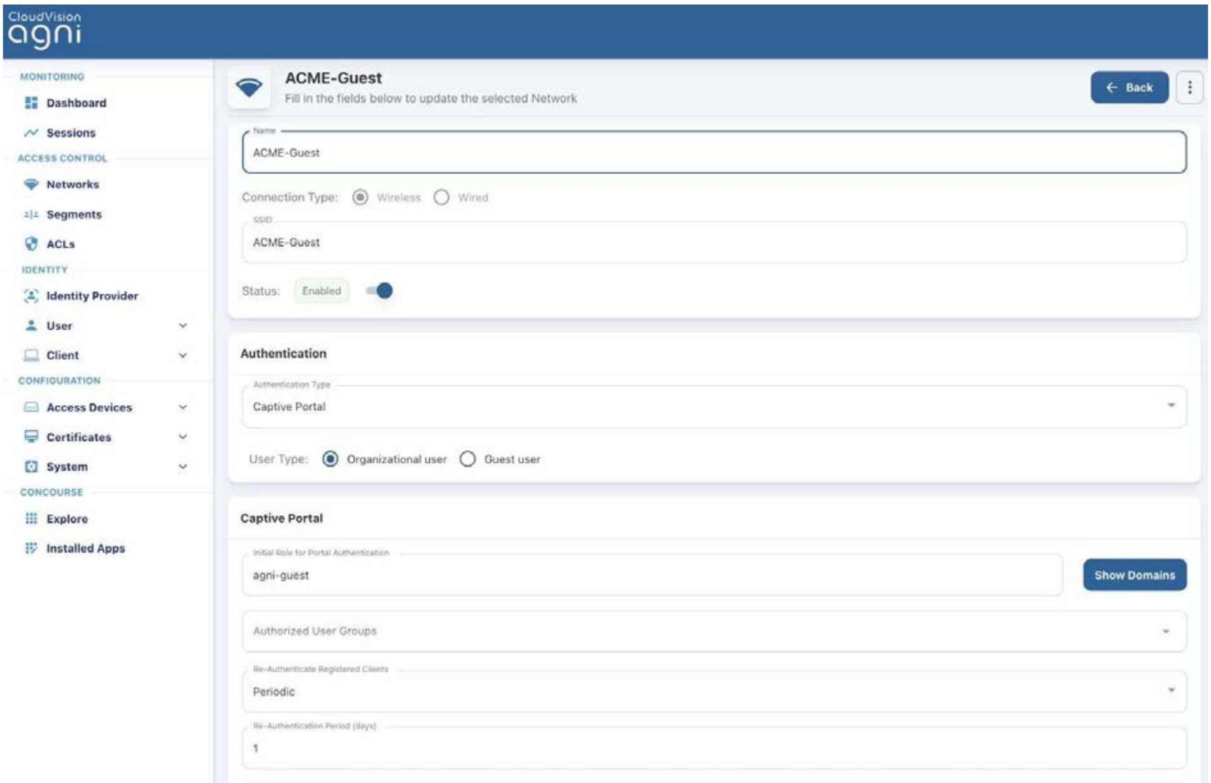
Prerequisites

- Wireless SSID should be configured on the APs to perform Captive Portal authentication.
- Onboarding roles should be configured on the APs.
- Onboarding PSK passphrase should be configured on the SSID.
- Walled garden domain names should be configured to allow access to the required domains (more details under the *Show Domains* section below).
- When using Captive Portal for guest users, ensure the guest portals are configured in Arista Guest Manager application and CV-CUE concourse application credentials have permission to load the guest portals.

Configuration

1. Navigate to **Access Control** → **Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **ConnectionType** as Wireless
3. Enter the **SSID** name. Ensure the name matches the SSID configured in the wireless APs
4. **Status**
   a. **Enabled** - Enables this network to honor incoming requests.
   b. **Disabled** - Disables this network.

5. **Authentication Type** – Authentication type should be set to Captive Portal. This enables the system to honor browser-based authentication requests.
6. **User Type**
    a. **Organizational user** - When set, the system uses configured IDP and authenticates the users externally via SSO.
    b. **Guest user** - When set, the guest portals are loaded from the Arista Guest Manager application. Select the desired guest portal.
7. **Captive Portal**
    a. **Initial Role for Portal Authentication** - Specify the initial role as configured in the AP required for portal authentication. Note that the client remains in this role until the user is successfully authenticated.
    b. **Show Domains** - Displays the list of walled garden domain names that need to be allow-listed in your network infrastructure (wired or wireless) to allow the onboarding process. Without this, the user authentication may be blocked by the network infrastructure.
    c. **Re-authenticate Clients** - This setting is applicable when the user type is set to *Guest user*.
        i. **Periodic** - When set, the clients are re-authenticated once in every *Re-authentication Period (days)* configured. Re-authentication Period (days) specifies the frequency of re-authentication in days.
        ii. **Always** - When set, the clients are re-authenticated whenever connected to the captive portal network.
8. **Authorized User Group** - This setting is optional and applicable when the User Type is set to *Organizational user*. Choose the names of the User Groups, if you need to allow onboarding to be permitted for the users belonging to these groups. When this setting is not provided the system honors onboarding requests from all the users of the organization.
9. **Re-authenticate Registered Clients** - This setting is applicable when the user type is set to *Organizational user*.
    a. **Periodic** - When set, the clients are re-authenticated once in every *Re-authentication Period (days)* configured. Re-authentication Period (days) specifies the frequency of re-authentication in days.
    b. **Always** - When set, the clients are re-authenticated whenever connected to the captive portal network.
    c. **Not Required** - When set, the user is permitted always into the network after the first captive portal authentication.



ACME-Guest

Fill in the fields below to update the selected Network

Name: ACME-Guest

Connection Type: ◉ Wireless ○ Wired

SSID: ACME-Guest

Status: Enabled

Authentication

Authentication Type: Captive Portal

User Type: ◉ Organizational user ○ Guest user

Captive Portal

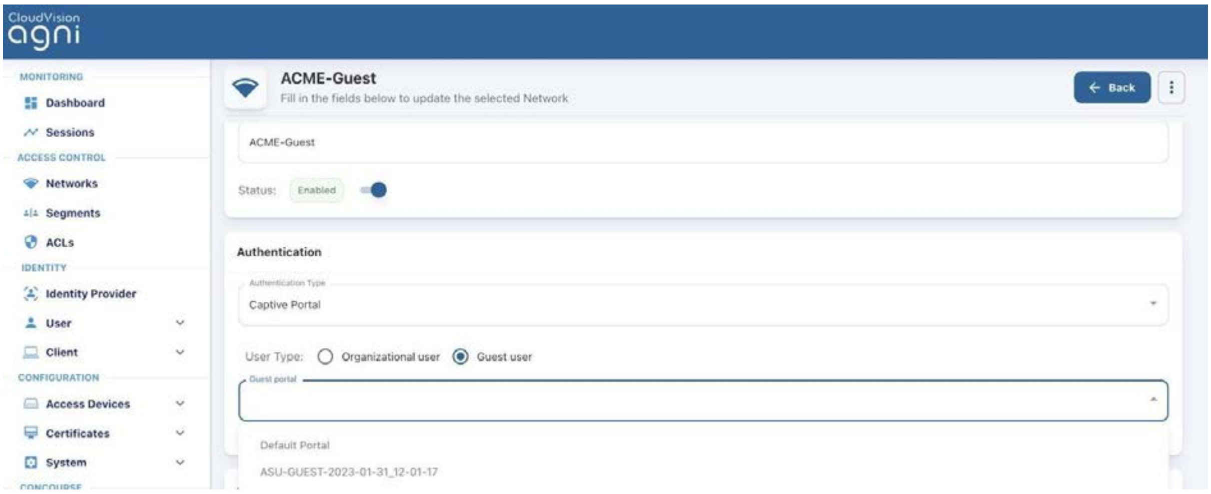
Initial Role for Portal Authentication: agni-guest

Authorized User Groups

Re-Authenticate Registered Clients: Periodic

Re-Authentication Period (days): 1

Figure: Wireless Captive Portal Network-page-1



ACME-Guest

Fill in the fields below to update the selected Network

ACME-Guest

Status: Enabled

Authentication

Authentication Type: Captive Portal

User Type: ○ Organizational user ◉ Guest user

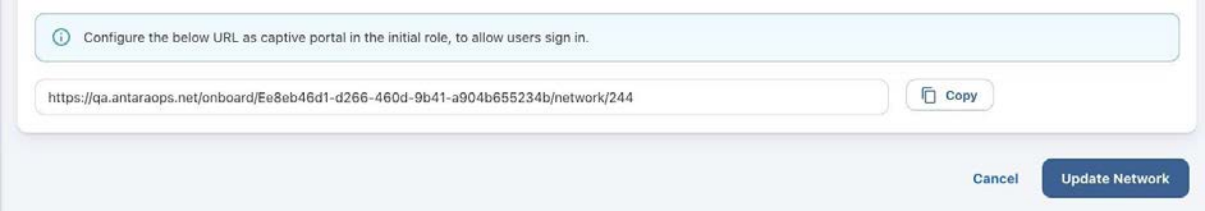
Guest portal

Default Portal

ASU-GUEST-2023-01-31_12-01-17

Figure: Wireless Captive Portal Network-page2

10. Click on the **Add Network** button. The process:
    - Creates the network.
    - Creates an **Onboarding URL**, which should be set as a captive portal URL in the WiFi configuration of your AP. Clients are redirected to this URL for onboarding.



Configure the below URL as captive portal in the initial role, to allow users sign in.

https://qa.antaraops.net/onboard/Ee8eb46d1-d266-460d-9b41-a904b655234b/network/244

Figure: Wireless Captive Portal Network Onboarding

Configuring Guest Portal in AGNI for Wireless Clients

This section describes the steps to configure the guest portal using AGNI for wireless clients. To configure the guest portal, you must configure both AGNI and CV-CUE.

Configuring AGNI

1. Log in to AGNI and navigate to **Configuration > System > Portal Settings**.

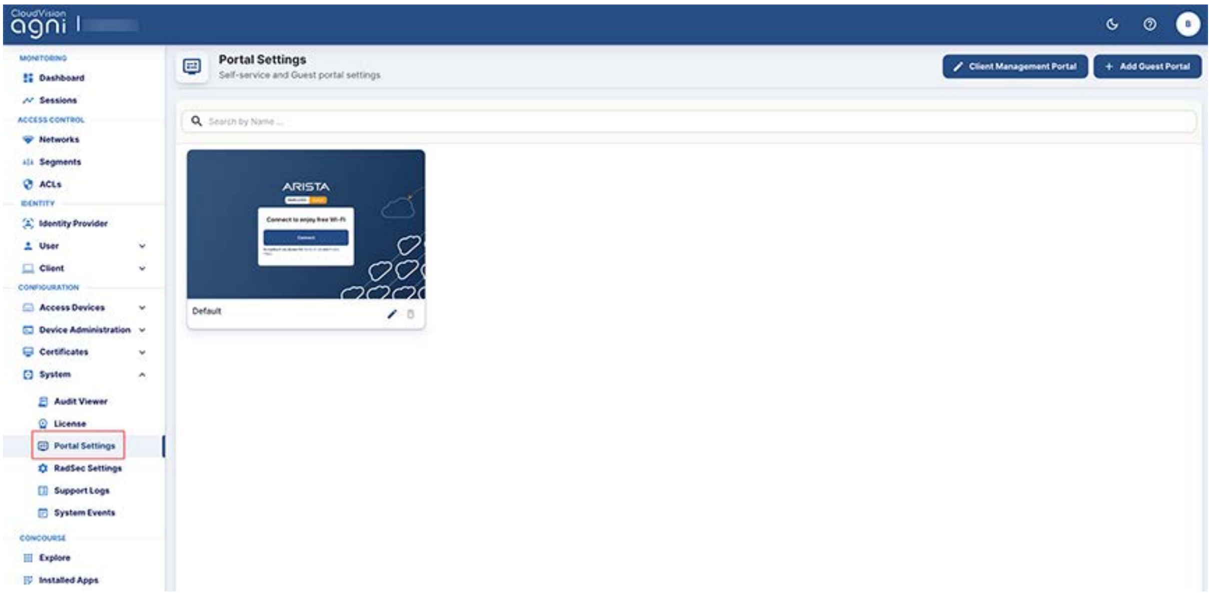


Figure: Portal Settings

2. In **Portal Settings**, the **Default** portal is always present, which is non-removable. You can use the same for configuration. For this article, let’s create a new guest portal.
3. Click the **Add Guest Portal** button.

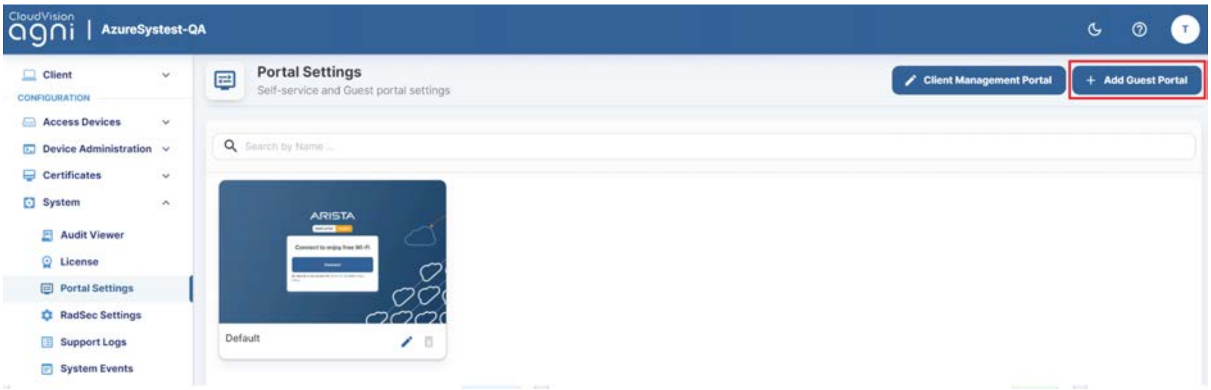
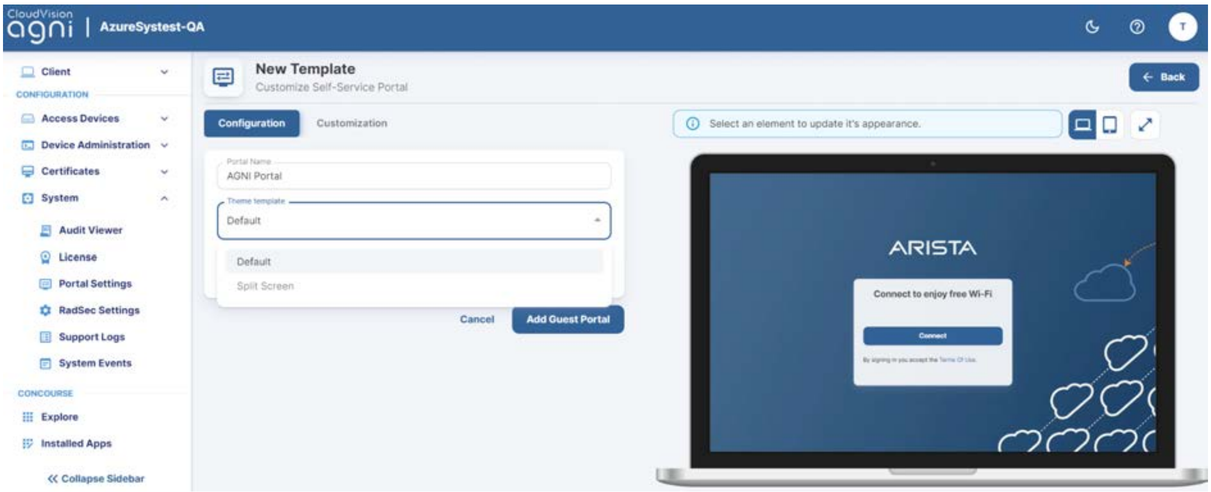


Figure: Portal Settings -1

4. In the **Configuration** tab, provide the portal name and select the theme of the portal. The available theme options are **Default** or **Split Screen**.



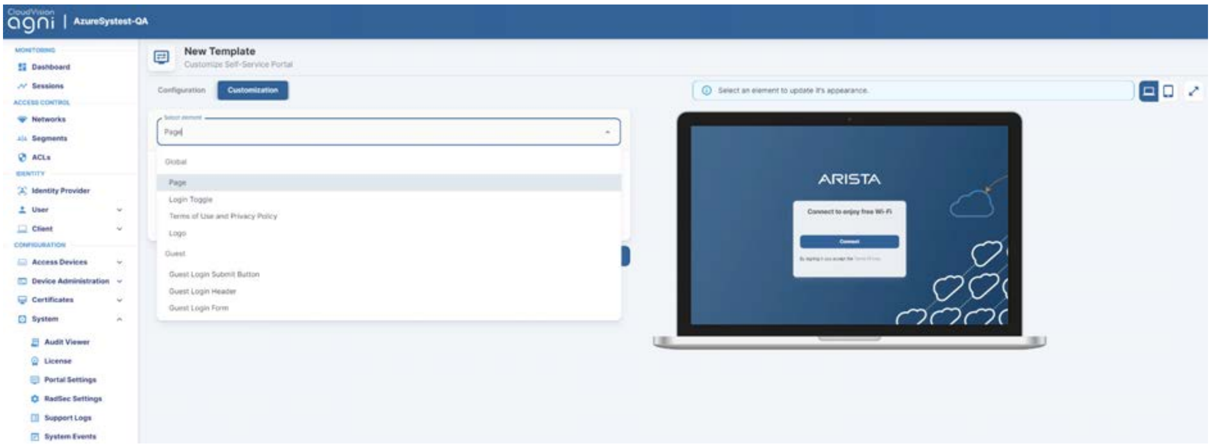
New Template
Customize Self-Service Portal

Portal Name: AGNI Portal

Theme template: Default

Figure:Portal Settings - Template

5. Select the Authentication Type as **Clickthrough**.
6. Click the **Customization** tab to customize the portal settings, including:
    - ○ Page
    - ○ Login Toggle
    - ○ Terms of Use and Privacy Policy
    - ○ Logo
    - ○ Guest Login Submit Button

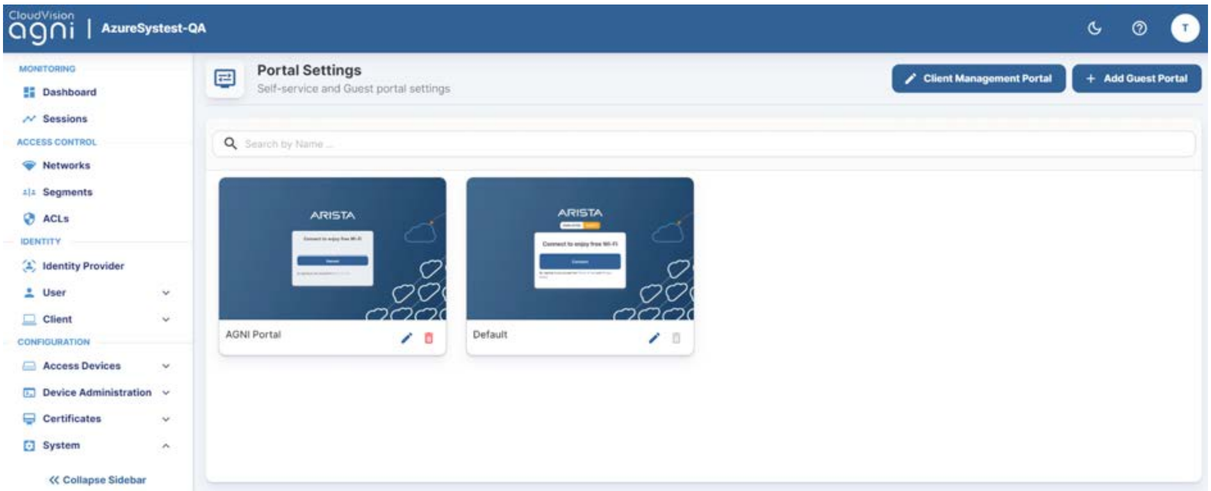


New Template
Customize Self-Service Portal

Select element: Page

Figure:Portal Settings- Template-1

7. When done, click **Add Guest Portal**. The portal gets listed in the portal listing.



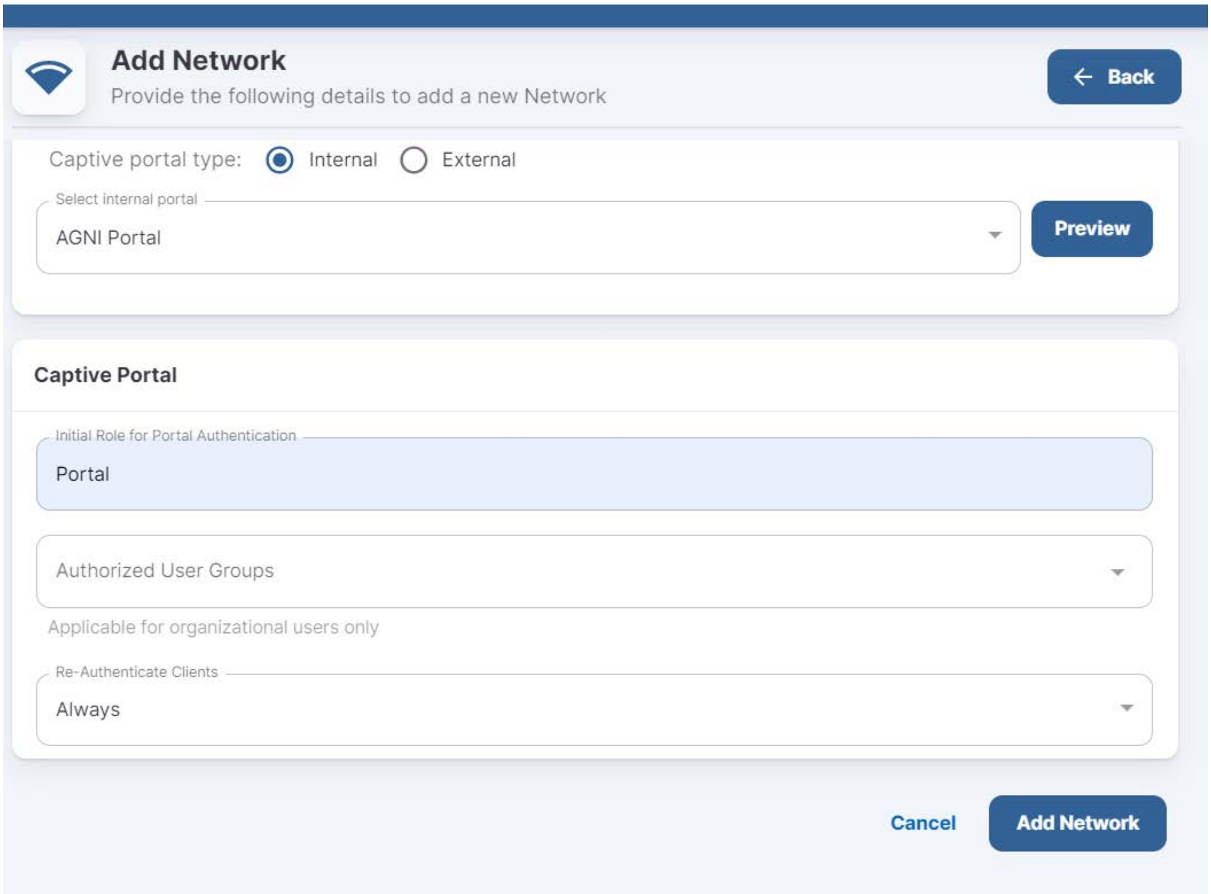
Portal Settings
Self-service and Guest portal settings

AGNI Portal

Default

Figure: Portal Settings page

8. Navigate to the **Access Control > Network**.
9. Add a new network with following settings:
    - Network Name
    - Connection Type — Wireless
    - Authentication
        - Authentication Type
        - Captive Portal Type
    - Captive Portal
        - Internal Portal
        - Re-Authenticate Clients



Add Network
Provide the following details to add a new Network

Captive portal type: ● Internal ○ External

Select internal portal: AGNI Portal

Captive Portal

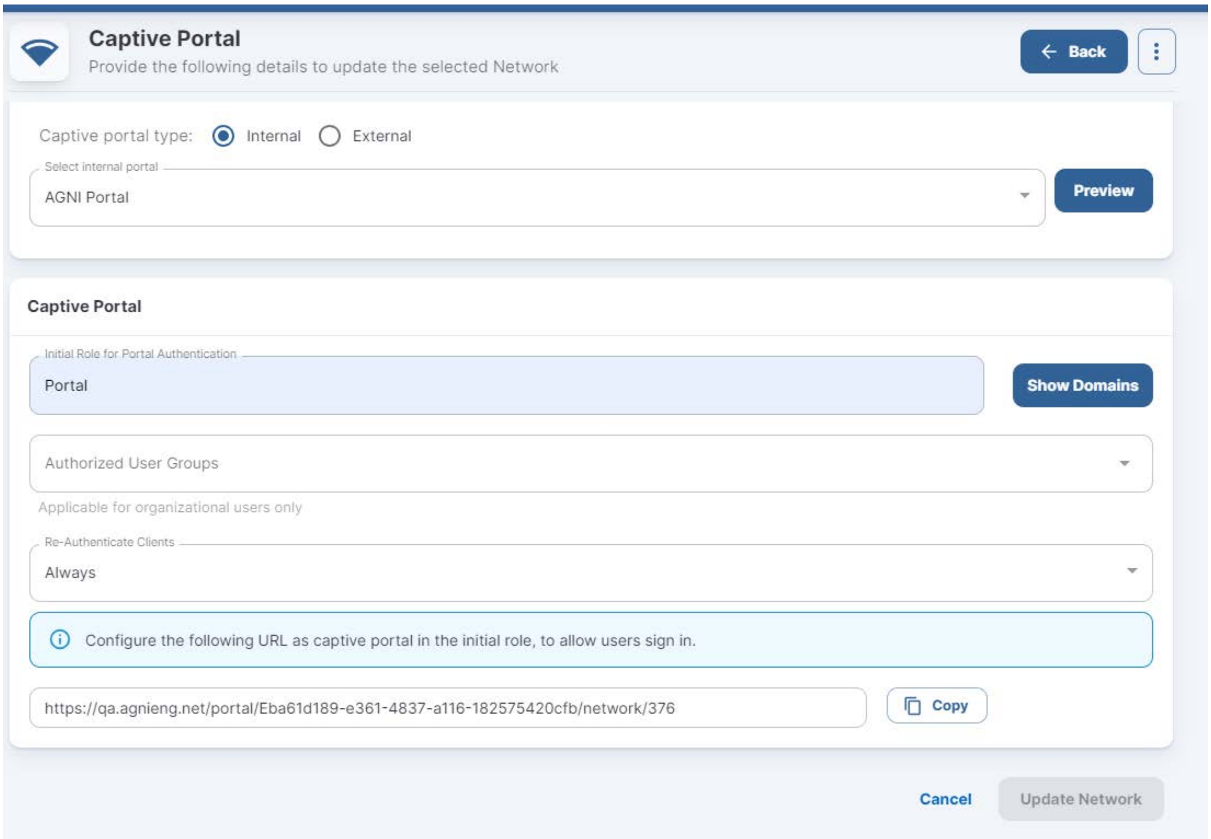
Initial Role for Portal Authentication: Portal

Authorized User Groups

Applicable for organizational users only

Re-Authenticate Clients: Always

10. Click **Add Network**.
11. Edit the added network and copy the portal URL.



Captive Portal

Provide the following details to update the selected Network

Captive portal type: ● Internal ○ External

Select internal portal: AGNI Portal

Captive Portal

Initial Role for Portal Authentication: Portal

Authorized User Groups

Applicable for organizational users only

Re-Authenticate Clients: Always

Configure the following URL as captive portal in the initial role, to allow users sign in.

https://qa.agnieng.net/portal/Eba61d189-e361-4837-a116-182575420cfb/network/376

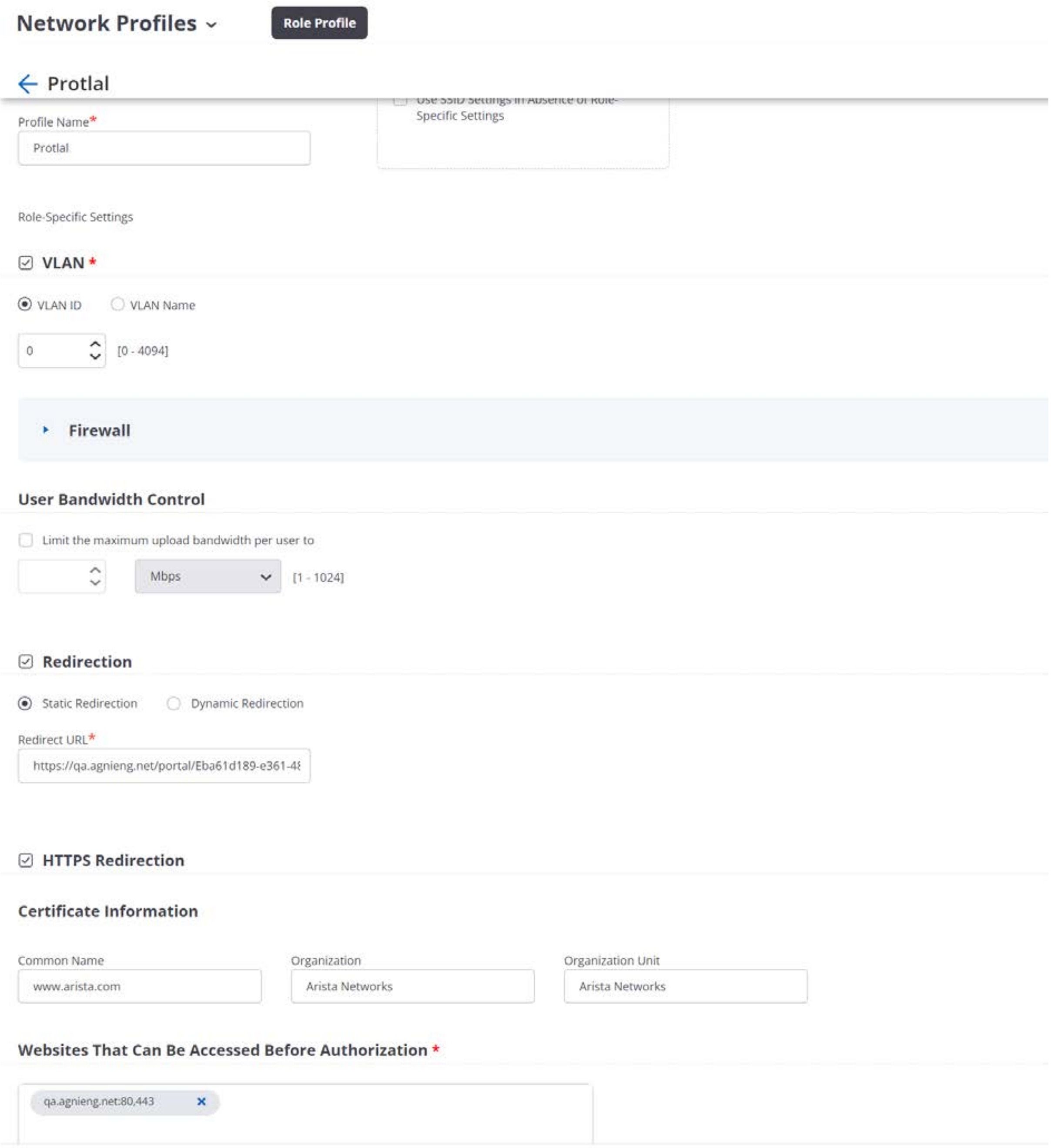
Figure: Captive Portal

Configuring CV-CUE

In CV-CUE, configure a role profile and the SSID settings. Ensure that the SSID is enabled for the captive portal with redirection to the portal URL.

Configuring Role Profile

1. Log in to CV-CUE and navigate to **Configure > Network Profiles > Role Profile**.
2. Add a **Role Profile**.
3. Add the Role Name as **Portal**.
4. Enable the **Redirection** check box and select **Static Redirection**.
5. In the **Redirect URL** field, add the portal URL that you have copied from AGNI.
6. Keep other settings to default.



Network Profiles ⌄ Role Profile

← Protlal

□ Use SSID Settings in Absence of Role-Specific Settings

Profile Name* Protlal

Role-Specific Settings

☑ VLAN *

● VLAN ID ○ VLAN Name

0 [0 - 4094]

▸ Firewall

User Bandwidth Control

□ Limit the maximum upload bandwidth per user to

Mbps [1 - 1024]

☑ Redirection

● Static Redirection ○ Dynamic Redirection

Redirect URL* https://qa.agnieng.net/portal/Eba61d189-e361-48

☑ HTTPS Redirection

Certificate Information

Common Name: www.arista.com

Organization: Arista Networks

Organization Unit: Arista Networks

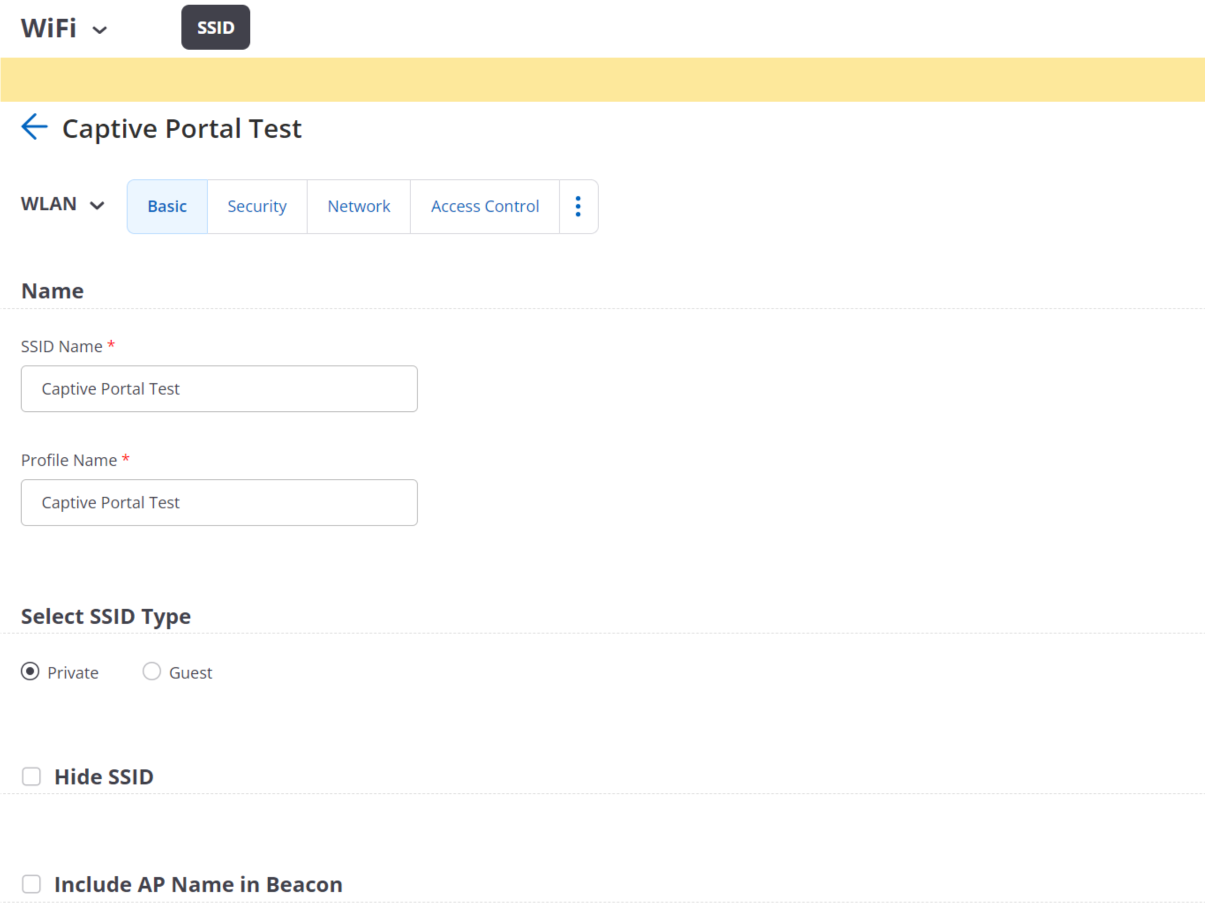
Websites That Can Be Accessed Before Authorization *

qa.agnieng.net:80,443 ×

Figure:Network Profiles

Configuring SSID

1. **Navigate to Configure > WiFi**.
2. Add a new SSID.
3. Provide the SSID Name — Captive Portal Test.



Name

SSID Name *: Captive Portal Test

Profile Name *: Captive Portal Test

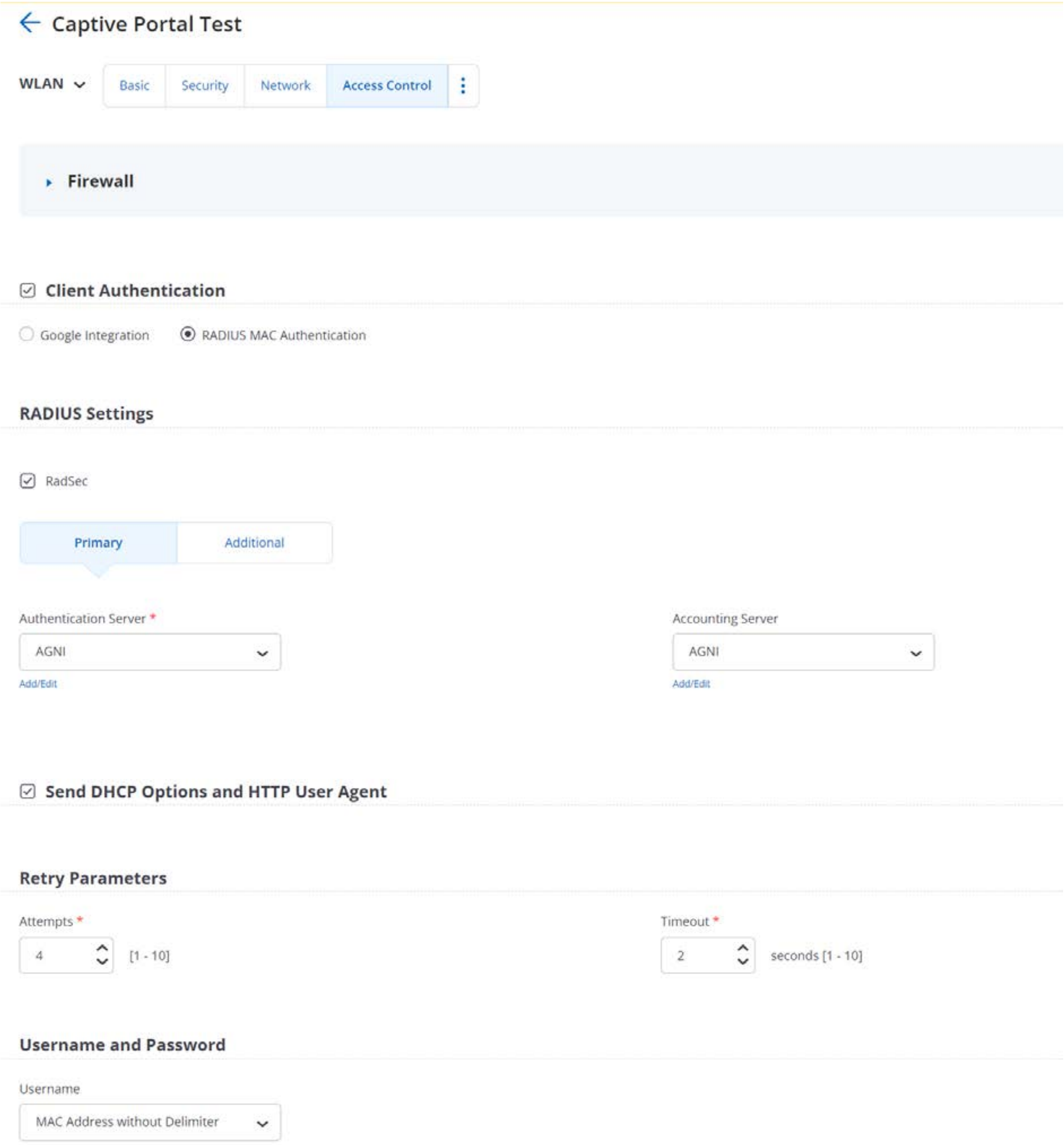
Select SSID Type

● Private ○ Guest

□ Hide SSID

□ Include AP Name in Beacon

4. Click the **Access Control** tab.
5. Enable the **Client Authentication** check box and select **RADIUS MAC Authentication**.
6. Select **RadSec**.
7. Select the **Authentication** and **Accounting** servers.



← Captive Portal Test

WLAN ⌄ | Basic | Security | Network | Access Control | ⋮

▸ Firewall

☑ Client Authentication

○ Google Integration ● RADIUS MAC Authentication

RADIUS Settings

☑ RadSec

Primary | Additional

Authentication Server * AGNI

Add/Edit

Accounting Server AGNI

Add/Edit

☑ Send DHCP Options and HTTP User Agent

Retry Parameters

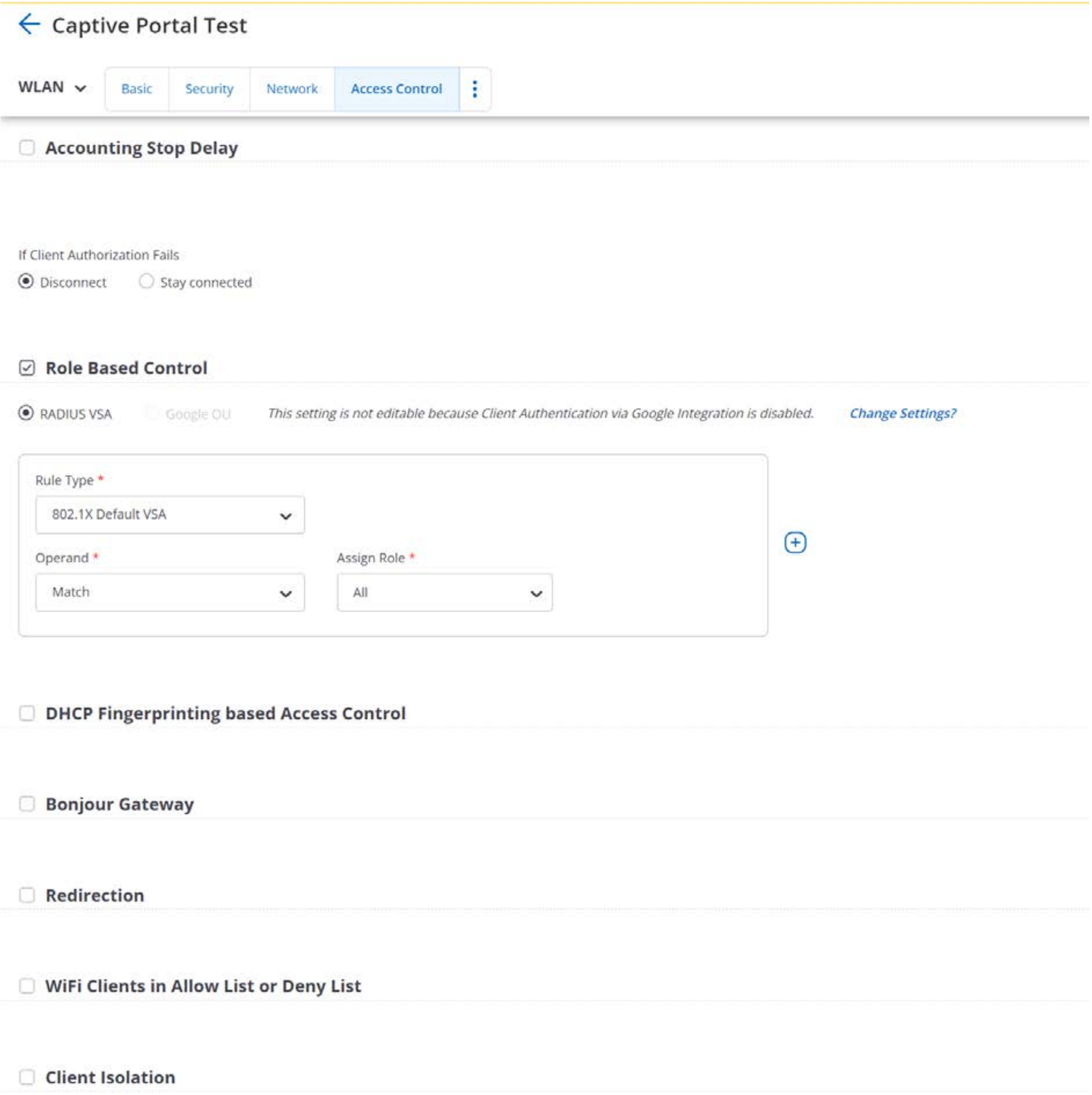
Attempts * 4 [1 - 10]

Timeout * 2 seconds [1 - 10]

Username and Password

Username MAC Address without Delimiter

8. Select the **Role Based Control** checkbox and configure the following settings:
   - Rule Type — 802.1X Default VSA
   - Operand — Match
   - Role — Portal. You have created the **Portal** role profile while configuring the Role Profile in the previous section.



Captive Portal Test

WLAN | Basic | Security | Network | Access Control

□ Accounting Stop Delay

If Client Authorization Fails

● Disconnect ○ Stay connected

☑ Role Based Control

● RADIUS VSA ○ Google OU *This setting is not editable because Client Authentication via Google Integration is disabled.* ***Change Settings?***

Rule Type *: 802.1X Default VSA

Operand *: Match

Assign Role *: All

□ DHCP Fingerprinting based Access Control

□ Bonjour Gateway

□ Redirection

□ WiFi Clients in Allow List or Deny List

□ Client Isolation

9. Save the settings and turn ON the SSID.
   The clients get connected and authenticated via the portal authentication.

Wireless MAC Authentication

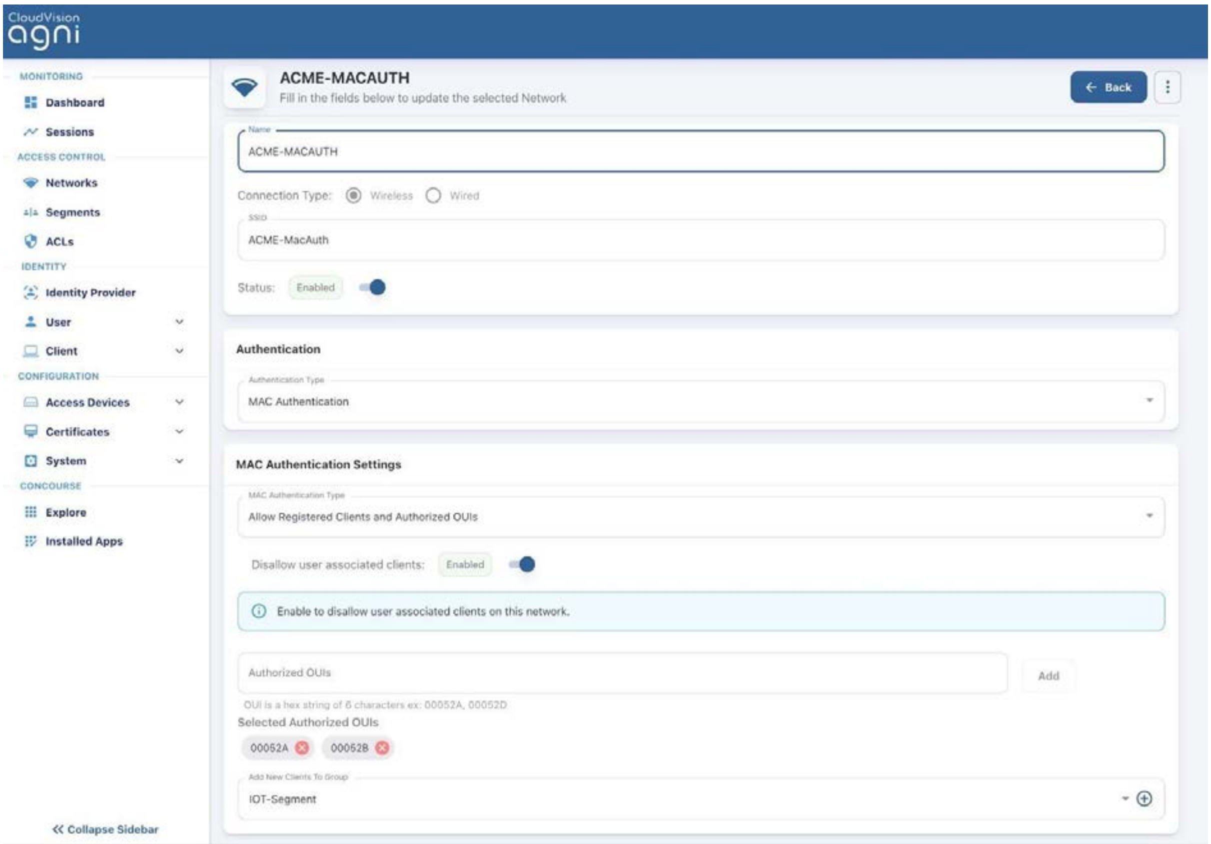
Wireless network configuration enables you to authenticate end clients connected to the network through client MAC addresses. This helps clients to associate with the network based on various factors surrounding MAC addresses such as *registered*, *allow all clients* or *vendor specific client* entities.

Prerequisites

- Wireless SSID should be configured on the AP to perform MAC Bypass Authentication.
- Roles/VLANs used in the segmentation policies should be configured on the AP.

Configuration

1. Navigate to **Access Control → Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **ConnectionType** as Wireless
3. Enter the **SSID** name. Ensure the name matches the SSID configured in the wireless APs
4. **Status**
    a. **Enabled** - Enables this network to honor incoming requests.
    b. **Disabled** - Disables this network.
5. **Authentication Type** – Authentication type should be set to MAC Authentication. This enables the system to honor MAC-Based authentication requests.
6. **MAC Authentication Settings**:
    a. **Allow All Clients** - Allows MAC authentication to succeed for all the clients irrespective of registration status.
        i. **Add New Clients to Group** - Specify the client group to persist the newly authenticated MAC addresses.
    b. **Allow Registered Clients Only** - Allows MAC authentication to succeed for the clients that are registered in AGNI.
        i. **Disallow user-associated clients** – When this option is enabled, the MAC authentication is rejected for the previously onboarded clients.
    c. **Allow Authorized OUIs Only** - Allows MAC authentication to succeed for the listed OUIs only.
        i. **Allow New Clients to Group** - Specify the client group to persist the newly authenticated MAC addresses.
    d. **Allow Registered Clients and Authorized OUIs** – This option behaves similarly to *Allow Registered Clients Only* and *Authorized OUIs Only* combined.



ACME-MACAUTH

Fill in the fields below to update the selected Network

Name: ACME-MACAUTH

Connection Type: ● Wireless ○ Wired

SSID: ACME-MacAuth

Status: Enabled

Authentication

Authentication Type: MAC Authentication

MAC Authentication Settings

MAC Authentication Type: Allow Registered Clients and Authorized OUIs

Disallow user associated clients: Enabled

Enable to disallow user associated clients on this network.

Authorized OUIs

OUI is a hex string of 6 characters ex: 00052A, 00052D

Selected Authorized OUIs

00052A 00052B

Add New Clients To Group: IOT-Segment

Figure: Wireless MAC Authentication Network

Wired 802.1X

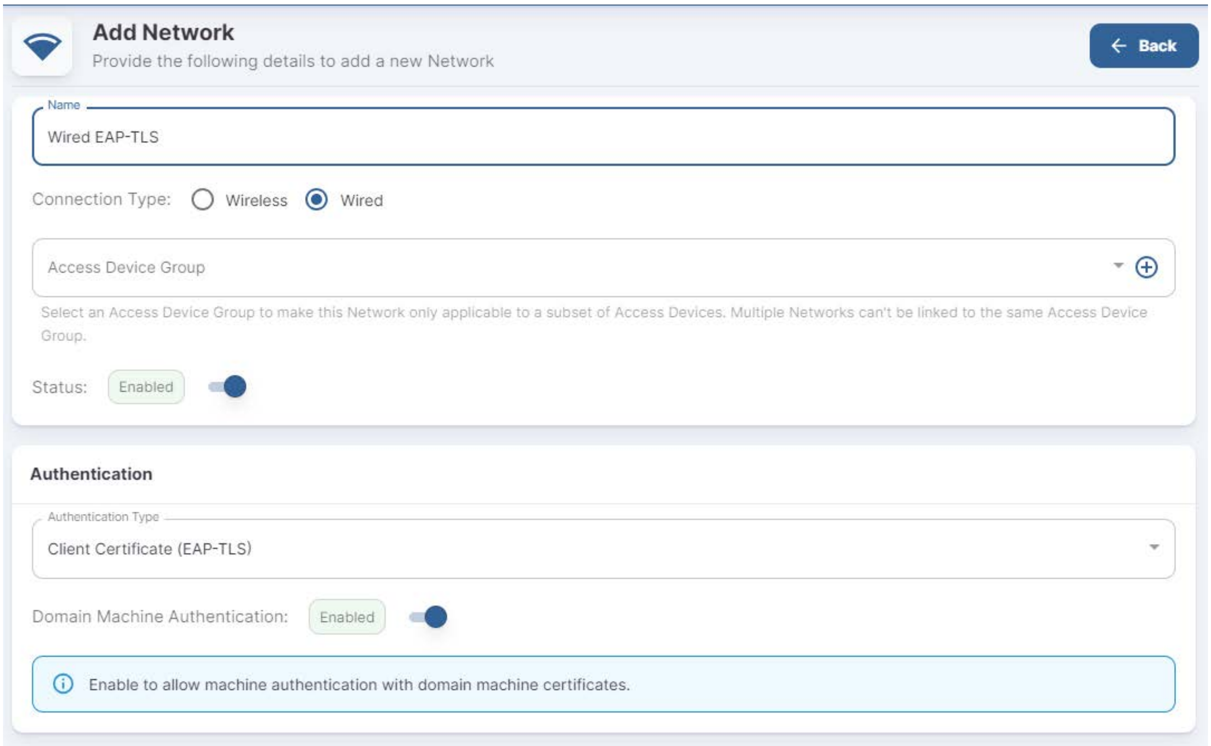
Wired network configuration enables you to authenticate end clients connected to the wired switch port. The system supports 802.1X authentications from the endpoints.

Prerequisites

- The switch should be configured to perform 802.1X against the product.
- VLANs/ACLs used in the segmentation policies should be configured on the switch.

Configuration

1. Navigate to **Access Control** → **Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **ConnectionType** as Wired
3. **Access Device Group** – (Optional setting) If the network authentication is only applicable to a subset of Access Devices, then choose the **Access Device Group**. Otherwise, the network applies to all the network access devices.
4. **Authentication** - Choose the **Authentication Type** as **Client Certificate (EAP-TLS)**
5. **Domain Machine Authentication** - Enable this setting to process the domain machine authentication (via EAP-TLS) requests.



Add Network

Provide the following details to add a new Network

Name: Wired EAP-TLS

Connection Type: ○ Wireless ● Wired

Access Device Group

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

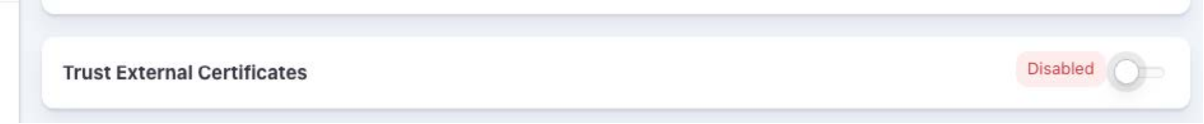
Authentication Type: Client Certificate (EAP-TLS)

Domain Machine Authentication: Enabled

Enable to allow machine authentication with domain machine certificates.

Figure: Add Network (Authentication)

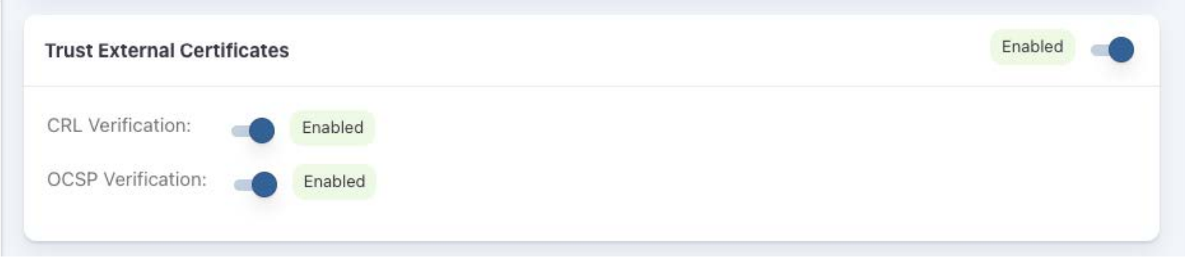
6. **Trust External Certificates**
   a. **Disabled** - Option is applicable when using the system's PKI. This is the default option.



Trust External Certificates: Disabled

Figure: Trust External Certificates

   b. **Enabled** – This option is applicable while using external PKI. You must import the *Root* and *Issuer CAs* into the system.
      i. **CRL Verification** - Select this option to verify the certificate revocation through CRLs.
      ii. **OCSP Verification** - Select this option to verify the certificate revocation through OCSP.



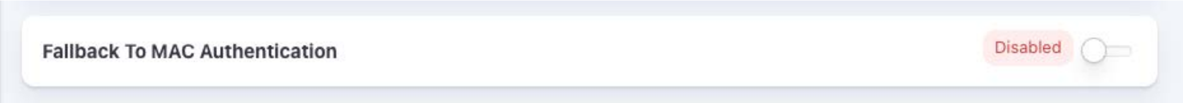
Trust External Certificates: Enabled

CRL Verification: Enabled

OCSP Verification: Enabled

Figure: Add Network (Trusted External Certificates)

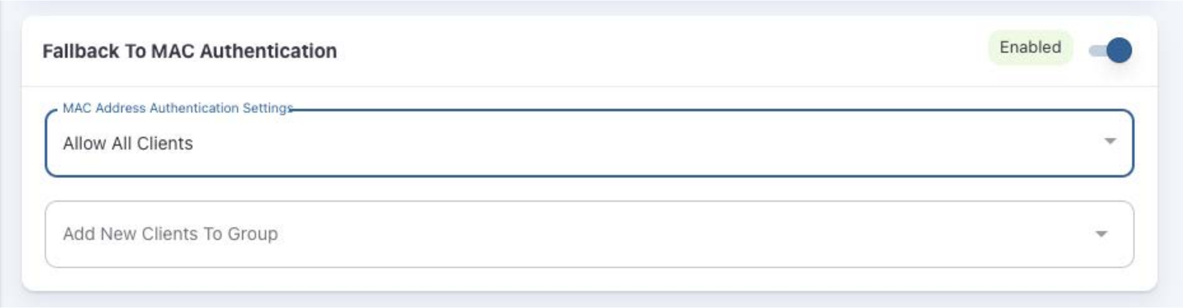
7. **Fallback to MAC Authentication**
    a. **Disabled** - When 802.1X authentication fails, the system rejects the client authentication attempt.



Fallback To MAC Authentication
Disabled

Figure 45: Add Network (Fallback To MAC Authentication)

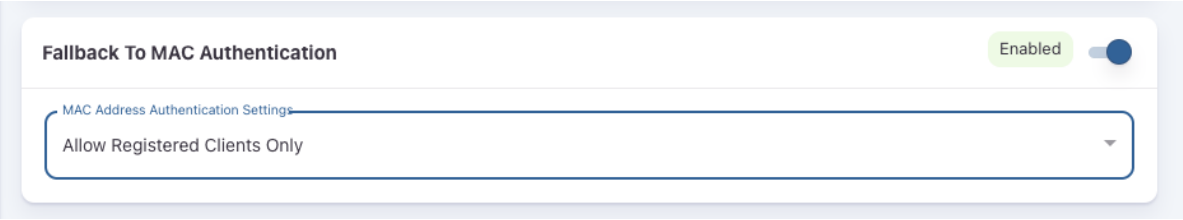
    b. **Enabled** - When 802.1X authentication fails, the system falls back to MAC authentication.
        i. **MAC Authentication Type** - Lists the available authentication settings and chooses the one applicable to the network.
            1. **Allow All Clients** - When set, the MAC authentication admits all the clients that are attempting the wired authentication. Choose a client group to add the authenticated MAC addresses. This enables to build an inventory of the client devices.



Fallback To MAC Authentication
Enabled
MAC Address Authentication Settings: Allow All Clients
Add New Clients To Group

Figure: Add Network (MAC Address Authentication Settings)

            2. **Allow Registered Clients Only** - The system honors MAC authentication attempts only from the registered clients. All the other clients are rejected.

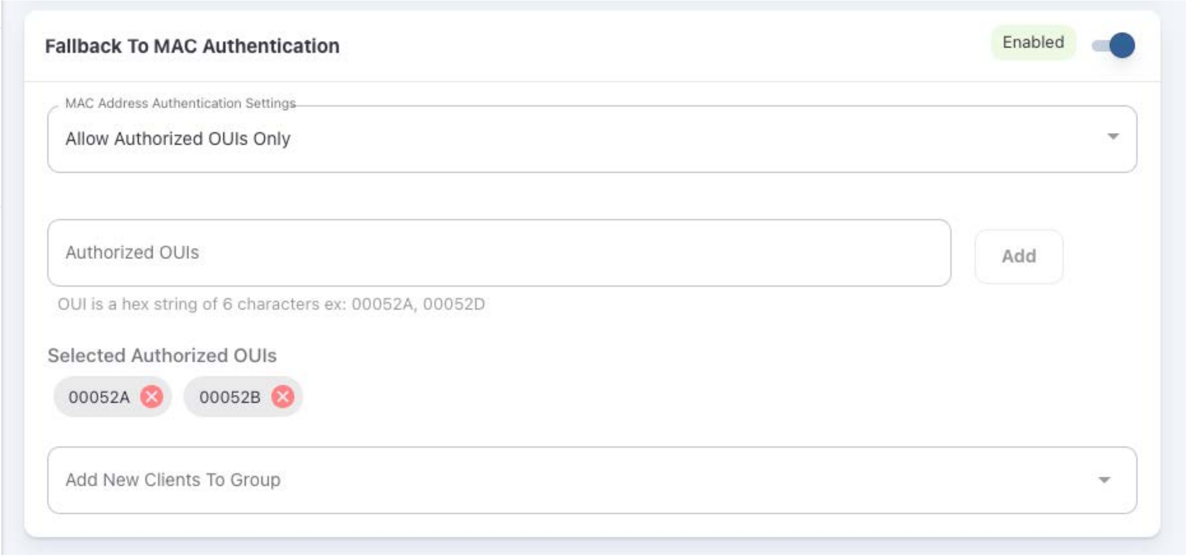


Fallback To MAC Authentication
Enabled
MAC Address Authentication Settings: Allow Registered Clients Only

Figure: Add Network (Fallback to MAC Authentication)

            3. **Allow Authorized OUIs Only** - When set, the system honors the MAC authentication attempts only from the clients matching the authorized OUI list. The Authorized OUI list should be specified for this setting. Choose a client group to add the authenticated MAC addresses. This enables to create an inventory of the client devices.

        ii. **Allow Registered Clients and Authorized OUIs** – This option behaves similarly to *Allow Registered Clients Only* and *Authorized OUIs Only* combined.



Fallback To MAC Authentication Enabled

MAC Address Authentication Settings: Allow Authorized OUIs Only

Authorized OUIs

Add

OUI is a hex string of 6 characters ex: 00052A, 00052D

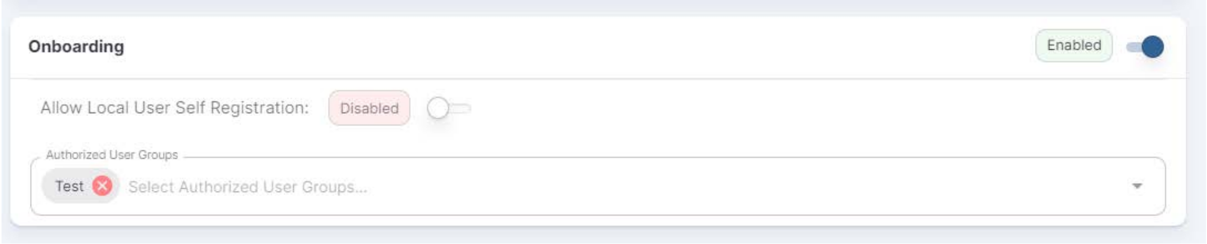
Selected Authorized OUIs

00052A ⊗ 00052B ⊗

Add New Clients To Group

Figure: Allow Authorized OUIs Only

c. **Onboarding** - The admin can enable the Onboarding option to enable self-certificate generation. Users can use the onboarding URL to get authenticated and generate the certificate. Admin can also allow onboarding for specific user groups.
For local users, the admin can enable self-registration to enroll them in the system.



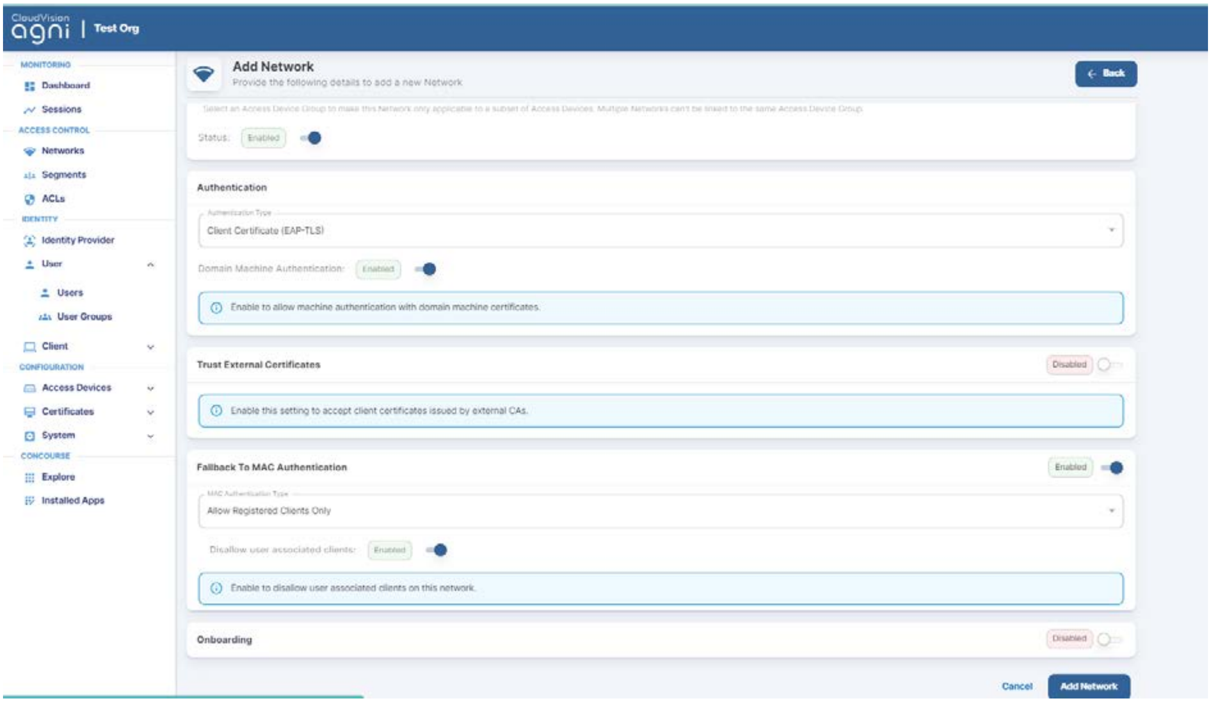
Onboarding Enabled

Allow Local User Self Registration: Disabled

Authorized User Groups: Test ⊗ Select Authorized User Groups...

Figure: Onboarding

8. Click on the **Add Network** button to save the configuration. The created wired 802.1X network is displayed (see image below).



Add Network

Provide the following details to add a new Network

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: Enabled

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: Enabled

Enable to disallow user associated clients on this network.

Onboarding: Disabled

Figure: Sample Wired 802.1X configuration

Wired MAC Authentication

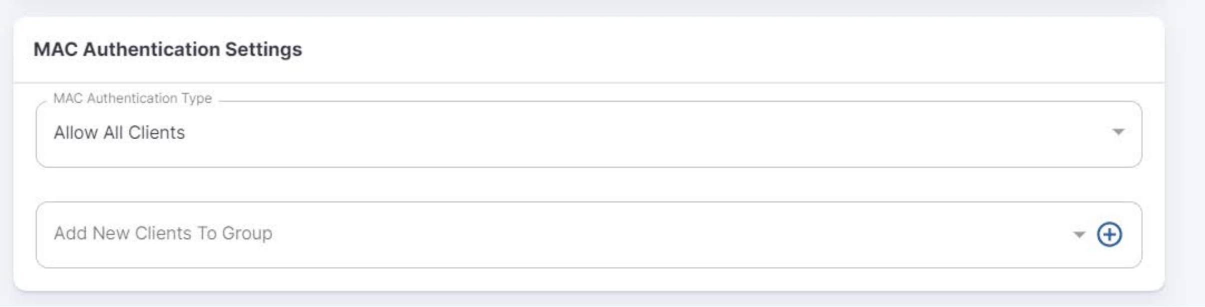
Wired network configuration enables you to authenticate end clients connected to the wired switch port. MAC authentication is a way of authenticating wired clients if the endpoint do not follow the 802.1X authentication method.

Prerequisites

- Switch should be configured to perform MAC ByPass authentication against the product.
- VLANs/ACLs used in the segmentation policies should be configured on the switch.

Configuration

1. Navigate to **Access Control** → **Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **ConnectionType** as Wired
3. **Access Device Group** – (Optional setting) If the network authentication is only applicable to a subset of Access Devices, then choose the **Access Device Group**. Otherwise, the network applies to all the network access devices.
4. **Authentication** - Choose the **Authentication Type** as **MAC Authentication**
5. **MAC Authentication Settings** - Lists the available authentication settings, you can choose the one applicable to the network.
    a. **Allow All Clients** - When set, the MAC authentication admits all the clients that are attempting the wired authentication. Choose a client group to add the authenticated MAC addresses. This help to build an inventory of the client devices.



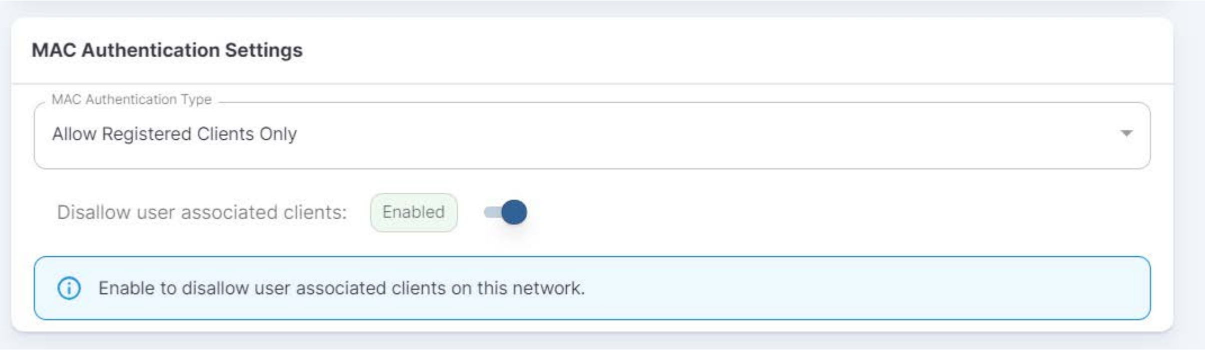
MAC Authentication Settings

MAC Authentication Type: Allow All Clients

Add New Clients To Group

Figure: Add Network

b. **Allow Registered Clients Only** - The system honors MAC authentication attempts only from the clients that are registered with the system. All the other clients are rejected.



MAC Authentication Settings

MAC Authentication Type: Allow Registered Clients Only

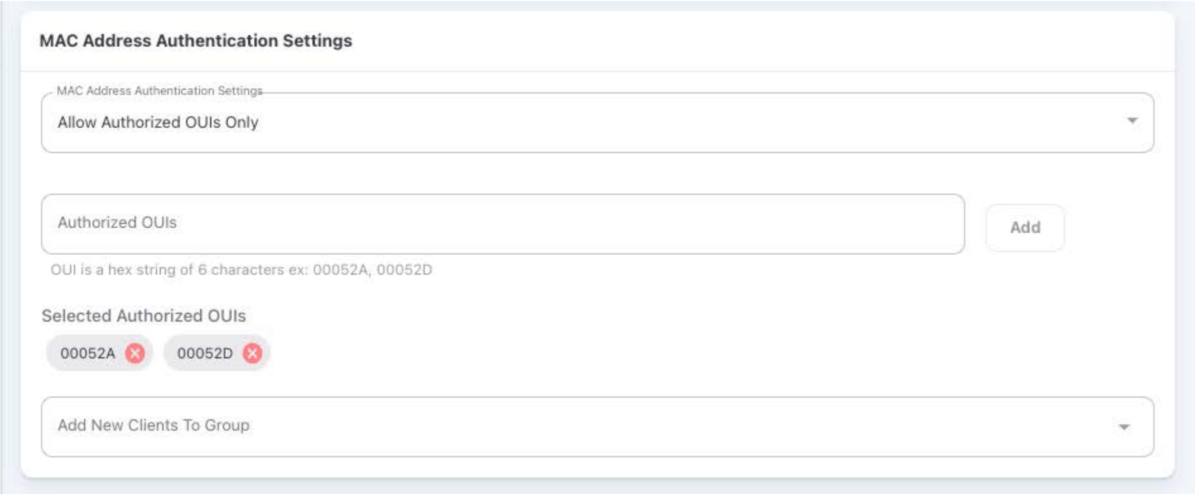
Disallow user associated clients: Enabled

Enable to disallow user associated clients on this network.

Figure: Add Network (MAC Address Authentication Settings)

c. **Allow Authorized OUIs Only** - When set, the system honors the MAC authentication attempts only from the clients matching the authorized OUI list. The Authorized OUI list should be specified for this setting. Choose a client group to add the authenticated MAC addresses. This helps to build an inventory of the client devices.

d. **Allow Registered Clients and Authorized OUIs** – This behavior is like *Allow Registered Clients Only* and *Authorized OUIs Only* combined.



MAC Address Authentication Settings

MAC Address Authentication Settings: Allow Authorized OUIs Only

Authorized OUIs

OUI is a hex string of 6 characters ex: 00052A, 00052D

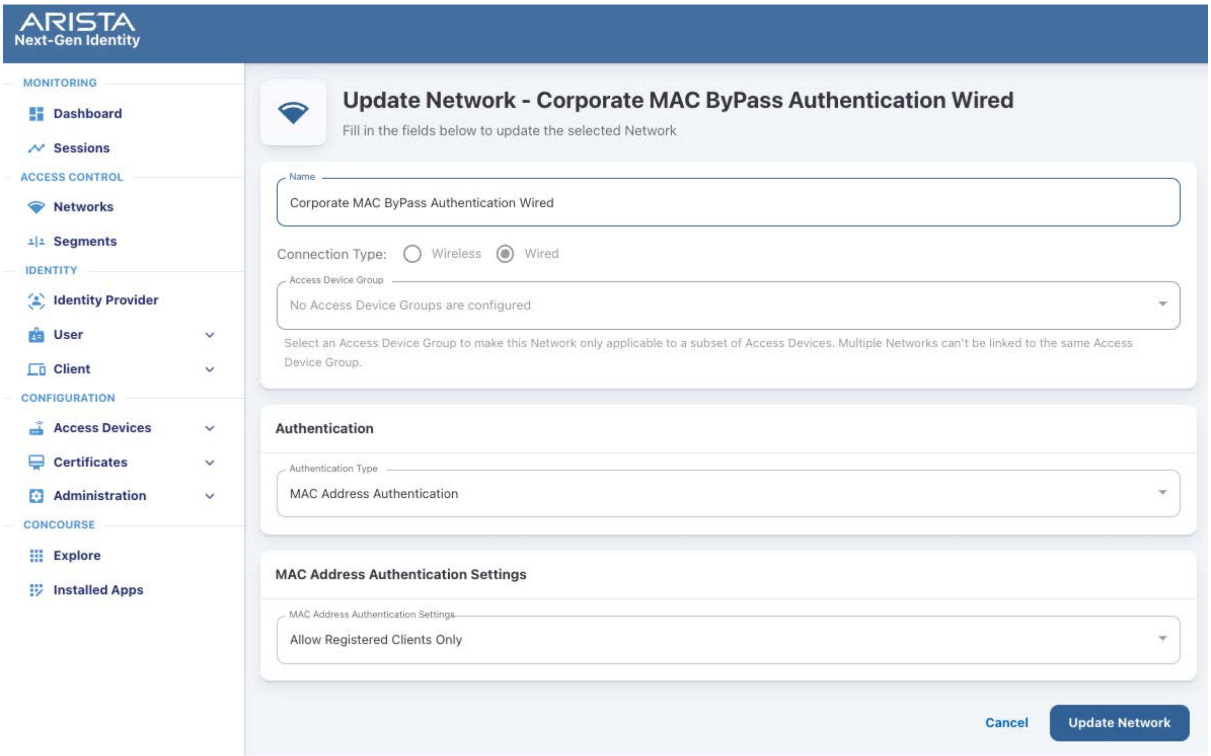
Selected Authorized OUIs

00052A 00052D

Add New Clients To Group

Figure: Add Network (Authorized OUIs)

6. Click on **Add Network** to save the configuration. The created wired MAC authentication network is displayed in the image below.



Update Network - Corporate MAC ByPass Authentication Wired

Fill in the fields below to update the selected Network

Name: Corporate MAC ByPass Authentication Wired

Connection Type: ○ Wireless ● Wired

Access Device Group: No Access Device Groups are configured

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.

Authentication

Authentication Type: MAC Address Authentication

MAC Address Authentication Settings

MAC Address Authentication Settings: Allow Registered Clients Only

Figure: MAC ByPass Authentication Configuration

Wired Captive Portal

Captive Portal authentication provides capabilities for L3 authentication in the network. The end user is connected to the switch port and is redirected to the Captive Portal to perform the authentication after the Mac Authentication. Network access is provided based on the authentication result.

With Captive Portal authentication, the network administrators have the flexibility to drive reauthentication at periodic intervals (in days), never, or always.

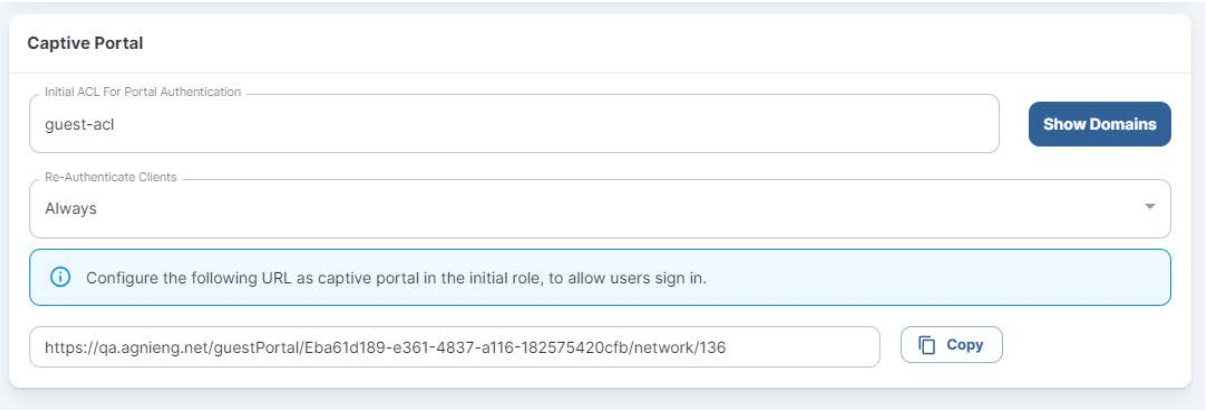
Prerequisites

- AGNI Captive Portal URL should be configured in the switch ACL.
- ACL and Mac Authentication should be configured on the switches.
- Network Enforcement details should be configured on the switch.

Configuration

1. Navigate to **Access Control** → **Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **ConnectionType** as Wired
3. **Authentication** – Choose the Authentication Type as Captive Portal

4. Captive Portal
    a. **Initial ACL for Portal Authentication** - Specify the initial ACL for Captive Portal authentication. Note that this ACL should be configured on the switch and the user is forced to redirect to the captive portal by ACL applied on the switch port.
    b. **Re-authenticate Registered Clients** - Specify one of the below options
        i. **Always** – Choose this option if the user should be authenticated every time they connect to the switch port.



Captive Portal

Initial ACL For Portal Authentication: guest-acl

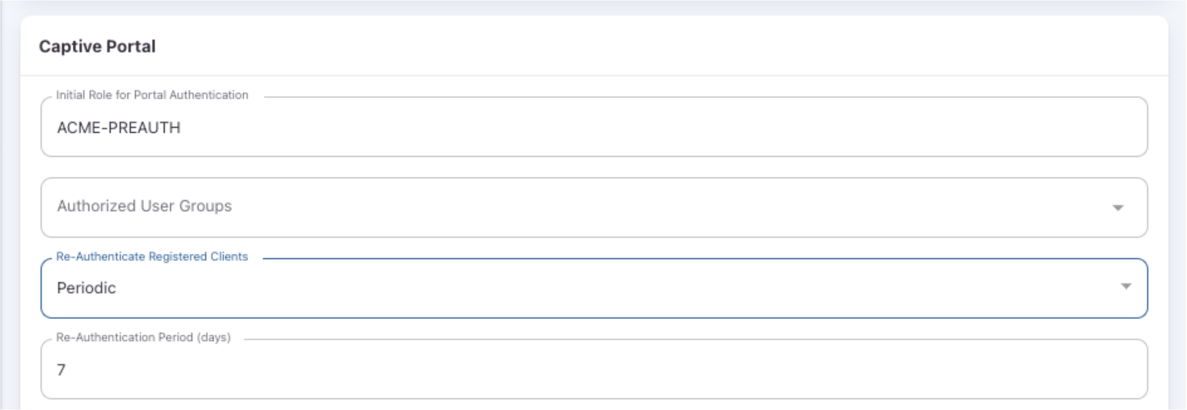
Re-Authenticate Clients: Always

Configure the following URL as captive portal in the initial role, to allow users sign in.

https://qa.agnieng.net/guestPortal/Eba61d189-e361-4837-a116-182575420cfb/network/136

Figure: Captive Portal

        ii. **Periodic** - If the re-authentication is required once in a few days. The configuration setting requires a Re-authentication period interval to be specified in days.



Captive Portal

Initial Role for Portal Authentication: ACME-PREAUTH

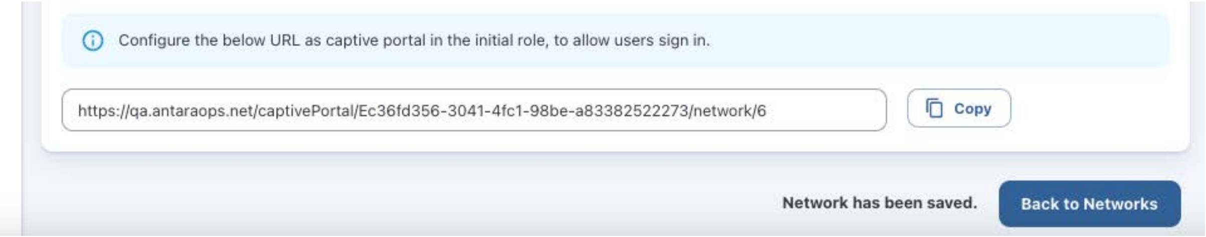
Authorized User Groups

Re-Authenticate Registered Clients: Periodic

Re-Authentication Period (days): 7

Figure: Captive Portal (Re-authentication Option Periodic)

5. Click on the **Add the network** button. The process generates a Captive Portal URL, which should be specified in the switch ACL.



Configure the below URL as captive portal in the initial role, to allow users sign in.

https://qa.antaraops.net/captivePortal/Ec36fd356-3041-4fc1-98be-a83382522273/network/6

Network has been saved.

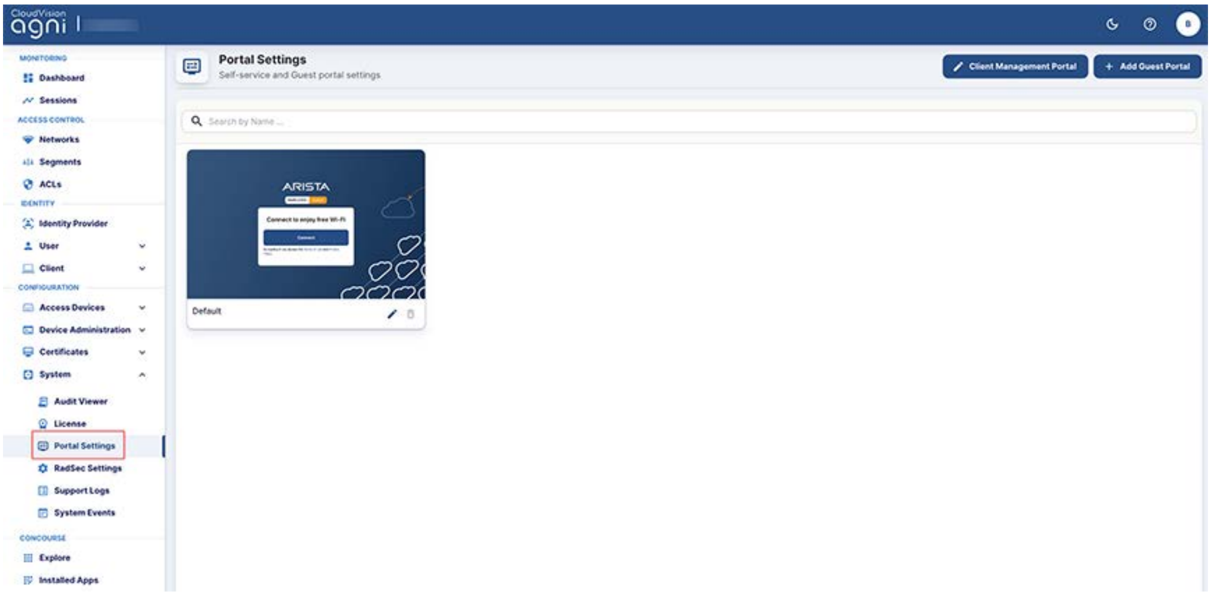
Figure: Captive Portal URL

Configuring Guest Portal in AGNI for Wired Clients

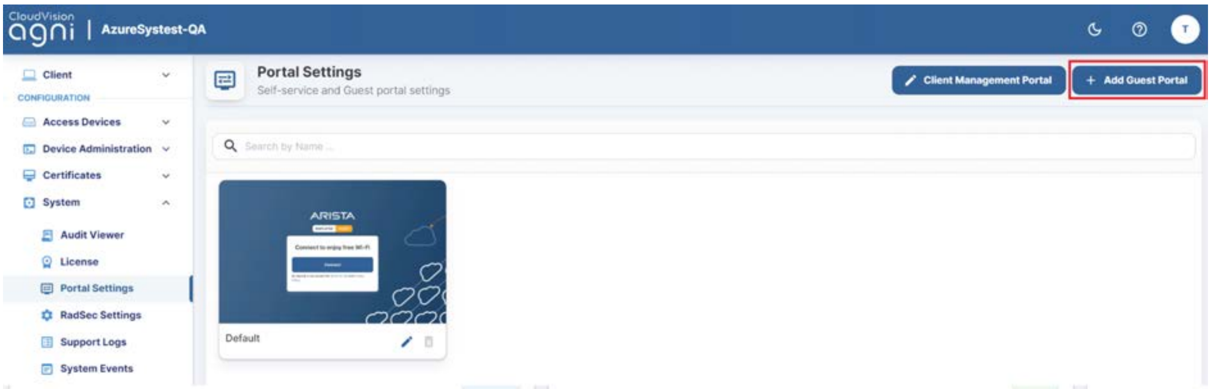
This section describes the steps to configure the guest portal using AGNI for wired clients. To configure the guest portal, you must configure AGNI and the switch.

Configuring AGNI

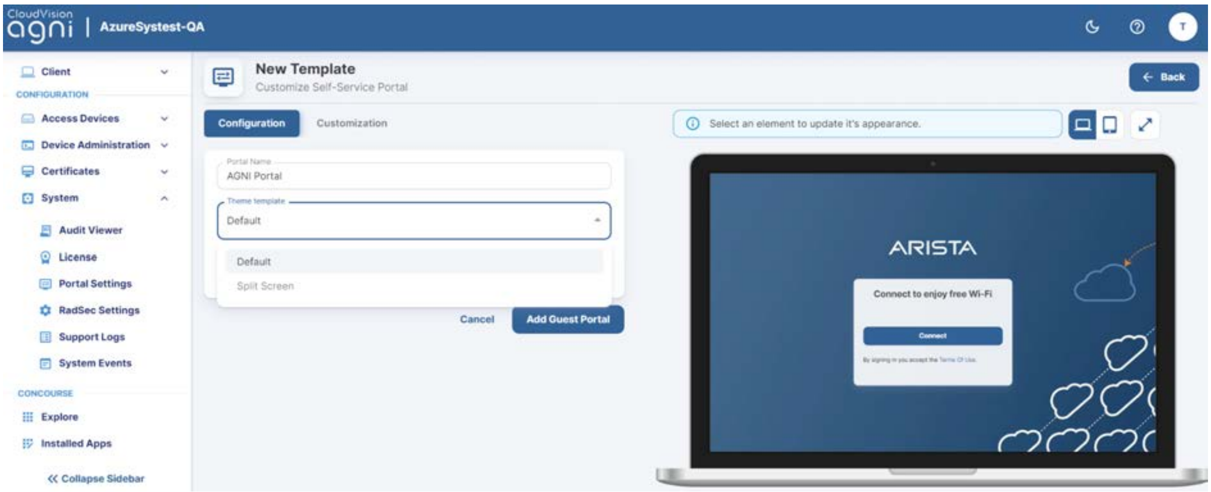
1. Log in to AGNI and navigate to **Configuration > System > Portal Settings**.



2. Click the **Add Guest Portal** button.



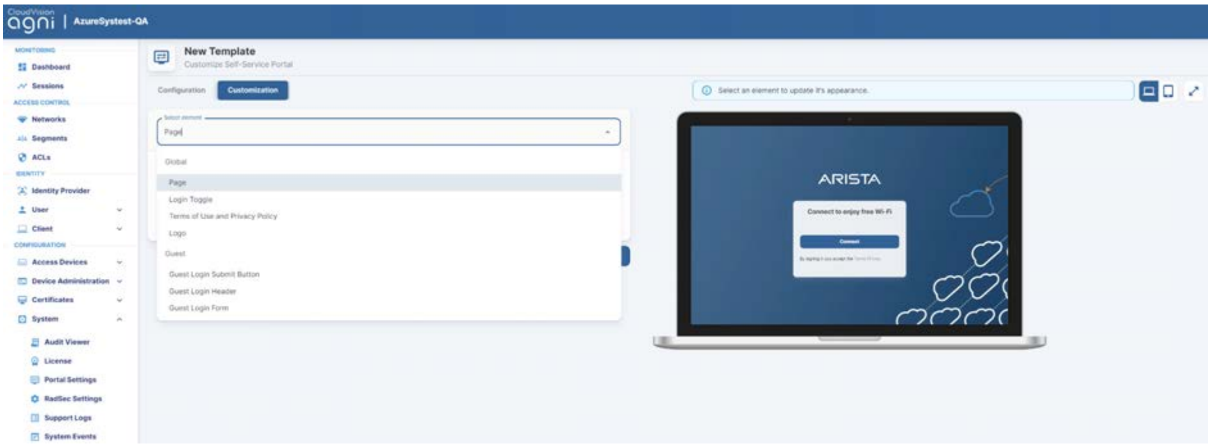
3. In the **Configuration** tab, provide the portal name and select the theme of the portal. The available theme options are **Default** or **Split Screen**.



Portal Name: AGNI Portal

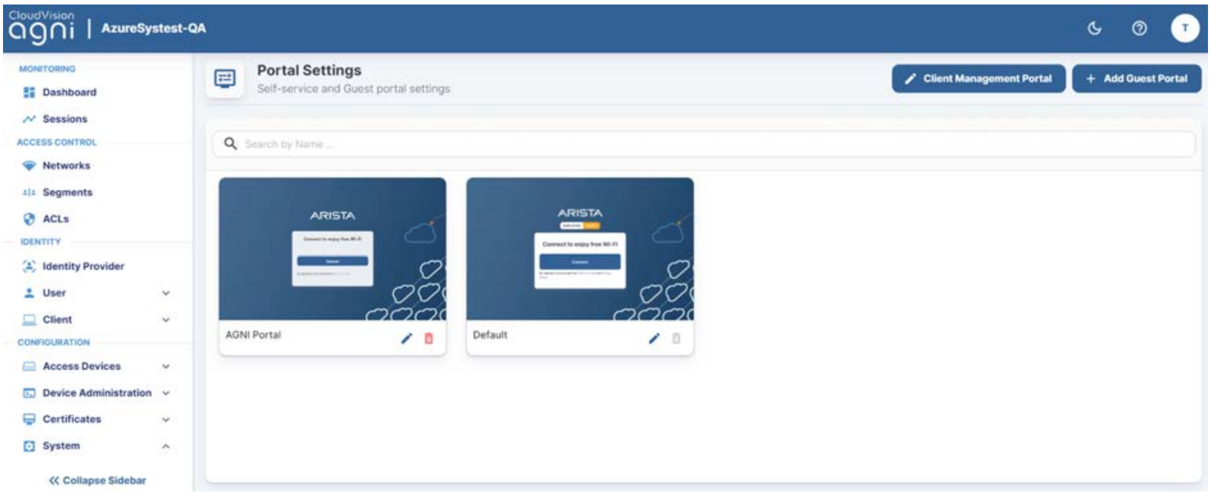
Theme template: Default

4. Select the Authentication Type as **Clickthrough**.
5. Click the **Customization** tab to customize the portal settings, including:
    - Page
    - Login Toggle
    - Terms of Use and Privacy Policy
    - Logo
    - Guest Login Submit Button



Select element: Page

6. When done, click **Add Guest Portal**. The portal gets listed in the portal listing.



Portal Settings

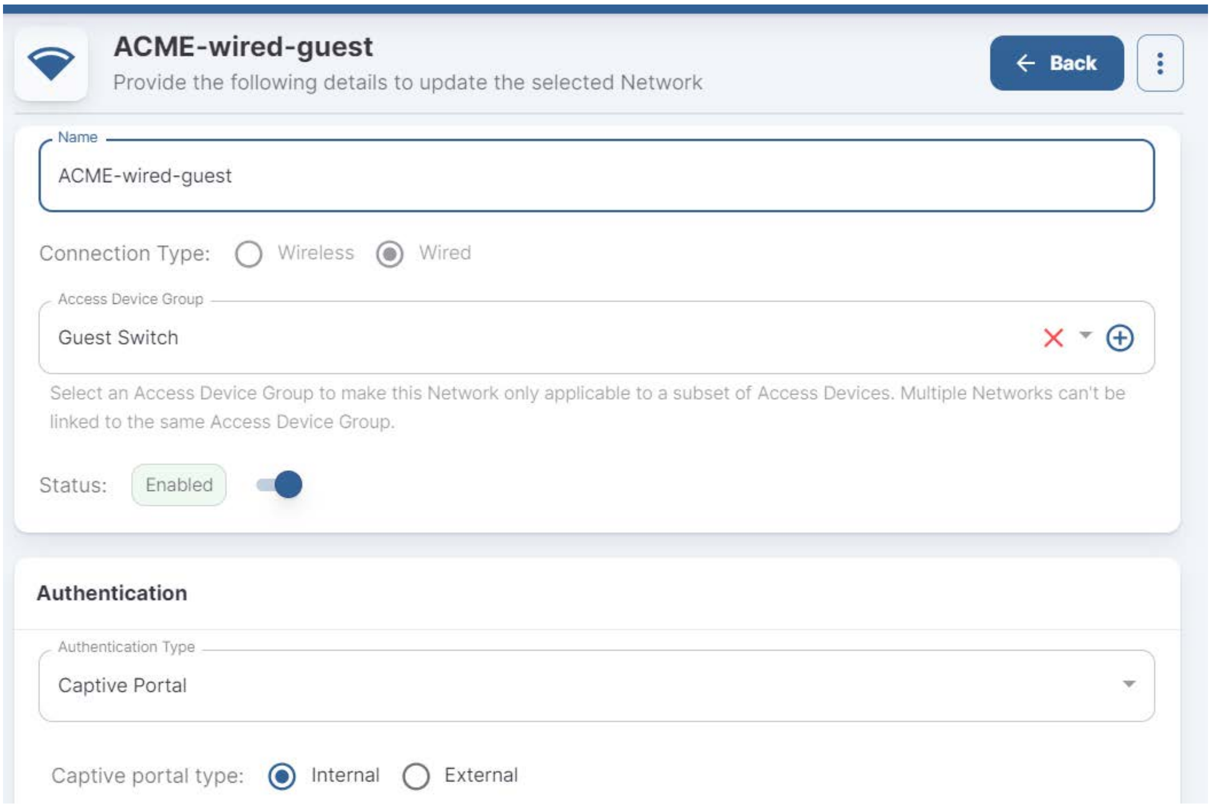
Self-service and Guest portal settings

AGNI Portal

Default

The portal gets listed in the portal listing.

7. Navigate to the **Access Control > Network**.
8. Add a new network with following settings:
   - Network Name
   - Connection Type — Wired
   - Access Device Group — Switch Group
   - Authentication
     - Authentication Type — Captive Portal
     - Captive portal Type — Internal for AGNI Hosted Captive Portal
   - Captive Portal
     - Initial ACL — ACL Name
     - Authorized user group — if applicable
     - Re-Authentication Clients — per requirement



ACME-wired-guest

Provide the following details to update the selected Network

Name: ACME-wired-guest

Connection Type: ○ Wireless ● Wired

Access Device Group: Guest Switch

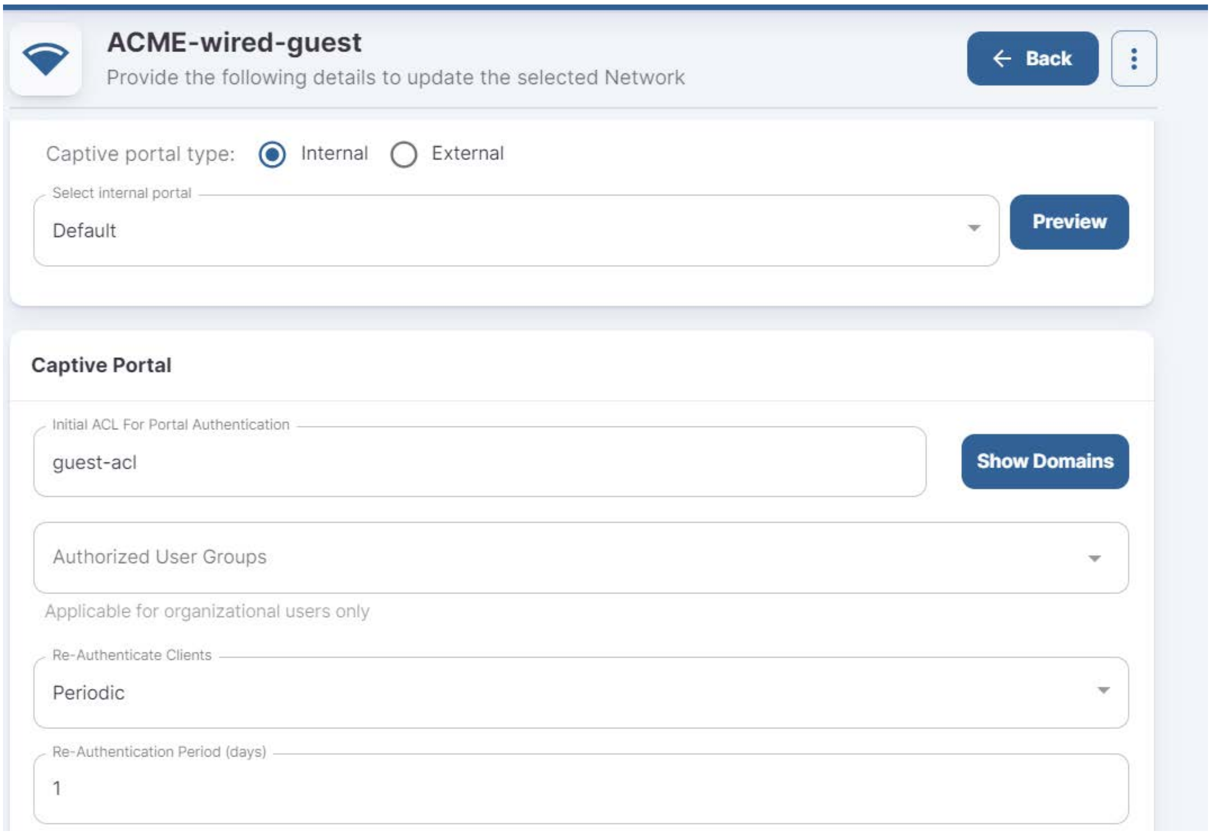
Select an Access Device Group to make this Network only applicable to a subset of Access Devices. Multiple Networks can't be linked to the same Access Device Group.

Status: Enabled

Authentication

Authentication Type: Captive Portal

Captive portal type: ● Internal ○ External



ACME-wired-guest

Provide the following details to update the selected Network

Captive portal type: ● Internal ○ External

Select internal portal: Default

Captive Portal

Initial ACL For Portal Authentication: guest-acl

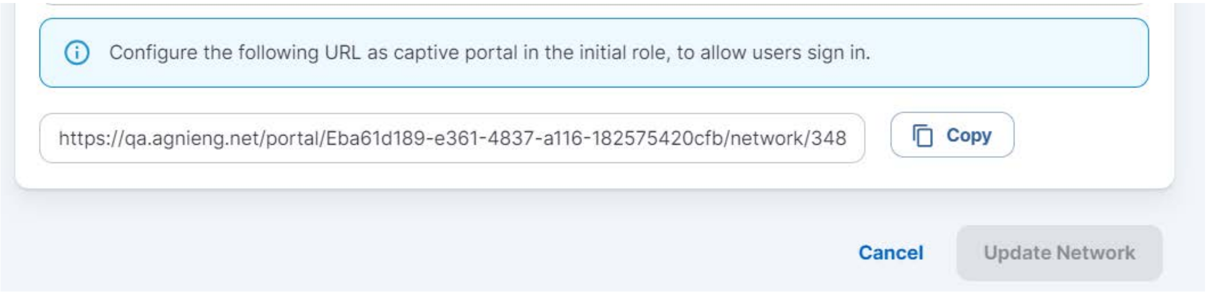
Authorized User Groups

Applicable for organizational users only

Re-Authenticate Clients: Periodic

Re-Authentication Period (days): 1

9. Click **Add Network**.
10. Edit the added network and copy the portal URL.



Configure the following URL as captive portal in the initial role, to allow users sign in.

https://qa.agnieng.net/portal/Eba61d189-e361-4837-a116-182575420cfb/network/348

Configuring EOS

An administrator must also configure the Arista Switch for the guest workflow. Log in to the switch and add the following commands:

```
dot1x
   aaa accounting update interval 60 seconds
   mac based authentication hold period 300 seconds
   radius av-pair service-type
   mac-based-auth radius av-pair user-name delimiter none lowercase
   Captive-portal
!
```

```
ip access-list guest-acl
   10 permit udp any any eq bootps
   20 permit udp any any eq domain
   50 deny tcp any any copy captive-portal
   60 deny ip any any
!
```

Segments

Segments allow a way to provide differentiated access for the incoming access request. The segments comprise Status, Conditions, and Actions.

Status

The Segment status comprises Enable, Disable, and Monitor modes.

- **Enable** - Enables the segment configuration. Segment is evaluated and if the conditions match, then an appropriate action is returned as part of segment evaluation.
- **Disable** - Disables the segment configuration. Segment is not evaluated even if it is configured.
- **Monitor** - Sets up the segment in monitor mode only. The actions are ignored even if the conditions match. This is useful to evaluate the segment before rolling out to production.

Conditions

Conditions define rules based on various attributes associated with:

- RADIUS request
- Networks
- Clients
- Users
- Access Devices

The conditions are evaluated in the order of the configuration and they proceed to match all evaluation algorithms. The condition is evaluated to be true only if all the rules match.

Actions

Actions define the result that needs to be sent to access devices. The results can take various forms that are interpreted by the network access device. Actions can be formed through:

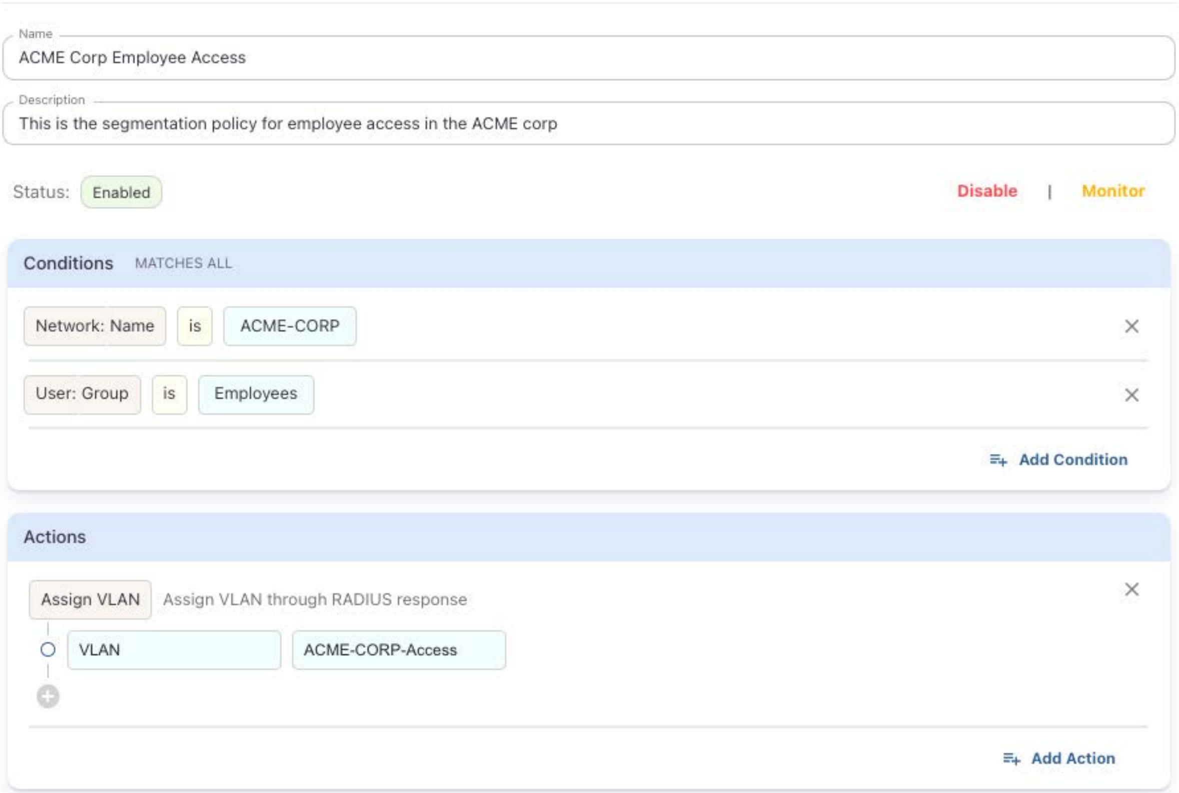
- VLAN assignment
- Application of ACLs
- Allow or deny helper access primitives
- Standard RADIUS attributes
- VSAs

Configuration

1. Navigate to **Access Control** → **Segments**. Click on the **Add Segment** button.
2. Enter **Name** and **Description**.
3. Add **Conditions**.
4. Add **Actions**.
5. Click on **Add Segment** to save the segment.

Sample Segments

Here is a sample of the Employee Access Segment policy for reference:



Name: ACME Corp Employee Access

Description: This is the segmentation policy for employee access in the ACME corp

Status: Enabled

Conditions MATCHES ALL

Network: Name is ACME-CORP

User: Group is Employees

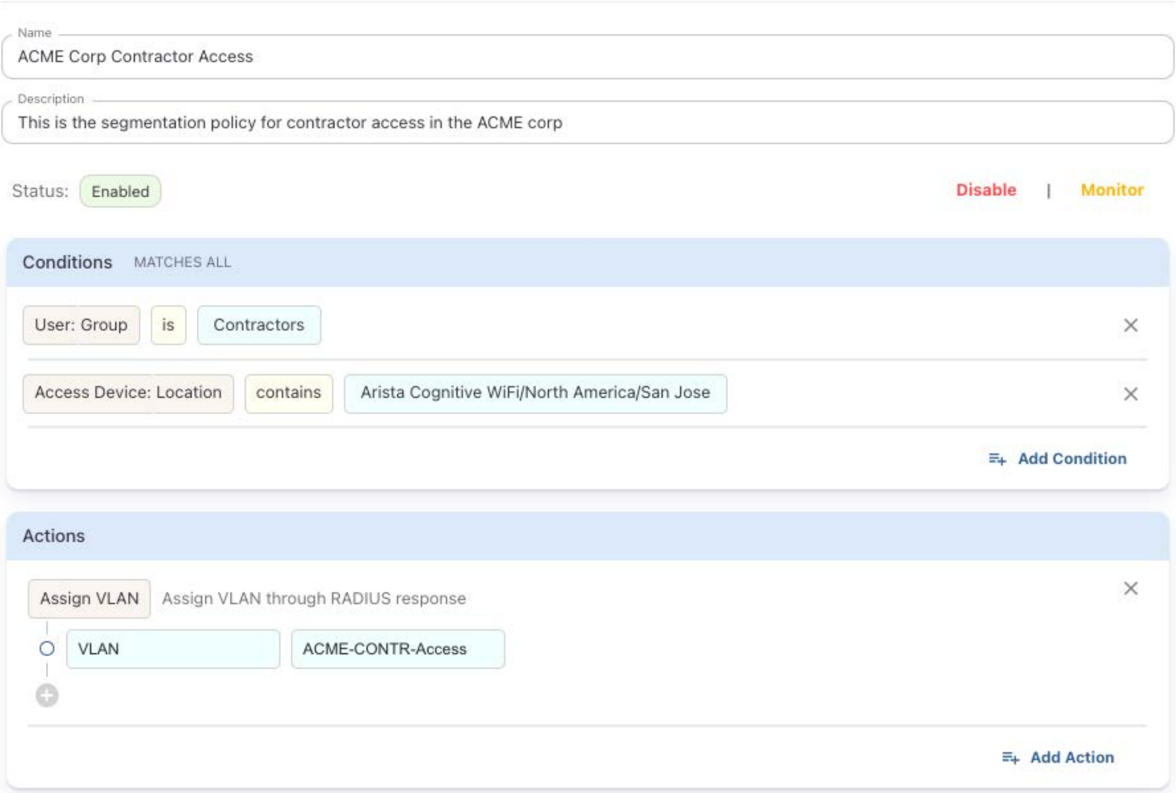
Actions

Assign VLAN Assign VLAN through RADIUS response

VLAN ACME-CORP-Access

Figure: Employee Access Segment Policy

Sample Contractor Access Segment



Name
ACME Corp Contractor Access

Description
This is the segmentation policy for contractor access in the ACME corp

Status: Enabled

Conditions MATCHES ALL

User: Group is Contractors

Access Device: Location contains Arista Cognitive WiFi/North America/San Jose

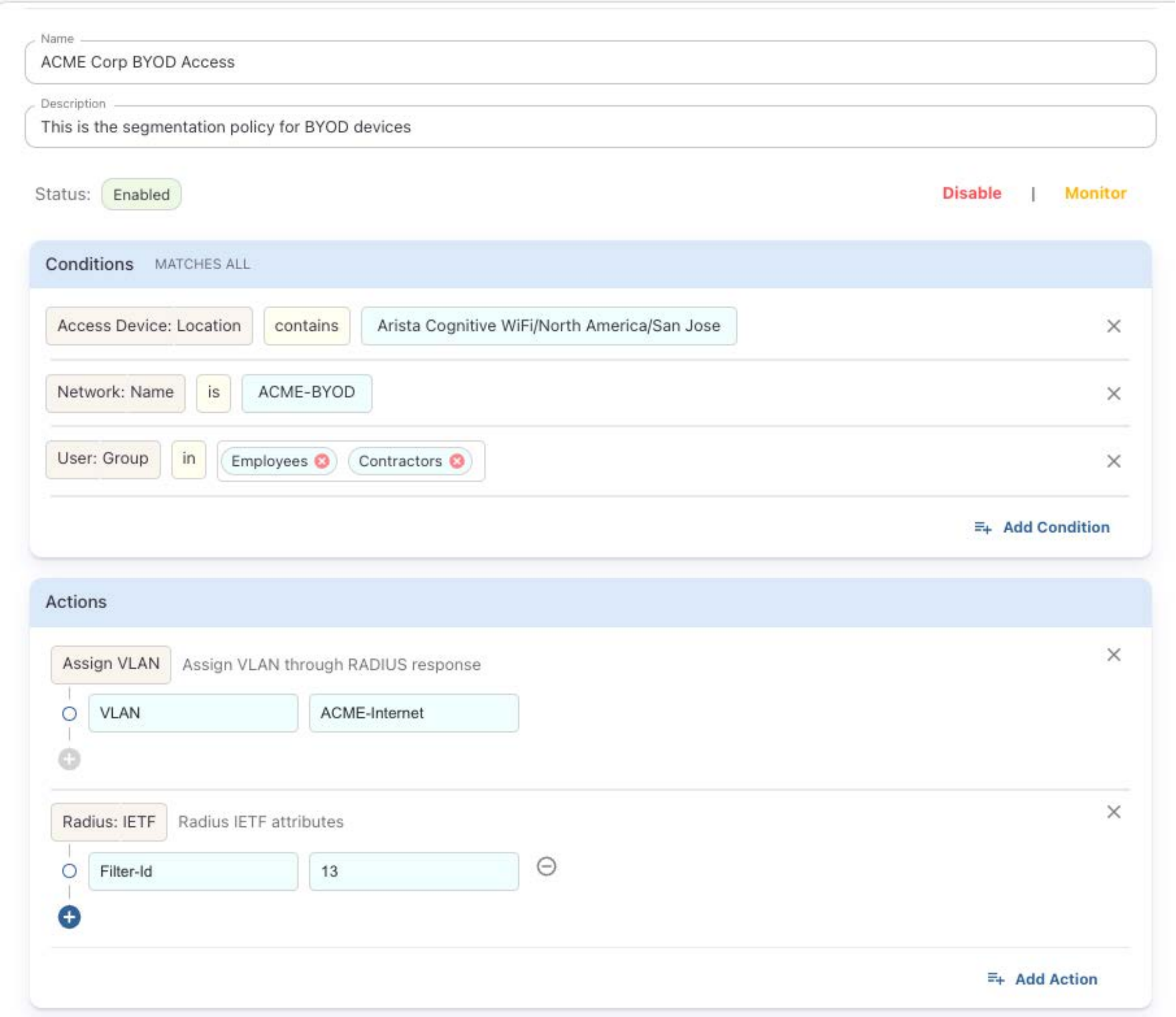
Actions

Assign VLAN Assign VLAN through RADIUS response

VLAN ACME-CONTR-Access

Figure: Contractor Access Segment Policy

Sample BYOD Access Segment



Name: ACME Corp BYOD Access

Description: This is the segmentation policy for BYOD devices

Status: Enabled

Conditions MATCHES ALL

Access Device: Location contains Arista Cognitive WiFi/North America/San Jose

Network: Name is ACME-BYOD

User: Group in Employees Contractors

Actions

Assign VLAN Assign VLAN through RADIUS response

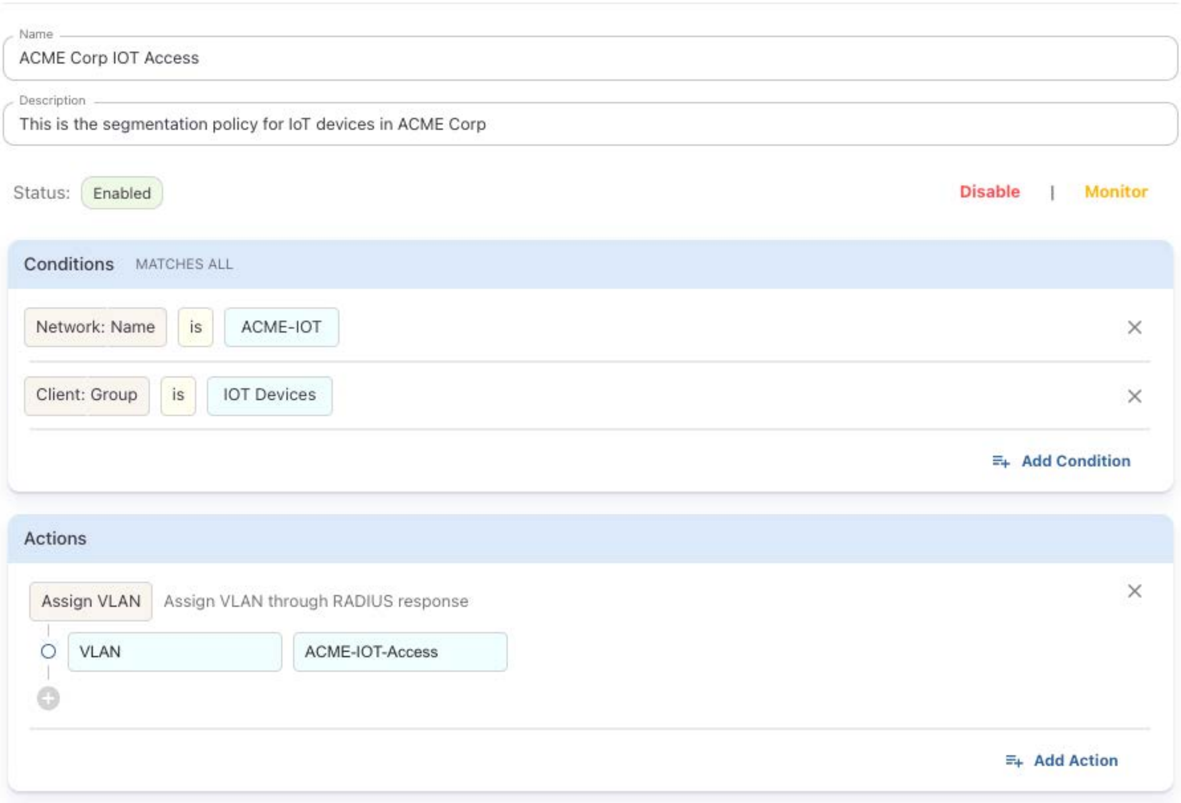
VLAN ACME-Internet

Radius: IETF Radius IETF attributes

Filter-Id 13

Figure: BYOD Access Segment Policy

Sample IOT Access Segment



Name
ACME Corp IOT Access

Description
This is the segmentation policy for IoT devices in ACME Corp

Status: Enabled

Conditions MATCHES ALL

Network: Name is ACME-IOT

Client: Group is IOT Devices

Actions

Assign VLAN Assign VLAN through RADIUS response

VLAN ACME-IOT-Access

Figure: IOT Access Segment Policy

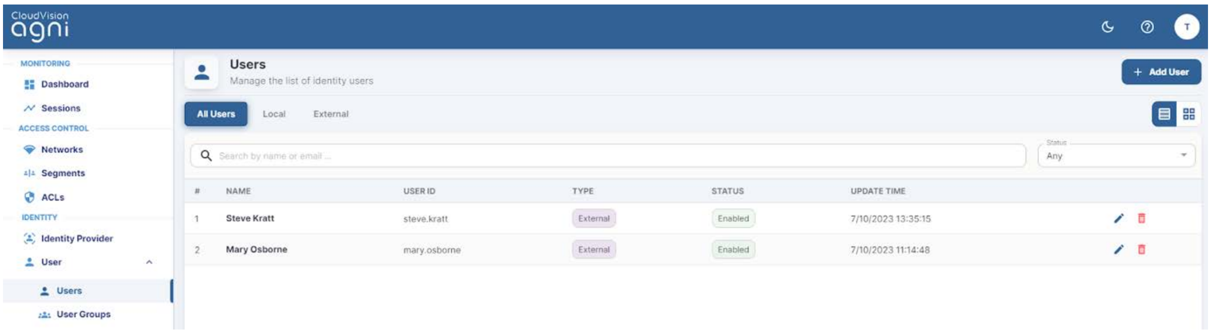
User Configurations

Users

Admin can manage local and external users from the **Users** tab. External users correspond to the users in external identity providers while the local users are those within AGNI's local identity provider.

External Users

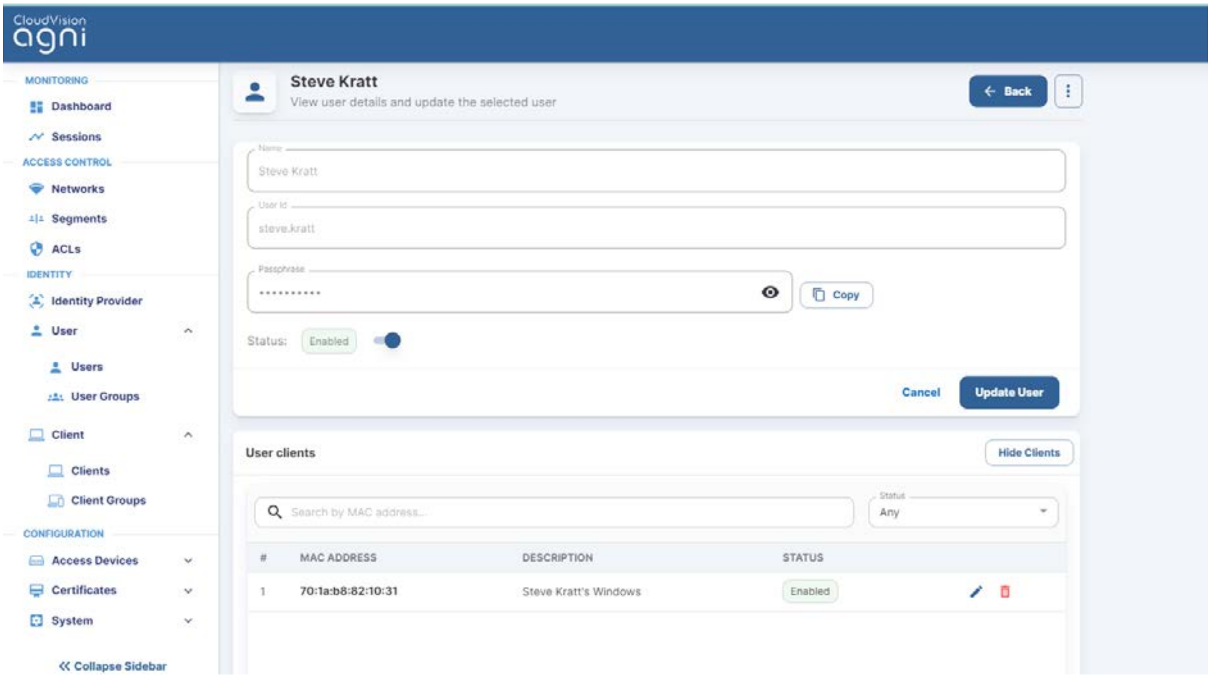
AGNI synchronizes the users in external IDPs (eg: Azure AD, Okta, OneLogin, and others) along with user attributes and group memberships. The users are marked external in the user's listing.



#	NAME	USER ID	TYPE	STATUS	UPDATE TIME
1	Steve Kratt	steve.kratt	External	Enabled	7/10/2023 13:35:15
2	Mary Osborne	mary.osborne	External	Enabled	7/10/2023 11:14:48

Figure: External Users

Admin can enable or disable the status of these users if IDP sync is disabled. If the sync is enabled, then the user status configured in IDPs is reflected in AGNI. Also, the admin can manage the devices logged in using this username.



Name: Steve Kratt

User Id: steve.kratt

Passphrase: ••••••••••

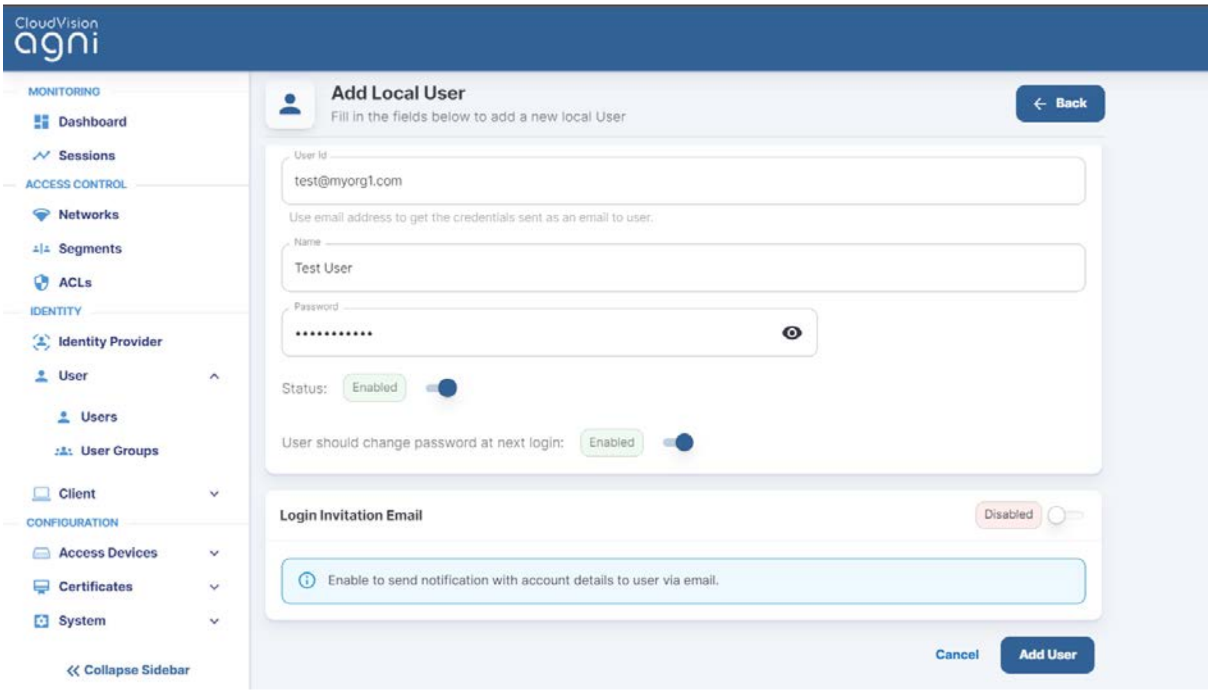
Status: Enabled

#	MAC ADDRESS	DESCRIPTION	STATUS
1	70:1a:b8:82:10:31	Steve Kratt's Windows	Enabled

Figure: External User Updation

Local User

Local users are managed within AGNI and can be used for any of the product workflows to locally authenticate with the system. The emails are sent by AGNI only if the Login **Invitation Email** option is enabled.



Add Local User

Fill in the fields below to add a new local User

User Id: test@myorg1.com

Use email address to get the credentials sent as an email to user.

Name: Test User

Password: •••••••••••

Status: Enabled

User should change password at next login: Enabled

Login Invitation Email: Disabled

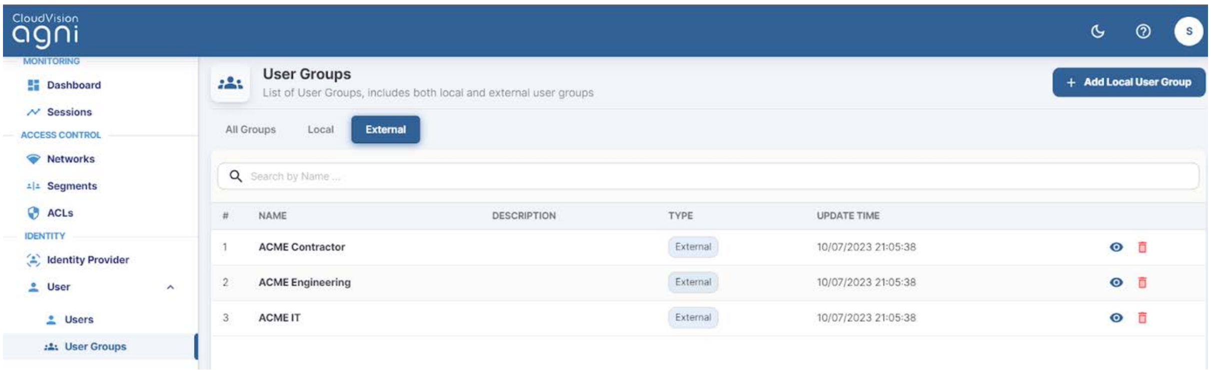
Enable to send notification with account details to user via email.

Figure: Local Users Addition

User Groups

User Groups facilitate the management of external and local groups. External groups are managed through external IDP and local groups are managed locally on the system. User Groups can be used in the segmentation policies to authorize the users into the network.

External User Groups are synchronized with the configured IDPs. These are managed externally. AGNI provides visibility of the group details in this interface. If an external user group needs to be deleted then Admin should remove it from the Available Groups in the IDP config. The changes are local to the system and not reflected in the external IDPs.



User Groups

List of User Groups, includes both local and external user groups

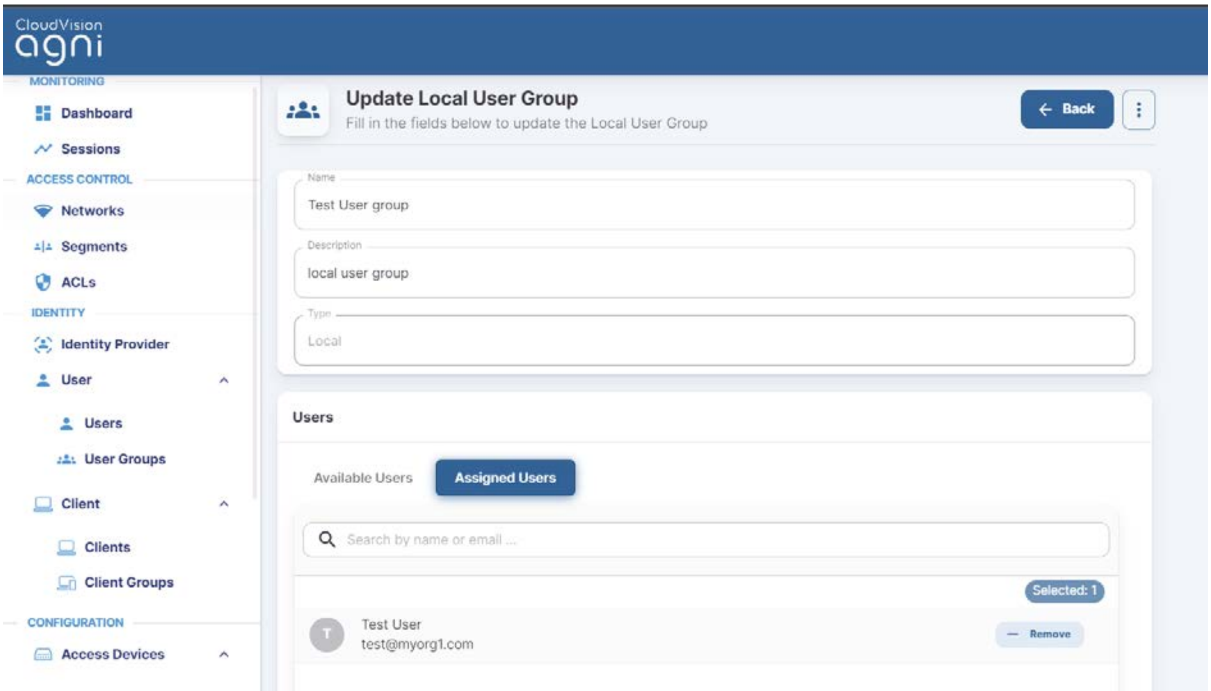
#	NAME	DESCRIPTION	TYPE	UPDATE TIME
1	ACME Contractor		External	10/07/2023 21:05:38
2	ACME Engineering		External	10/07/2023 21:05:38
3	ACME IT		External	10/07/2023 21:05:38

Figure: External User Groups

Local User Groups

Local User Groups provide the ability for administrators to manage the users within local group membership. With this, you can map local users with the configured local user group.

As this is managed locally in the system, the administrators can add, modify, and delete these entities.



Update Local User Group

Fill in the fields below to update the Local User Group

Name: Test User group

Description: local user group

Type: Local

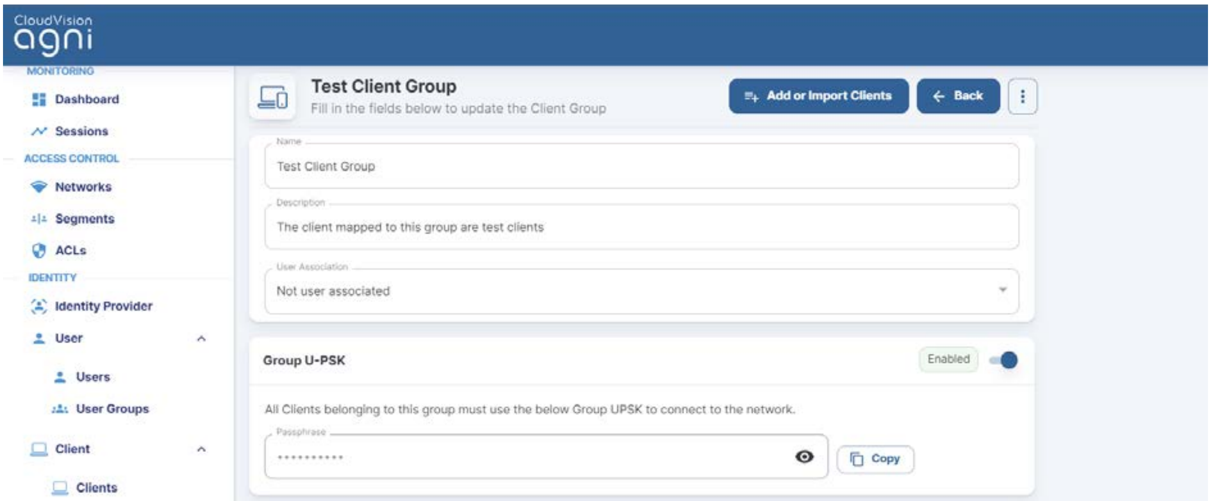
Users

Test User
test@myorg1.com

Figure: Local User Groups

Client Configuration

- **Client Groups** - Client Groups manage the client devices that are being authenticated by AGNI. The clients can be added either manually or dynamically by the system.
- **Group UPSK** - Client Groups can be defined within a Group UPSK, which can be used to onboard the desired client devices in that specific group.



Test Client Group

Fill in the fields below to update the Client Group

Name: Test Client Group

Description: The client mapped to this group are test clients

User Association: Not user associated

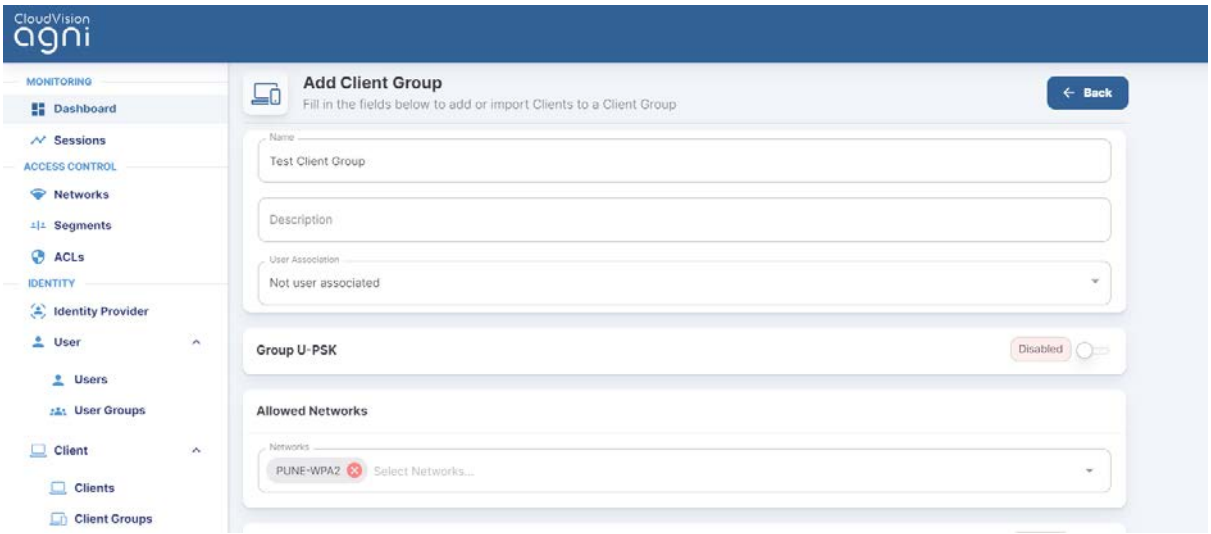
Group U-PSK: Enabled

All Clients belonging to this group must use the below Group UPSK to connect to the network.

Passphrase: ••••••••••

Figure: Client Group UPSK

- **Allowed Networks** - The network access to the clients under the group can be controlled by specifying the **Allowed Network** option.



Add Client Group

Fill in the fields below to add or import Clients to a Client Group

Name: Test Client Group

Description

User Association: Not user associated

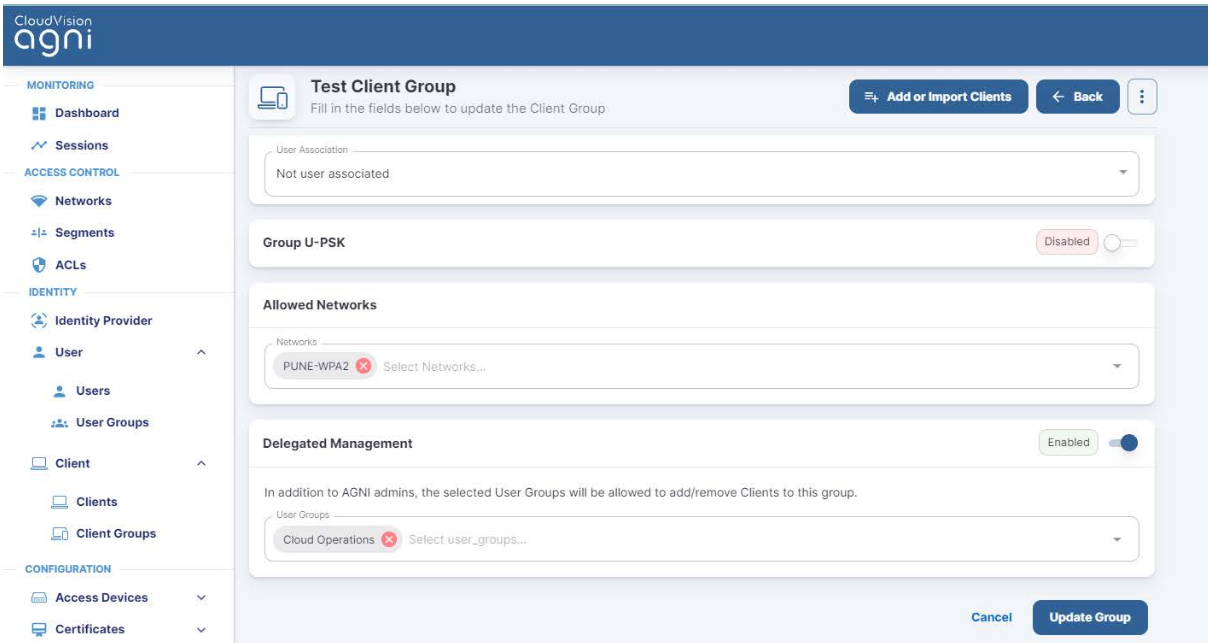
Group U-PSK: Disabled

Allowed Networks

Networks: PUNE-WPA2 Select Networks...

Figure: Client Group Allowed Network

- **Delegated Management** - The Client Group management can be delegated to a User Group that is specified under this setting. This is required if the administrator decides to delegate the responsibility of managing a specific set of client groups to specific users in an organization. This allows delegated administrators to add or remove clients from the group.



Test Client Group

Fill in the fields below to update the Client Group

User Association: Not user associated

Group U-PSK: Disabled

Allowed Networks

Networks: PUNE-WPA2 Select Networks...

Delegated Management: Enabled

In addition to AGNI admins, the selected User Groups will be allowed to add/remove Clients to this group.

User Groups: Cloud Operations Select user_groups...

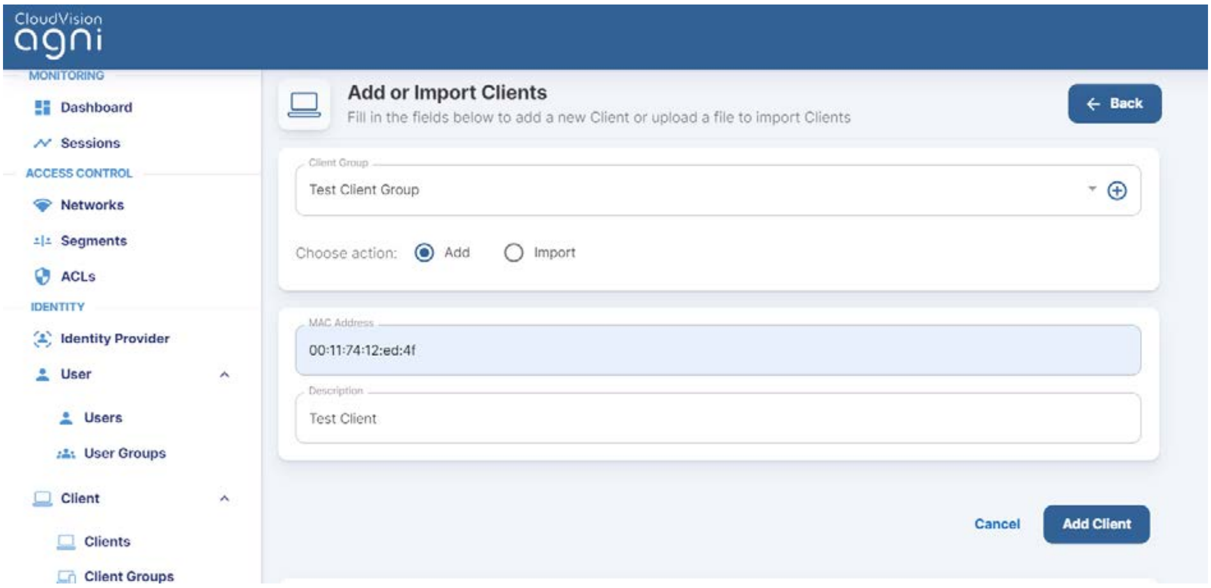
Figure: Client Group Delegated Management

Clients

The Clients section captures the endpoints in the following scenarios:

- Dynamically registered clients as part of authentication (eg: auto registered via UPSK)
- Manually registered clients as part of self registration
- Manually registered clients as part of user onboarding
- Clients synchronized as part of a Concourse application

The clients can also be imported or added into the system through the **Add Clients** or **Import Clients** option. The addition of the clients requires the MAC address of the clients, while import requires the client entries to be present in a .CSV file. A sample reference CSV file import template can be used to construct the client entries.



Add or Import Clients

Fill in the fields below to add a new Client or upload a file to import Clients

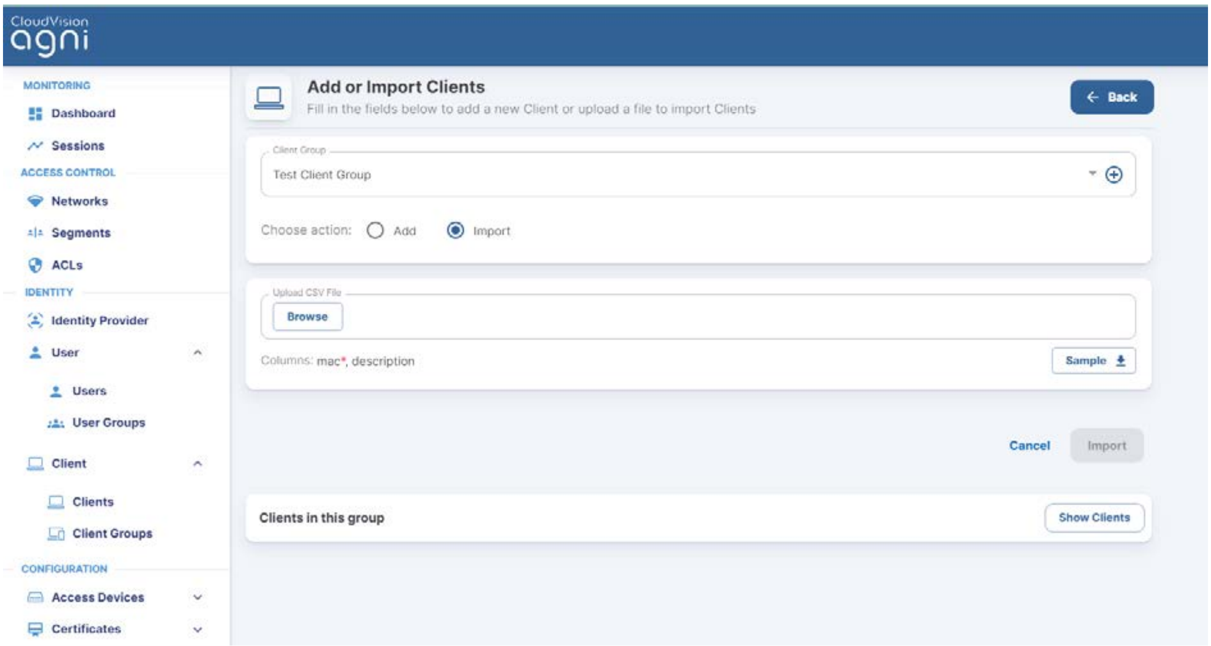
Client Group: Test Client Group

Choose action: ● Add ○ Import

MAC Address: 00:11:74:12:ed:4f

Description: Test Client

Figure: Client Addition



Add or Import Clients

Fill in the fields below to add a new Client or upload a file to import Clients

Client Group: Test Client Group

Choose action: ○ Add ● Import

Upload CSV File

Columns: mac*, description

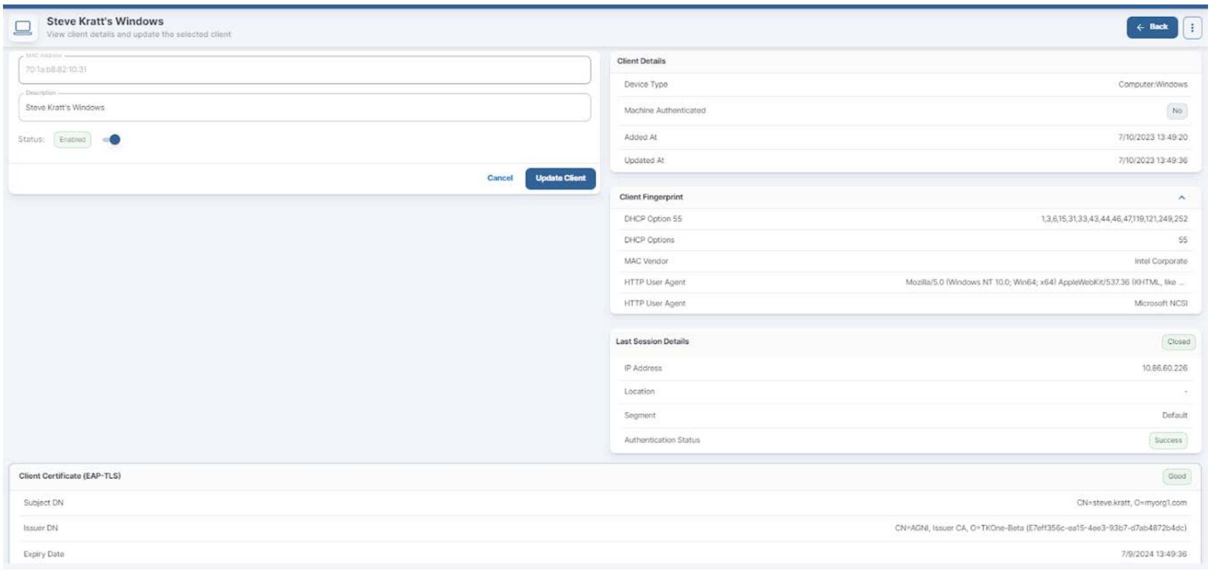
Clients in this group

Figure: Client Import

Client Details

Click on the clients to display the client details:

- **Client Information** – Displays MAC address, description, client group, passphrase, and status
- **Client Attributes** – Displays custom attributes associated with the client if available
- **Client Details** – Displays client device classification details
- **Client Fingerprint** – Displays the DHCP, MAC OUI, and User Agent fingerprinting information if available
- **Last Session Details** – Displays the details about the last client connectivity to the network
- **Network** – Displays the Network details
- **Access Device** – Displays the Client connection to the access device and its details
- **Sessions** – Displays the current and past sessions associated with the client
- **Client Activity** – Displays the Client activity present if there is a CoA activity for the client



Steve Kratt's Windows

View client details and update the selected client

MAC Address: 70:1a:b8:82:10:31

Description: Steve Kratt's Windows

Status: Enabled

Client Details

Device Type	Computer:Windows
Machine Authenticated	No
Added At	7/10/2023 13:49:20
Updated At	7/10/2023 13:49:36

Client Fingerprint

DHCP Option 55	1,3,6,15,31,33,43,44,46,47,119,121,249,252
DHCP Options	55
MAC Vendor	Intel Corporate
HTTP User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like ...
HTTP User Agent	Microsoft NCSI

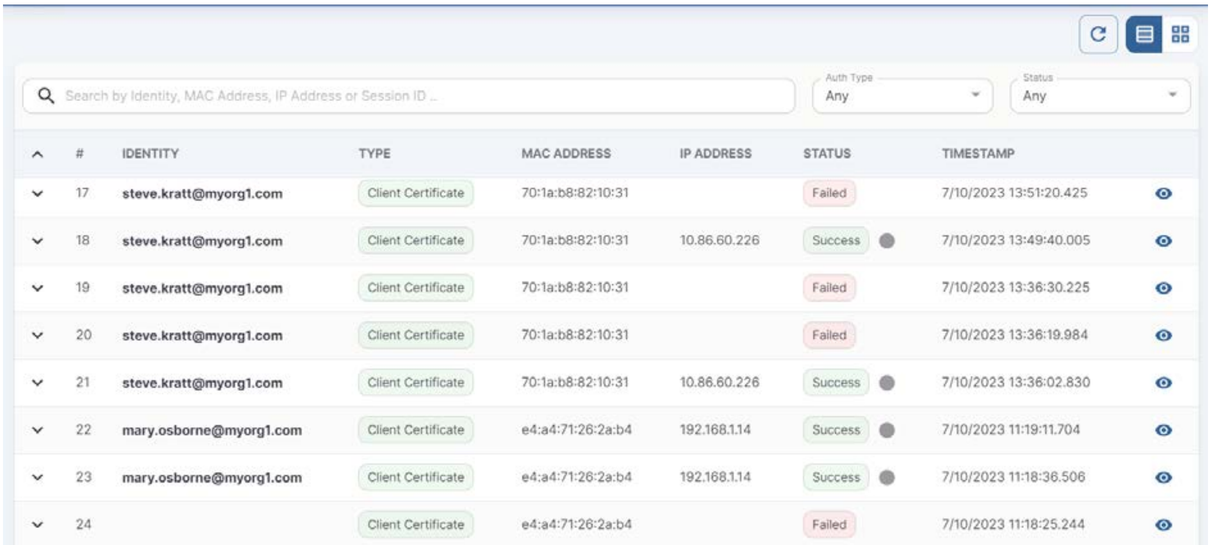
Last Session Details Closed

IP Address	10.86.60.226
Location	-
Segment	Default
Authentication Status	Success

Client Certificate (EAP-TLS) Good

Subject DN	CN=steve.kratt, O=myorg1.com
Issuer DN	CN=AGNI, Issuer CA, O=TKOne-Beta (E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc)
Expiry Date	7/9/2024 13:49:36

Figure: Client Details



Search by Identity, MAC Address, IP Address or Session ID ...

Auth Type: Any

Status: Any

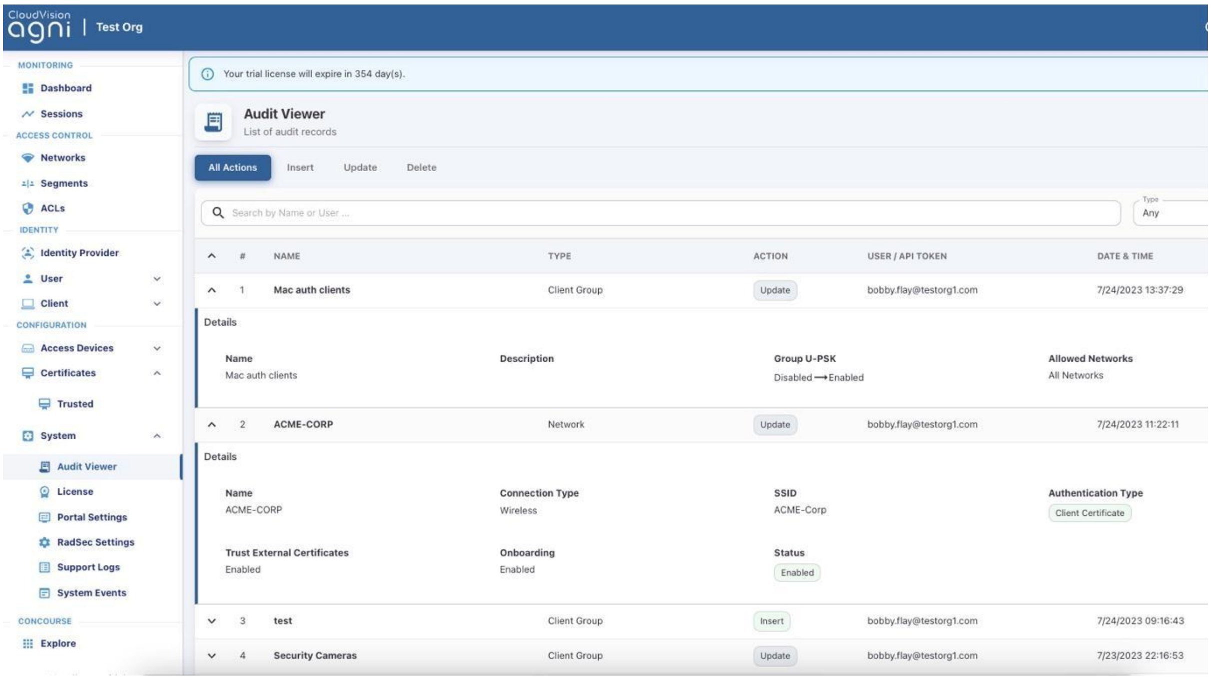
#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
17	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31		Failed	7/10/2023 13:51:20.425
18	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31	10.86.60.226	Success ●	7/10/2023 13:49:40.005
19	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31		Failed	7/10/2023 13:36:30.225
20	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31		Failed	7/10/2023 13:36:19.984
21	steve.kratt@myorg1.com	Client Certificate	70:1a:b8:82:10:31	10.86.60.226	Success ●	7/10/2023 13:36:02.830
22	mary.osborne@myorg1.com	Client Certificate	e4:a4:71:26:2a:b4	192.168.1.14	Success ●	7/10/2023 11:19:11.704
23	mary.osborne@myorg1.com	Client Certificate	e4:a4:71:26:2a:b4	192.168.1.14	Success ●	7/10/2023 11:18:36.506
24		Client Certificate	e4:a4:71:26:2a:b4		Failed	7/10/2023 11:18:25.244

Figure: Client sessions

System

This section captures the administrative tasks at the system level.

- **Audit Viewer**: Captures details about system configuration modifications. This helps to track any changes performed on the system along with the owner, modified details and timestamp.



Your trial license will expire in 354 day(s).

Audit Viewer

List of audit records

Type: Any

#	NAME	TYPE	ACTION	USER / API TOKEN	DATE & TIME
1	Mac auth clients	Client Group	Update	bobby.flay@testorg1.com	7/24/2023 13:37:29
2	ACME-CORP	Network	Update	bobby.flay@testorg1.com	7/24/2023 11:22:11
3	test	Client Group	Insert	bobby.flay@testorg1.com	7/24/2023 09:16:43
4	Security Cameras	Client Group	Update	bobby.flay@testorg1.com	7/23/2023 22:16:53

Details (1)

Name: Mac auth clients

Description:

Group U-PSK: Disabled → Enabled

Allowed Networks: All Networks

Details (2)

Name: ACME-CORP

Connection Type: Wireless

SSID: ACME-Corp

Authentication Type: Client Certificate

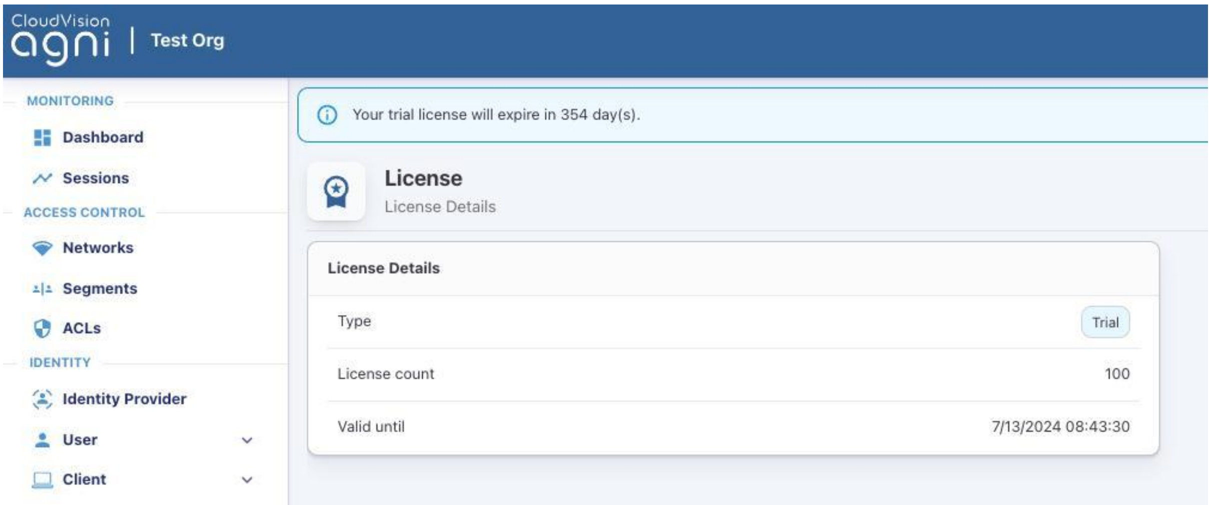
Trust External Certificates: Enabled

Onboarding: Enabled

Status: Enabled

Figure: Audit Viewer

- **License**: Displays the licensing information about the type, count, and validity period.



Your trial license will expire in 354 day(s).

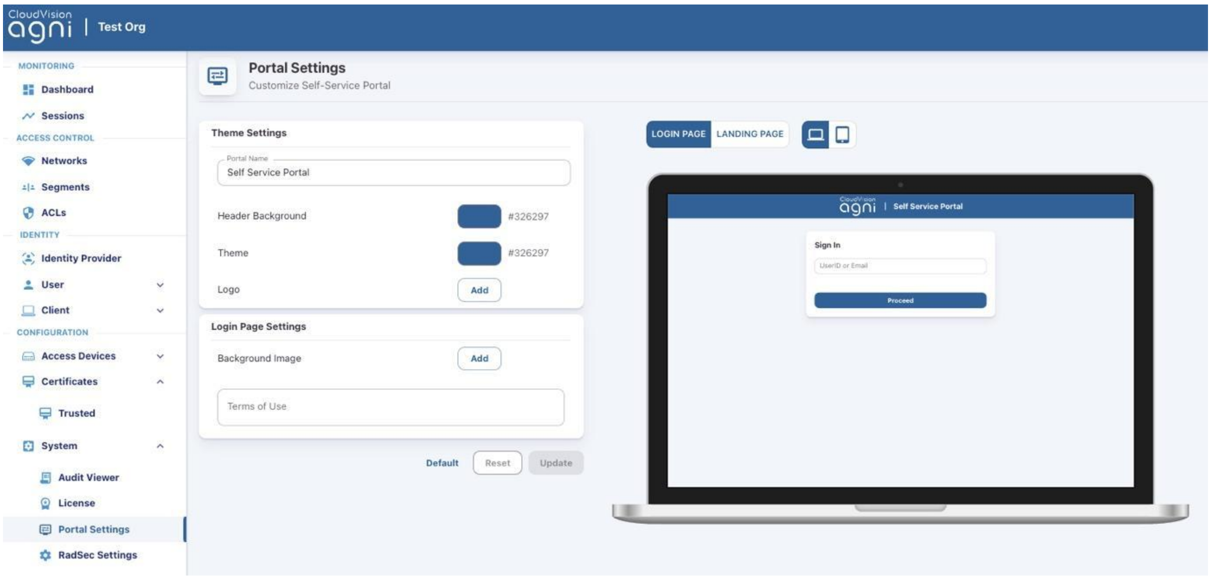
License Details

Type	Trial
License count	100
Valid until	7/13/2024 08:43:30

Figure: License

Portal Settings

The Portal Settings can be used to customize the Captive Portal network user experience. This allows customization of logo, text, images, and theme to be applied on the captive portal page for the organization's needs. The customization can be applied to landing as well as login pages.



Theme Settings

Portal Name: Self Service Portal

Header Background: #326297

Theme: #326297

Logo: Add

Login Page Settings

Background Image: Add

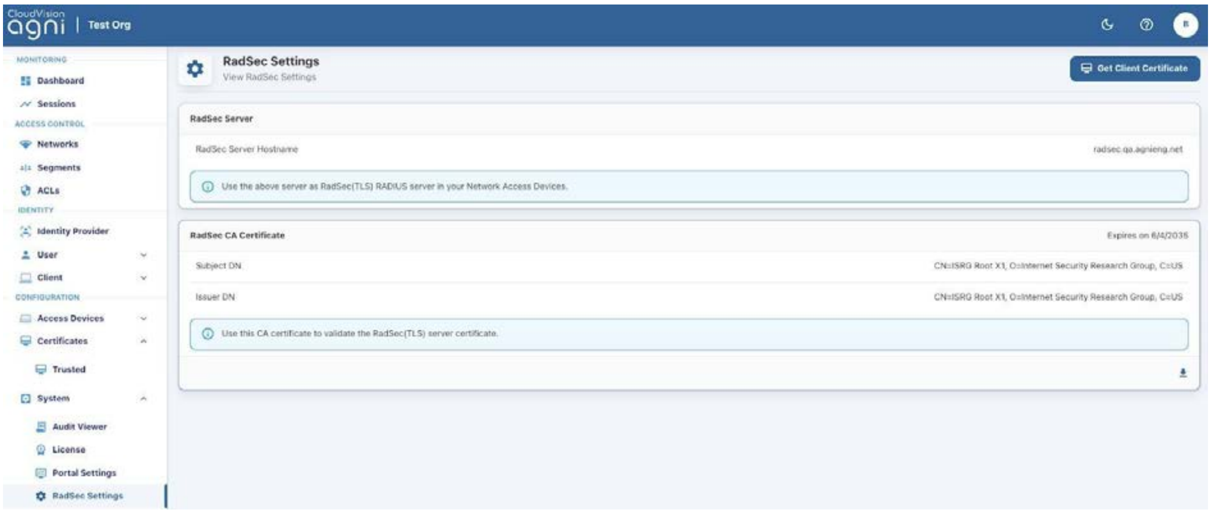
Terms of Use

Default Reset Update

Figure: Portal Settings

RadSec Settings

The RadSec certificate of the system can be viewed and downloaded from **Configuration** → **System** → **RadSec Settings**. Import the certificate into the network access devices for the successful establishment of the RadSec tunnel.



RadSec Settings
View RadSec Settings

RadSec Server

RadSec Server Hostname: radsec.qa.agnieng.net

Use the above server as RadSec(TLS) RADIUS server in your Network Access Devices.

RadSec CA Certificate — Expires on 6/4/2035

Subject DN: CN=ISRG Root X1, O=Internet Security Research Group, C=US

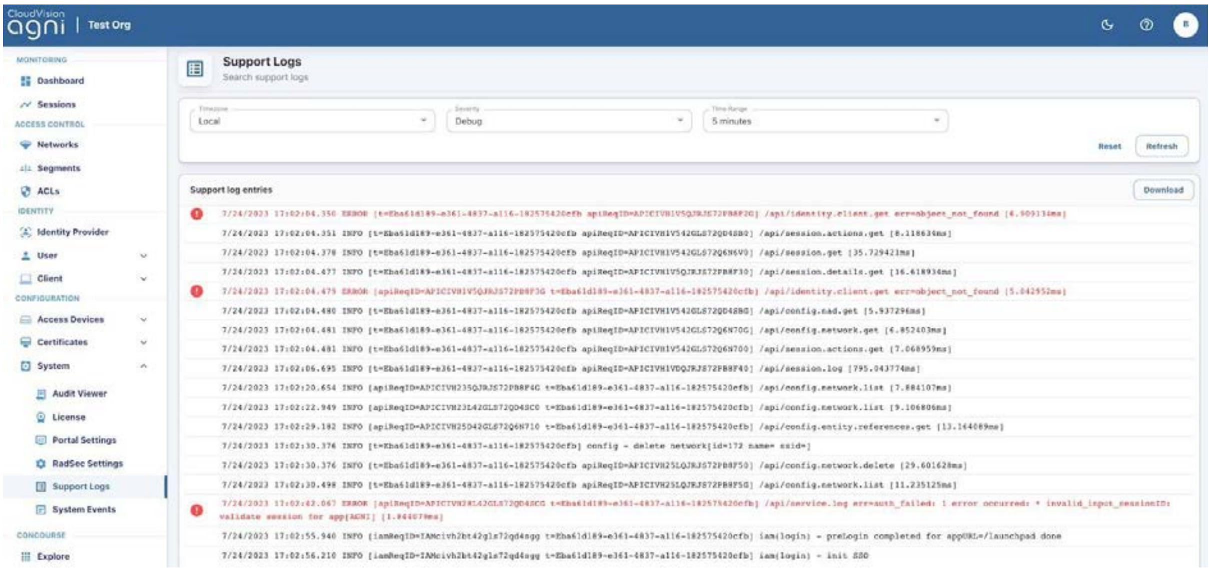
Issuer DN: CN=ISRG Root X1, O=Internet Security Research Group, C=US

Use this CA certificate to validate the RadSec(TLS) server certificate.

Figure: RadSec Settings

Support Logs

The Support Logs section provides the ability to view and download the system logs for the specified duration that can be used to analyze the system operations. The logs are displayed from various services running as part of the system operation and can be used for troubleshooting purposes.



Support Logs
Search support logs

Timezone: Local
Severity: Debug
Time Range: 5 minutes

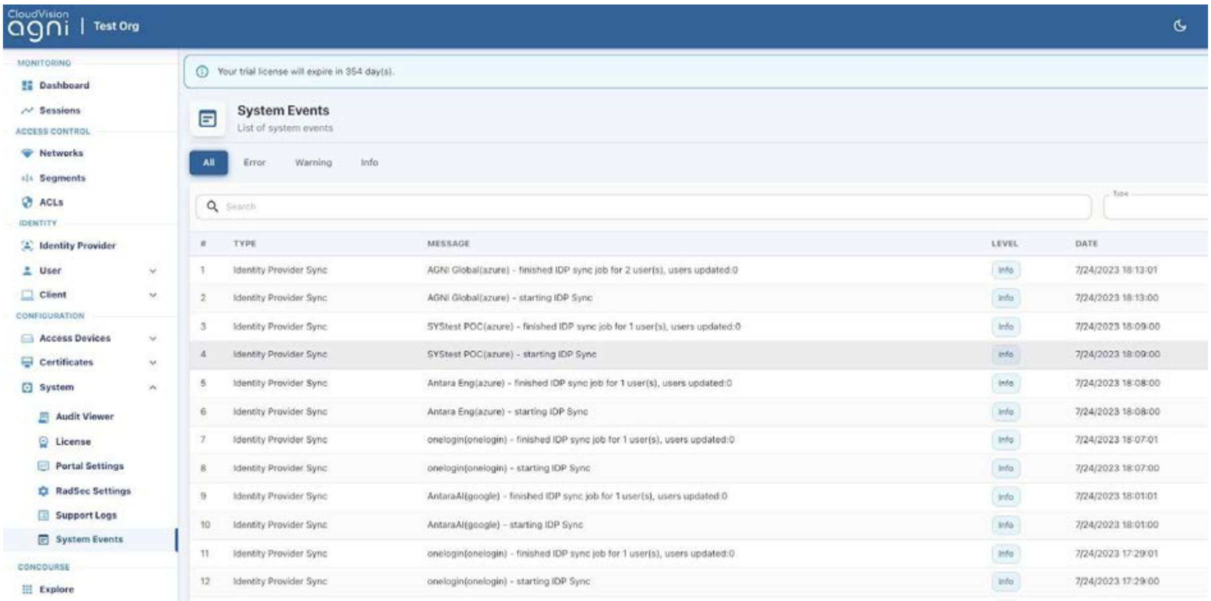
Support log entries

```
7/24/2023 17:02:04.350 ERROR [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V5QJRJS72PB8F2G] /api/identity.client.get err=object_not_found [6.909134ms]
7/24/2023 17:02:04.351 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V542GLS72QD48B0] /api/session.actions.get [8.118634ms]
7/24/2023 17:02:04.378 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V542GLS72Q6N6V0] /api/session.get [35.729421ms]
7/24/2023 17:02:04.477 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V5QJRJS72PB8F30] /api/session.details.get [16.618934ms]
7/24/2023 17:02:04.479 ERROR [apiReqID=APICIVH1V5QJRJS72PB8F3G t=Eba61d189-e361-4837-a116-182575420cfb] /api/identity.client.get err=object_not_found [5.042952ms]
7/24/2023 17:02:04.480 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V542GLS72QD48BG] /api/config.nad.get [5.937296ms]
7/24/2023 17:02:04.481 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V542GLS72Q6N70G] /api/config.network.get [6.852403ms]
7/24/2023 17:02:04.481 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1V542GLS72Q6N700] /api/session.actions.get [7.068959ms]
7/24/2023 17:02:06.695 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH1VDQJRJS72PB8F40] /api/session.log [795.043774ms]
7/24/2023 17:02:20.654 INFO [apiReqID=APICIVH23SQJRJS72PB8F4G t=Eba61d189-e361-4837-a116-182575420cfb] /api/config.network.list [7.884107ms]
7/24/2023 17:02:22.949 INFO [apiReqID=APICIVH23L42GLS72QD4SC0 t=Eba61d189-e361-4837-a116-182575420cfb] /api/config.network.list [9.106806ms]
7/24/2023 17:02:29.182 INFO [apiReqID=APICIVH25D42GLS72Q6N710 t=Eba61d189-e361-4837-a116-182575420cfb] /api/config.entity.references.get [13.164089ms]
7/24/2023 17:02:30.376 INFO [t=Eba61d189-e361-4837-a116-182575420cfb] config - delete network[id=172 name= ssid=]
7/24/2023 17:02:30.376 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH25LQJRJS72PB8F50] /api/config.network.delete [29.601628ms]
7/24/2023 17:02:30.498 INFO [t=Eba61d189-e361-4837-a116-182575420cfb apiReqID=APICIVH25LQJRJS72PB8F5G] /api/config.network.list [11.235125ms]
7/24/2023 17:02:42.067 ERROR [apiReqID=APICIVH28L42GLS72QD4SCG t=Eba61d189-e361-4837-a116-182575420cfb] /api/service.log err=auth_failed: 1 error occurred: * invalid_input_sessionID:
validate session for app[AGNI] [1.844079ms]
7/24/2023 17:02:55.940 INFO [iamReqID=IAMcivh2bt42gls72qd4sgg t=Eba61d189-e361-4837-a116-182575420cfb] iam(login) - preLogin completed for appURL=/launchpad done
7/24/2023 17:02:56.210 INFO [iamReqID=IAMcivh2bt42gls72qd4sgg t=Eba61d189-e361-4837-a116-182575420cfb] iam(login) - init SSO
```

Figure: Support Logs

System Events

Various events recorded by the services are logged under System Events. They provide information, warnings, or error messages related to the system operation. Remediation action can be taken if necessary.



Your trial license will expire in 354 day(s).

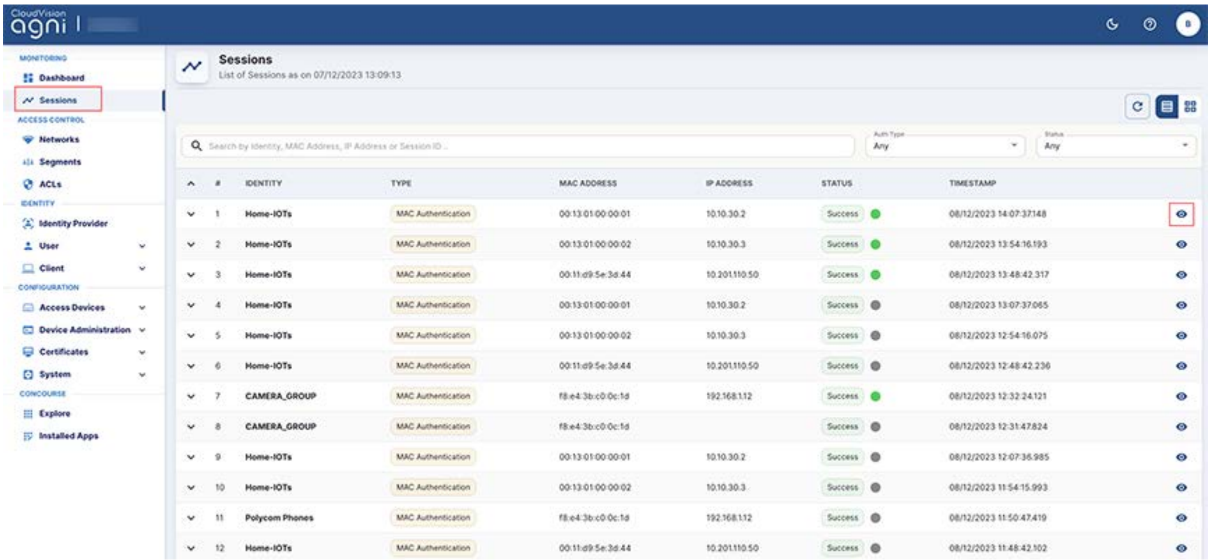
System Events
List of system events

#	TYPE	MESSAGE	LEVEL	DATE
1	Identity Provider Sync	AGNI Global(azure) - finished IDP sync job for 2 user(s), users updated:0	Info	7/24/2023 18:13:01
2	Identity Provider Sync	AGNI Global(azure) - starting IDP Sync	Info	7/24/2023 18:13:00
3	Identity Provider Sync	SYStest POC(azure) - finished IDP sync job for 1 user(s), users updated:0	Info	7/24/2023 18:09:00
4	Identity Provider Sync	SYStest POC(azure) - starting IDP Sync	Info	7/24/2023 18:09:00
5	Identity Provider Sync	Antara Eng(azure) - finished IDP sync job for 1 user(s), users updated:0	Info	7/24/2023 18:08:00
6	Identity Provider Sync	Antara Eng(azure) - starting IDP Sync	Info	7/24/2023 18:08:00
7	Identity Provider Sync	onelogin(onelogin) - finished IDP sync job for 1 user(s), users updated:0	Info	7/24/2023 18:07:01
8	Identity Provider Sync	onelogin(onelogin) - starting IDP Sync	Info	7/24/2023 18:07:00
9	Identity Provider Sync	AntaraAI(google) - finished IDP sync job for 1 user(s), users updated:0	Info	7/24/2023 18:01:01
10	Identity Provider Sync	AntaraAI(google) - starting IDP Sync	Info	7/24/2023 18:01:00
11	Identity Provider Sync	onelogin(onelogin) - finished IDP sync job for 1 user(s), users updated:0	Info	7/24/2023 17:29:01
12	Identity Provider Sync	onelogin(onelogin) - starting IDP Sync	Info	7/24/2023 17:29:00

Figure : System Events

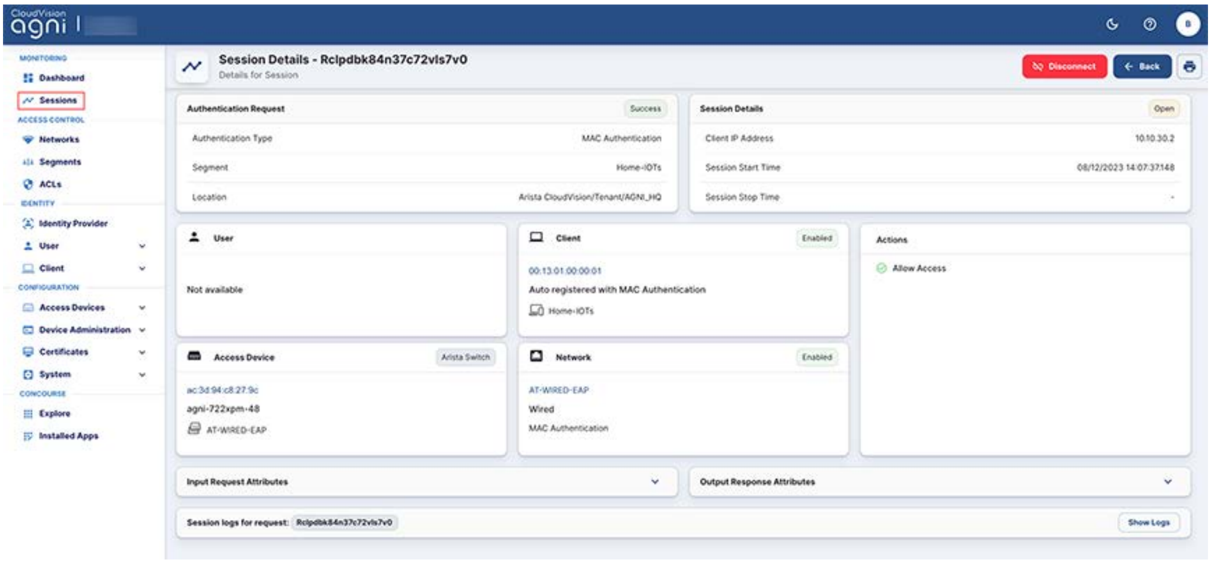
Sessions

This section provides you details on how to access and view the session details in AGNI. To access the Session details, navigate to Monitoring -> Sessions. The Sessions page displays a table with list of devices and the corresponding session details. Click the eye icon at the far right column to view the details of that session. (see images below)



Sessions
List of Sessions as on 07/12/2023 13:09:13

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success 🟢	08/12/2023 14:07:37.148
2	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success 🟢	08/12/2023 13:54:16.193
3	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success 🟢	08/12/2023 13:48:42.317
4	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success ●	08/12/2023 13:07:37.065
5	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success ●	08/12/2023 12:54:16.075
6	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success ●	08/12/2023 12:48:42.236
7	CAMERA_GROUP	MAC Authentication	f8:e4:3b:c0:0c:1d	192.168.1.12	Success 🟢	08/12/2023 12:32:24.121
8	CAMERA_GROUP	MAC Authentication	f8:e4:3b:c0:0c:1d		Success ●	08/12/2023 12:31:47.824
9	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success ●	08/12/2023 12:07:36.985
10	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success ●	08/12/2023 11:54:15.993
11	Polycom Phones	MAC Authentication	f8:e4:3b:c0:0c:1d	192.168.1.12	Success ●	08/12/2023 11:50:47.419
12	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success ●	08/12/2023 11:48:42.102



Session Details - Rclpdbk84n37c72vls7v0
Details for Session

Authentication Request — Success

Authentication Type	MAC Authentication
Segment	Home-IOTs
Location	Arista CloudVision/Tenant/AGNI_HQ

Session Details — Open

Client IP Address	10.10.30.2
Session Start Time	08/12/2023 14:07:37.148
Session Stop Time	-

User

Not available

Client — Enabled

00:13:01:00:00:01
Auto registered with MAC Authentication
Home-IOTs

Actions

Allow Access

Access Device — Arista Switch

ac:3d:94:c8:27:9c
agni-722xpm-48
AT-WIRED-EAP

Network — Enabled

AT-WIRED-EAP
Wired
MAC Authentication

Input Request Attributes

Output Response Attributes

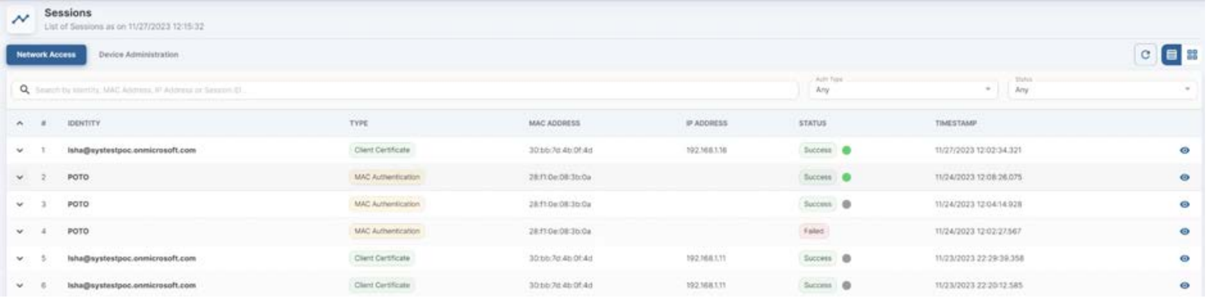
Session logs for request: Rclpdbk84n37c72vls7v0

On-Demand Disconnecting a Client from the Network

This section describes the steps to manually disconnect a client from the network. You must log in as a network admin user to perform the steps.

To disconnect a client device on-demand, navigate to the Sessions menu on the left pane of the dashboard and:

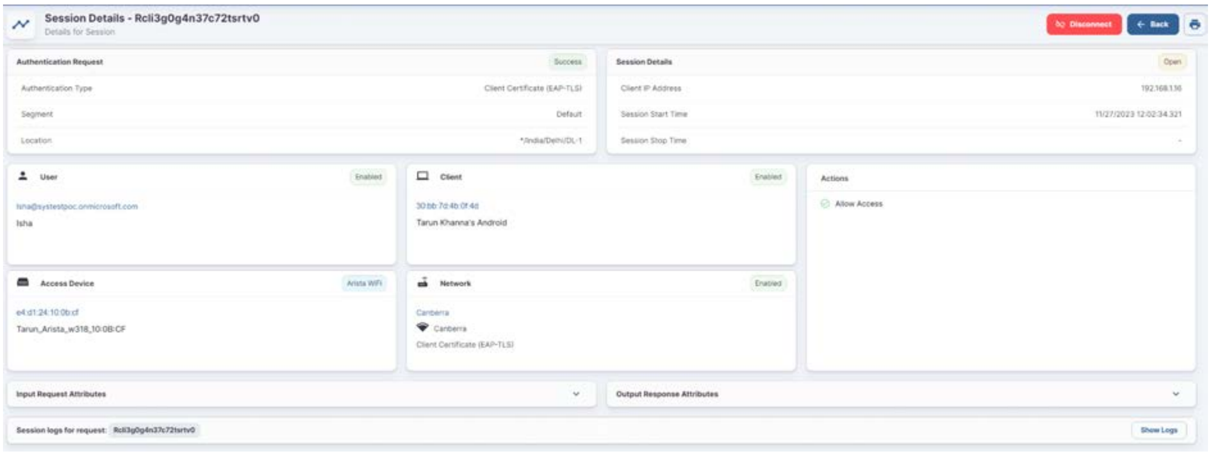
1. Open the client's active session (see image below).



Sessions
List of Sessions as on 11/27/2023 12:15:32

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	Isha@systestpoc.onmicrosoft.com	Client Certificate	30:bb:7d:4b:0f:4d	192.168.1.16	Success ●	11/27/2023 12:02:34.321
2	POTO	MAC Authentication	28:f1:0e:08:3b:0a		Success ●	11/24/2023 12:08:26.075
3	POTO	MAC Authentication	28:f1:0e:08:3b:0a		Success ●	11/24/2023 12:04:14.928
4	POTO	MAC Authentication	28:f1:0e:08:3b:0a		Failed	11/24/2023 12:02:27.567
5	Isha@systestpoc.onmicrosoft.com	Client Certificate	30:bb:7d:4b:0f:4d	192.168.1.11	Success ●	11/23/2023 22:29:39.358
6	Isha@systestpoc.onmicrosoft.com	Client Certificate	30:bb:7d:4b:0f:4d	192.168.1.11	Success ●	11/23/2023 22:20:12.585

2. Click the “**eye**” icon to open the active session details (see image below).



Session Details - Rcli3g0g4n37c72tsrtv0
Details for Session

Authentication Request	Success
Authentication Type	Client Certificate (EAP-TLS)
Segment	Default
Location	*/India/Delhi/DL-1

Session Details	Open
Client IP Address	192.168.1.16
Session Start Time	11/27/2023 12:02:34.321
Session Stop Time	-

User — Enabled
isha@systestpoc.onmicrosoft.com
Isha

Client — Enabled
30:bb:7d:4b:0f:4d
Tarun Khanna's Android

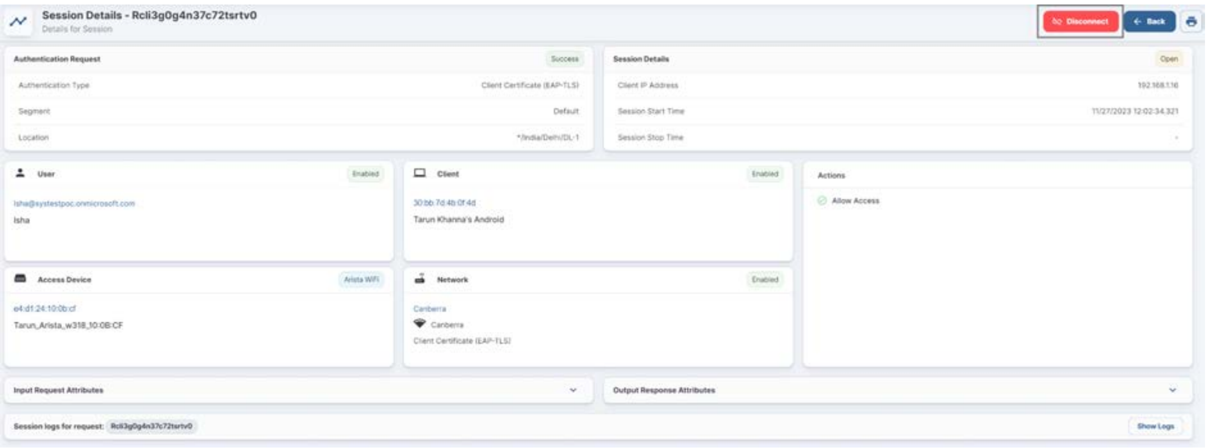
Actions
Allow Access

Access Device — Arista WiFi
e4:d1:24:10:0b:cf
Tarun_Arista_w318_10:0B:CF

Network — Enabled
Canberra
Canberra
Client Certificate (EAP-TLS)

Session logs for request: Rcli3g0g4n37c72tsrtv0

3. Click the **Disconnect** button.



Session Details - Rcli3g0g4n37c72tsrtv0
Details for Session

Authentication Request	Success
Authentication Type	Client Certificate (EAP-TLS)
Segment	Default
Location	*/India/Delhi/DL-1

Session Details	Open
Client IP Address	192.168.1.16
Session Start Time	11/27/2023 12:02:34.321
Session Stop Time	-

User — Enabled
isha@systestpoc.onmicrosoft.com
Isha

Client — Enabled
30:bb:7d:4b:0f:4d
Tarun Khanna's Android

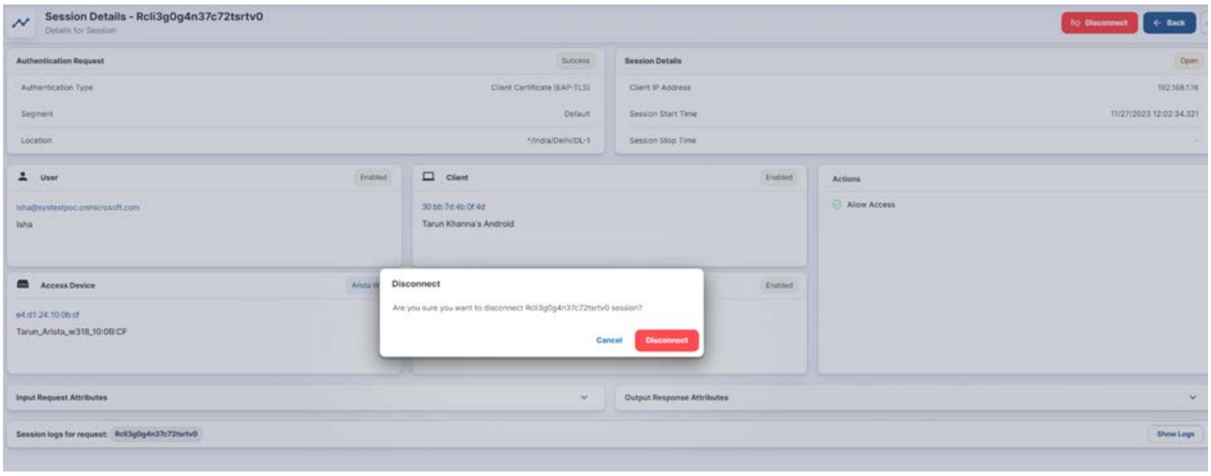
Actions
Allow Access

Access Device — Arista WiFi
e4:d1:24:10:0b:cf
Tarun_Arista_w318_10:0B:CF

Network — Enabled
Canberra
Canberra
Client Certificate (EAP-TLS)

Session logs for request: Rcli3g0g4n37c72tsrtv0

AGNI dashboard displays a confirmation message for admin approval (see image below).



Session Details - Rcli3g0g4n37c72tsrtv0
Details for Session

Authentication Request	Success
Authentication Type	Client Certificate (EAP-TLS)
Segment	Default
Location	*/India/Delhi/DL-1

Session Details	Open
Client IP Address	192.168.1.16
Session Start Time	11/27/2023 12:02:34.321
Session Stop Time	-

User — Enabled
isha@systestpoc.onmicrosoft.com
Isha

Client — Enabled
30:bb:7d:4b:0f:4d
Tarun Khanna's Android

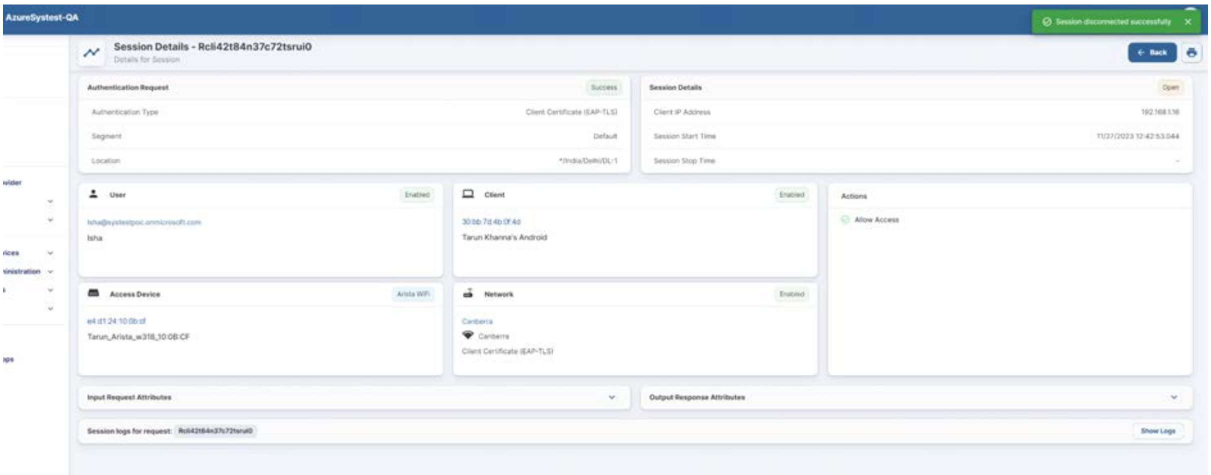
Actions
Allow Access

Access Device — Arista W
e4:d1:24:10:0b:cf
Tarun_Arista_w318_10:0B:CF

Disconnect
Are you sure you want to disconnect Rcli3g0g4n37c72tsrtv0 session?

Session logs for request: Rcli3g0g4n37c72tsrtv0

4. Click **Approve**.
   A Change of Authorization (COA) disconnect request is sent to the client device and the device gets disconnected from the network.



AzureSystest-QA

Session disconnected successfully

Session Details - Rcli42t84n37c72tsrui0

Details for Session

← Back

Authentication Request — Success

Authentication Type: Client Certificate (EAP-TLS)

Segment: Default

Location: */India/Delhi/DL-1

Session Details — Open

Client IP Address: 192.168.1.16

Session Start Time: 11/27/2023 12:42:53.044

Session Stop Time: -

User — Enabled

isha@systestpoc.onmicrosoft.com

Isha

Client — Enabled

30:bb:7d:4b:0f:4d

Tarun Khanna's Android

Actions

Allow Access

Access Device — Arista WiFi

e4:d1:24:10:0b:cf

Tarun_Arista_w318_10:0B:CF

Network — Enabled

Canberra

Canberra

Client Certificate (EAP-TLS)

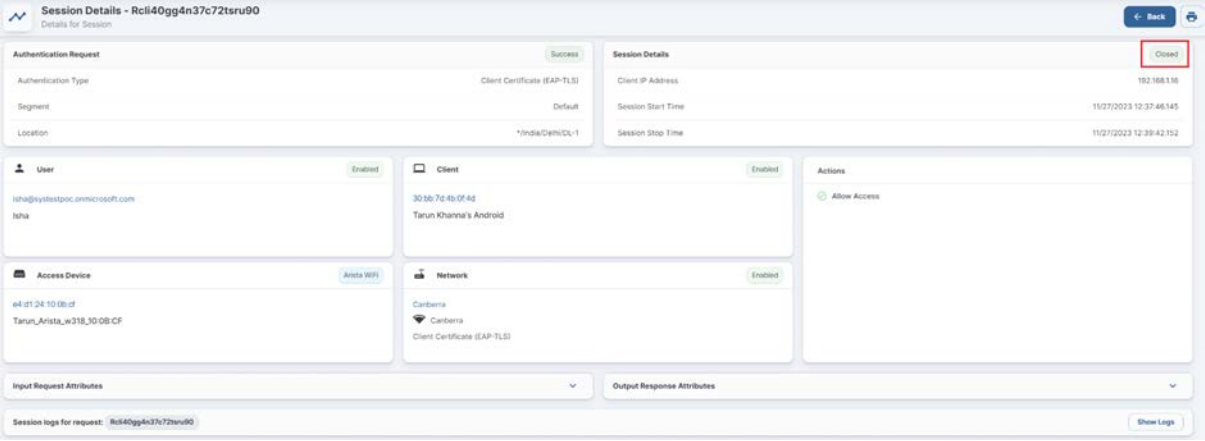
Input Request Attributes

Output Response Attributes

Session logs for request: Rcli42t84n37c72tsrui0

Show Logs

Now the client session status changes from **Open** to **Closed**.



Session Details - Rcli40gg4n37c72tsru90

Details for Session

← Back

Authentication Request — Success

Authentication Type: Client Certificate (EAP-TLS)

Segment: Default

Location: */India/Delhi/DL-1

Session Details — Closed

Client IP Address: 192.168.1.16

Session Start Time: 11/27/2023 12:37:46.145

Session Stop Time: 11/27/2023 12:39:42.152

User — Enabled

isha@systestpoc.onmicrosoft.com

Isha

Client — Enabled

30:bb:7d:4b:0f:4d

Tarun Khanna's Android

Actions

Allow Access

Access Device — Arista WiFi

e4:d1:24:10:0b:cf

Tarun_Arista_w318_10:0B:CF

Network — Enabled

Canberra

Canberra

Client Certificate (EAP-TLS)

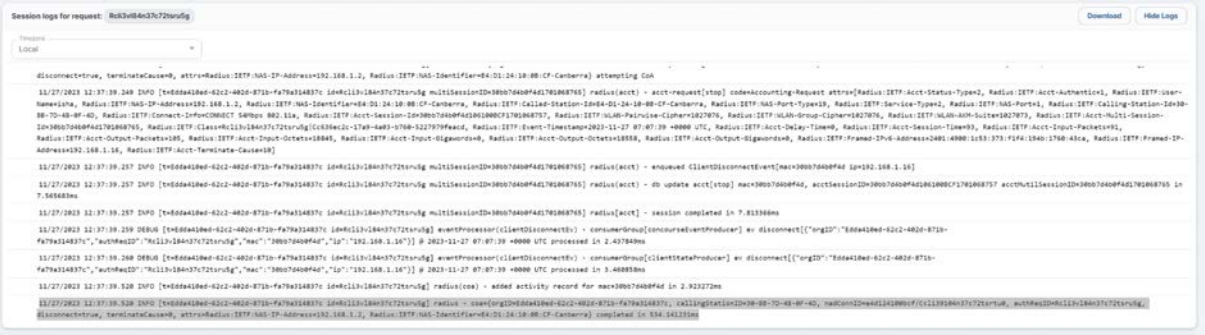
Input Request Attributes

Output Response Attributes

Session logs for request: Rcli40gg4n37c72tsru90

Show Logs

Note: You can verify the CoA disconnect logs from the AGNI debug logs file (see the image below).



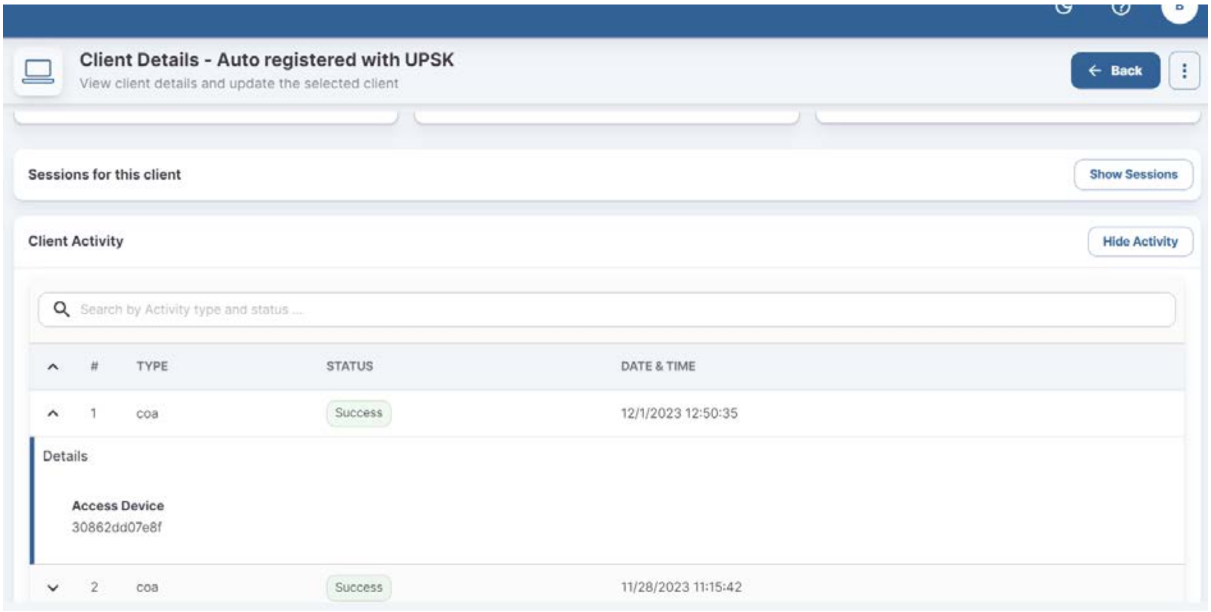
Session logs for request: Rcli3vl84n37c72tsru5g

Download | Hide Logs

Timezone: Local

```
disconnect=true, terminateCause=0, attrs=Radius:IETF:NAS-IP-Address=192.168.1.2, Radius:IETF:NAS-Identifier=E4:D1:24:10:0B:CF-Canberra) attempting CoA

11/27/2023 12:37:39.249 INFO [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g multiSessionID=30bb7d4b0f4d1701068765] radius(acct) - acct-request[stop] code=Accounting-Request attrs=[Radius:IETF:Acct-Status-Type=2, Radius:IETF:Acct-Authentic=1, Radius:IETF:User-
Name=isha, Radius:IETF:NAS-IP-Address=192.168.1.2, Radius:IETF:NAS-Identifier=E4:D1:24:10:0B:CF-Canberra, Radius:IETF:Called-Station-Id=E4-D1-24-10-0B-CF-Canberra, Radius:IETF:NAS-Port-Type=19, Radius:IETF:Service-Type=2, Radius:IETF:NAS-Port=1, Radius:IETF:Calling-Station-Id=30-
BB-7D-4B-0F-4D, Radius:IETF:Connect-Info=CONNECT 54Mbps 802.11a, Radius:IETF:Acct-Session-Id=30bb7d4b0f4d1061000CF1701068757, Radius:IETF:WLAN-Pairwise-Cipher=1027076, Radius:IETF:WLAN-Group-Cipher=1027076, Radius:IETF:WLAN-AKM-Suite=1027073, Radius:IETF:Acct-Multi-Session-
Id=30bb7d4b0f4d1701068765, Radius:IETF:Class=Rcli3vl84n37c72tsru5g|Cc636ec2c-17a9-4a03-b760-5227979feacd, Radius:IETF:Event-Timestamp=2023-11-27 07:07:39 +0000 UTC, Radius:IETF:Acct-Delay-Time=0, Radius:IETF:Acct-Session-Time=93, Radius:IETF:Acct-Input-Packets=91,
Radius:IETF:Acct-Output-Packets=105, Radius:IETF:Acct-Input-Octets=18845, Radius:IETF:Acct-Input-Gigawords=0, Radius:IETF:Acct-Output-Octets=18558, Radius:IETF:Acct-Output-Gigawords=0, Radius:IETF:Framed-IPv6-Address=2401:4900:1c53:373:f1f4:194b:1760:43ca, Radius:IETF:Framed-IP-
Address=192.168.1.16, Radius:IETF:Acct-Terminate-Cause=10]

11/27/2023 12:37:39.257 INFO [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g multiSessionID=30bb7d4b0f4d1701068765] radius(acct) - enqueued ClientDisconnectEvent[mac=30bb7d4b0f4d ip=192.168.1.16]

11/27/2023 12:37:39.257 INFO [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g multiSessionID=30bb7d4b0f4d1701068765] radius(acct) - db update acct[stop] mac=30bb7d4b0f4d, acctSessionID=30bb7d4b0f4d1061000CF1701068757 acctMutilSessionID=30bb7d4b0f4d1701068765 in
7.565683ms

11/27/2023 12:37:39.257 INFO [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g multiSessionID=30bb7d4b0f4d1701068765] radius[acct] - session completed in 7.813366ms

11/27/2023 12:37:39.259 DEBUG [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g] eventProcessor(clientDisconnectEv) - consumerGroup[concourseEventProducer] ev disconnect[{"orgID":"Edda410ed-62c2-402d-871b-
fa79a314837c","authReqID":"Rcli3vl84n37c72tsru5g","mac":"30bb7d4b0f4d","ip":"192.168.1.16"}] @ 2023-11-27 07:07:39 +0000 UTC processed in 2.437849ms

11/27/2023 12:37:39.260 DEBUG [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g] eventProcessor(clientDisconnectEv) - consumerGroup[clientStateProducer] ev disconnect[{"orgID":"Edda410ed-62c2-402d-871b-
fa79a314837c","authReqID":"Rcli3vl84n37c72tsru5g","mac":"30bb7d4b0f4d","ip":"192.168.1.16"}] @ 2023-11-27 07:07:39 +0000 UTC processed in 3.468858ms

11/27/2023 12:37:39.520 INFO [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g] radius(coa) - added activity record for mac=30bb7d4b0f4d in 2.923272ms

11/27/2023 12:37:39.520 INFO [t=Edda410ed-62c2-402d-871b-fa79a314837c id=Rcli3vl84n37c72tsru5g] radius - coa=(orgID=Edda410ed-62c2-402d-871b-fa79a314837c, callingStationID=30-BB-7D-4B-0F-4D, nadConnID=e4d124100bcf/Ccl139104n37c72tsrtu0, authReqID=Rcli3vl84n37c72tsru5g,
disconnect=true, terminateCause=0, attrs=Radius:IETF:NAS-IP-Address=192.168.1.2, Radius:IETF:NAS-Identifier=E4:D1:24:10:0B:CF-Canberra) completed in 534.141231ms
```

The CoA action status is displayed in the Client Activity tile under client details.



Client Details - Auto registered with UPSK

View client details and update the selected client

#	TYPE	STATUS	DATE & TIME
1	coa	Success	12/1/2023 12:50:35
2	coa	Success	11/28/2023 11:15:42

Details

Access Device
30862dd07e8f

Troubleshooting

Monitoring

AGNI provides monitoring tools such as dashboards and session details. The tools provide a mechanism to troubleshoot the system operations, client authentication, and network device connection establishment status with AGNI.

Dashboards

The user and client authentication details and access device status can be viewed from the AGNI dashboards. The Session Trend captures the authentication trend with the details on total and failed authentications over a specified period.

To access dashboards, navigate to **Monitoring → Dashboard**

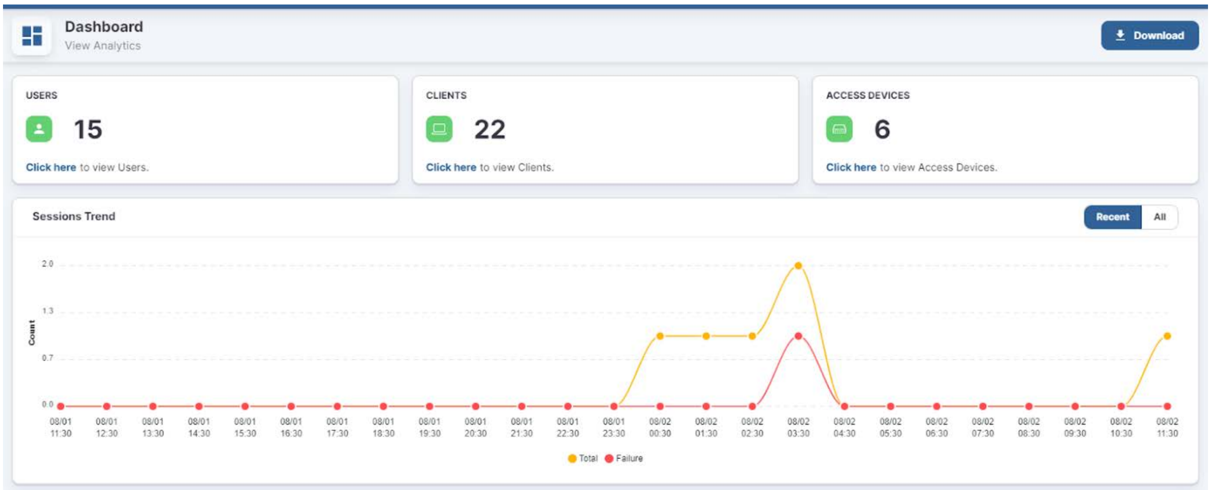


Figure: AGNI Dashboard and Session Trend

Charts are available to indicate the top failure reasons and top locations affected by the failures in the customer environment. The custom widget provides the ability to choose the charts based on the past date.

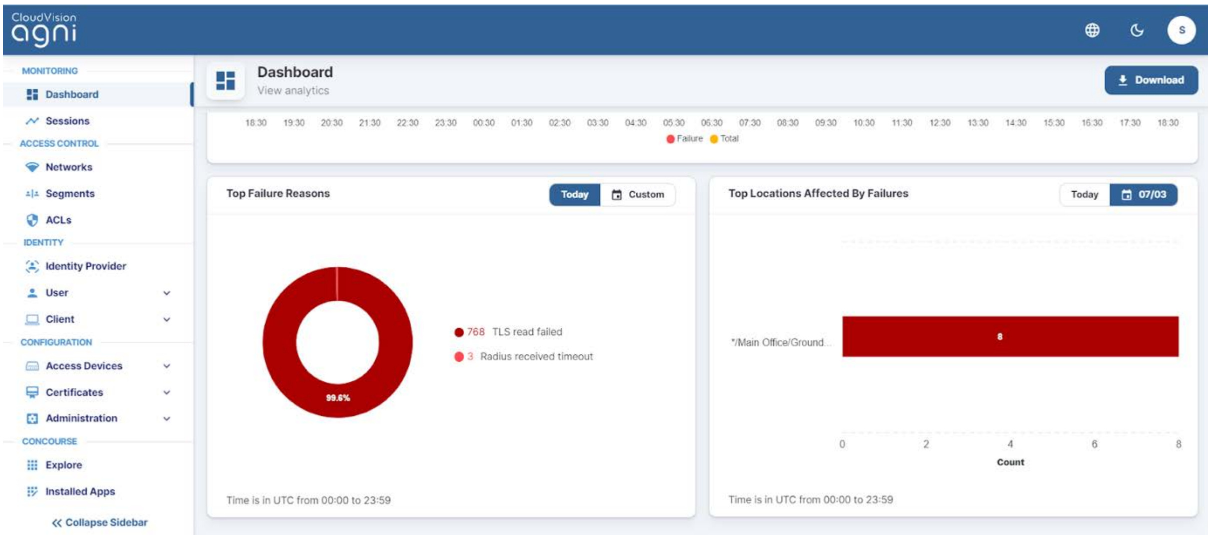


Figure: AGNI Dashboard and charts

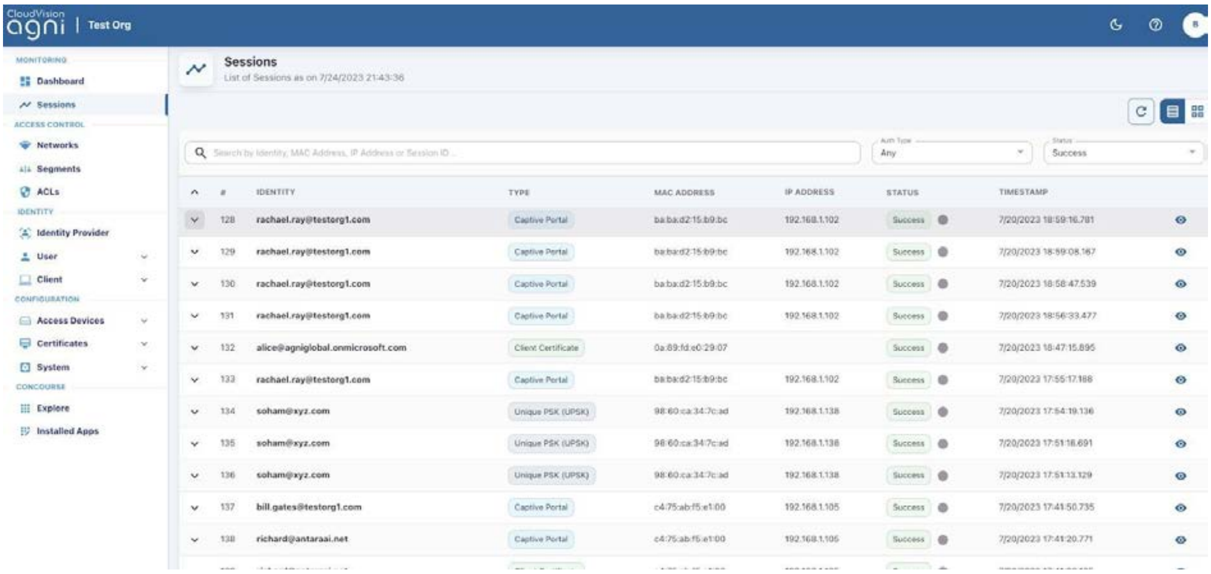
Sessions

Sessions provide a runtime view of authentication trends. All the authentication details from 802.1X, UPSK, Captive Portal, and MBA are captured in this view.

Sessions capture granular details about the incoming authentication request, system processing, and response. The sessions can be filtered based on:

- MAC address
- Identity
- IP address
- Session Identifier

To access sessions, navigate to **Monitoring** → **Sessions**.



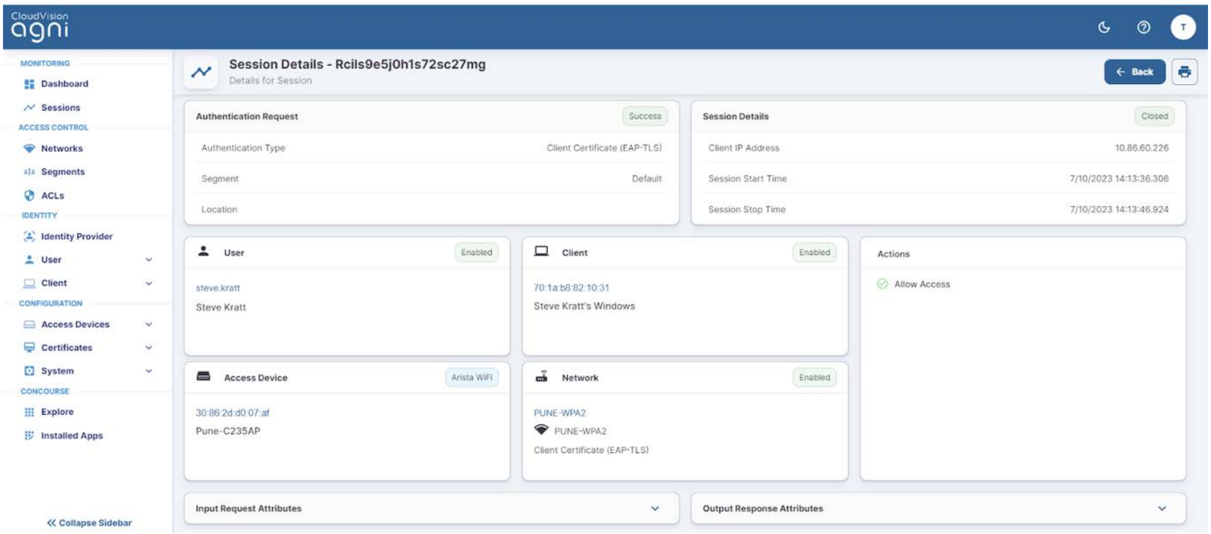
Sessions
List of Sessions as on 7/24/2023 21:43:36

Search by Identity, MAC Address, IP Address or Session ID ...
Auth Type: Any
Status: Success

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
128	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:b9:bc	192.168.1.102	Success	7/20/2023 18:59:16.781
129	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:b9:bc	192.168.1.102	Success	7/20/2023 18:59:08.167
130	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:b9:bc	192.168.1.102	Success	7/20/2023 18:58:47.539
131	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:b9:bc	192.168.1.102	Success	7/20/2023 18:56:33.477
132	alice@agniglobal.onmicrosoft.com	Client Certificate	0a:89:fd:e0:29:07		Success	7/20/2023 18:47:15.895
133	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:b9:bc	192.168.1.102	Success	7/20/2023 17:55:17.188
134	soham@xyz.com	Unique PSK (UPSK)	98:60:ca:34:7c:ad	192.168.1.138	Success	7/20/2023 17:54:19.136
135	soham@xyz.com	Unique PSK (UPSK)	98:60:ca:34:7c:ad	192.168.1.138	Success	7/20/2023 17:51:18.691
136	soham@xyz.com	Unique PSK (UPSK)	98:60:ca:34:7c:ad	192.168.1.138	Success	7/20/2023 17:51:13.129
137	bill.gates@testorg1.com	Captive Portal	c4:75:ab:f5:e1:00	192.168.1.105	Success	7/20/2023 17:41:50.735
138	richard@antaraai.net	Captive Portal	c4:75:ab:f5:e1:00	192.168.1.105	Success	7/20/2023 17:41:20.771

Figure: Sessions

To view the session details, click on the eye 👁 icon. This displays detailed session information and can be used for troubleshooting.



Session Details - Rcils9e5j0h1s72sc27mg
Details for Session

Authentication Request — Success

Authentication Type	Client Certificate (EAP-TLS)
Segment	Default
Location	

Session Details — Closed

Client IP Address	10.86.60.226
Session Start Time	7/10/2023 14:13:36.306
Session Stop Time	7/10/2023 14:13:46.924

User — Enabled
steve.kratt
Steve Kratt

Client — Enabled
70:1a:b8:82:10:31
Steve Kratt's Windows

Actions
✓ Allow Access

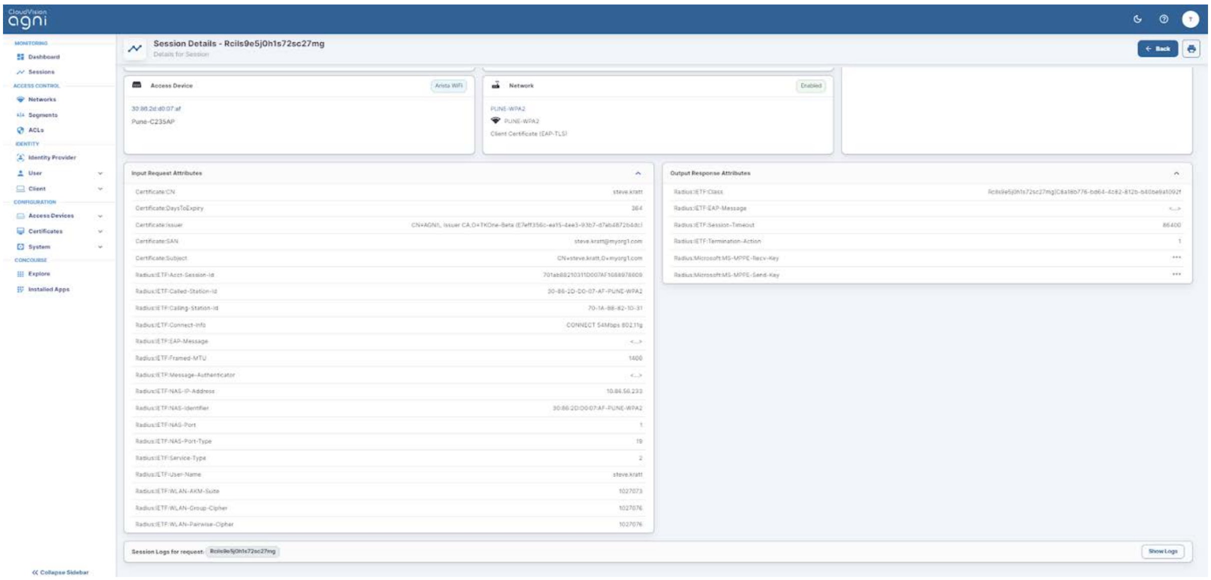
Access Device — Arista WiFi
30:86:2d:d0:07:af
Pune-C235AP

Network — Enabled
PUNE-WPA2
PUNE-WPA2
Client Certificate (EAP-TLS)

Input Request Attributes

Output Response Attributes

Figure: Session Details page-1



Session Details - Rcils9e5j0h1s72sc27mg
Details for Session

Access Device — Arista WiFi
30:86:2d:d0:07:af
Pune-C235AP

Network — Enabled
PUNE-WPA2
PUNE-WPA2
Client Certificate (EAP-TLS)

Input Request Attributes

Certificate:CN	steve.kratt
Certificate:DaysToExpiry	364
Certificate:Issuer	CN=AGNI\, Issuer CA,O=TKOne-Beta (E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc)
Certificate:SAN	steve.kratt@myorg1.com
Certificate:Subject	CN=steve.kratt,O=myorg1.com
Radius:IETF:Acct-Session-Id	701ab88210311D007AF1688978609
Radius:IETF:Called-Station-Id	30-86-2D-D0-07-AF-PUNE-WPA2
Radius:IETF:Calling-Station-Id	70-1A-B8-82-10-31
Radius:IETF:Connect-Info	CONNECT 54Mbps 802.11g
Radius:IETF:EAP-Message	<...>
Radius:IETF:Framed-MTU	1400
Radius:IETF:Message-Authenticator	<...>
Radius:IETF:NAS-IP-Address	10.86.56.233
Radius:IETF:NAS-Identifier	30:86:2D:D0:07:AF-PUNE-WPA2
Radius:IETF:NAS-Port	1
Radius:IETF:NAS-Port-Type	19
Radius:IETF:Service-Type	2
Radius:IETF:User-Name	steve.kratt
Radius:IETF:WLAN-AKM-Suite	1027073
Radius:IETF:WLAN-Group-Cipher	1027076
Radius:IETF:WLAN-Pairwise-Cipher	1027076

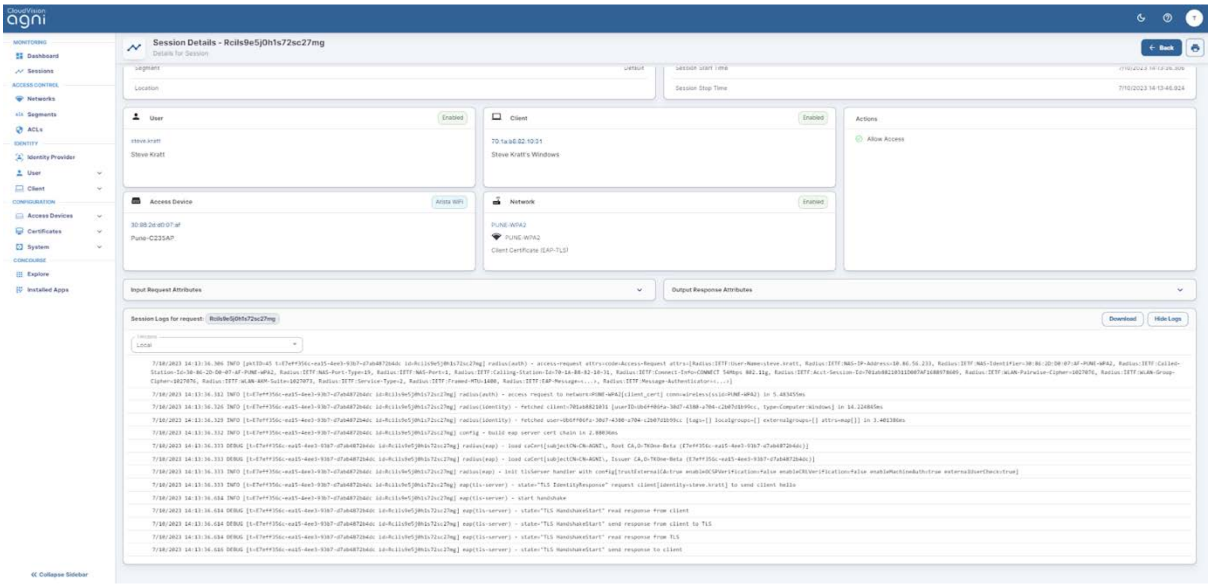
Output Response Attributes

Radius:IETF:Class	Rcils9e5j0h1s72sc27mg|C8a18b776-bd64-4c82-812b-b40be9a1092f
Radius:IETF:EAP-Message	<...>
Radius:IETF:Session-Timeout	86400
Radius:IETF:Termination-Action	1
Radius:Microsoft:MS-MPPE-Recv-Key	***
Radius:Microsoft:MS-MPPE-Send-Key	***

Session Logs for request: Rcils9e5j0h1s72sc27mg

Figure: Session Details page-2

Show logs option in session details provide information about the session and complete debug logs of the request. This can be used to troubleshoot the request failure and take appropriate action.



Session Details - Rcils9e5j0h1s72sc27mg
Details for Session

Segment — Default
Location
Session Start Time — 7/10/2023 14:13:36.306
Session Stop Time — 7/10/2023 14:13:46.924

User — Enabled
steve.kratt
Steve Kratt

Client — Enabled
70:1a:b8:82:10:31
Steve Kratt's Windows

Actions
Allow Access

Access Device — Arista WiFi
30:86:2d:d0:07:af
Pune-C235AP

Network — Enabled
PUNE-WPA2
PUNE-WPA2
Client Certificate (EAP-TLS)

Input Request Attributes

Output Response Attributes

Session Logs for request: Rcils9e5j0h1s72sc27mg

Location: Local

```
7/10/2023 14:13:36.306 INFO [pktID=45 t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(auth) - access-request attrs=code=Access-Request attrs=[Radius:IETF:User-Name=steve.kratt, Radius:IETF:NAS-IP-Address=10.86.56.233, Radius:IETF:NAS-Identifier=30:86:2D:D0:07:AF-PUNE-WPA2, Radius:IETF:Called-Station-Id=30-86-2D-D0-07-AF-PUNE-WPA2, Radius:IETF:NAS-Port-Type=19, Radius:IETF:NAS-Port=1, Radius:IETF:Calling-Station-Id=70-1A-B8-82-10-31, Radius:IETF:Connect-Info=CONNECT 54Mbps 802.11g, Radius:IETF:Acct-Session-Id=701ab88210311D007AF1688978609, Radius:IETF:WLAN-Pairwise-Cipher=1027076, Radius:IETF:WLAN-Group-Cipher=1027076, Radius:IETF:WLAN-AKM-Suite=1027073, Radius:IETF:Service-Type=2, Radius:IETF:Framed-MTU=1400, Radius:IETF:EAP-Message=<...>, Radius:IETF:Message-Authenticator=<...>]
7/10/2023 14:13:36.312 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(auth) - access request to network=PUNE-WPA2[client_cert] conn=wireless(ssid=PUNE-WPA2) in 5.483455ms
7/10/2023 14:13:36.326 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(identity) - fetched client=701ab8821031 [userID=Ub6ff06fa-38d7-4380-a704-c2b07d1b99cc, type=Computer:Windows] in 14.224845ms
7/10/2023 14:13:36.329 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(identity) - fetched user=Ub6ff06fa-38d7-4380-a704-c2b07d1b99cc [tags=[] localgroups=[] externalgroups=[] attrs=map[]] in 3.401380ms
7/10/2023 14:13:36.332 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] config - build eap server cert chain in 2.880360ms
7/10/2023 14:13:36.333 DEBUG [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(eap) - load caCert[subjectCN=CN=AGNI\, Root CA,O=TKOne-Beta (E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc)]
7/10/2023 14:13:36.333 DEBUG [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(eap) - load caCert[subjectCN=CN=AGNI\, Issuer CA,O=TKOne-Beta (E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc)]
7/10/2023 14:13:36.333 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] radius(eap) - init tlsServer handler with config[trustExternalCA:true enableOCSPVerification:false enableCRLVerification:false enableMachineAuth:true externalUserCheck:true]
7/10/2023 14:13:36.333 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] eap(tls-server) - state="TLS IdentityResponse" request client[identity=steve.kratt] to send client hello
7/10/2023 14:13:36.614 INFO [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] eap(tls-server) - start handshake
7/10/2023 14:13:36.614 DEBUG [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] eap(tls-server) - state="TLS HandshakeStart" read response from client
7/10/2023 14:13:36.614 DEBUG [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] eap(tls-server) - state="TLS HandshakeStart" send response from client to TLS
7/10/2023 14:13:36.614 DEBUG [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] eap(tls-server) - state="TLS HandshakeStart" read response from TLS
7/10/2023 14:13:36.616 DEBUG [t=E7eff356c-ea15-4ee3-93b7-d7ab4872b4dc id=Rcils9e5j0h1s72sc27mg] eap(tls-server) - state="TLS HandshakeStart" send response to client
```

Figure: Sessions and Show Logs

Appendix

OIDC Vs SAML

The following factors may help in choosing between OIDC and SAML:

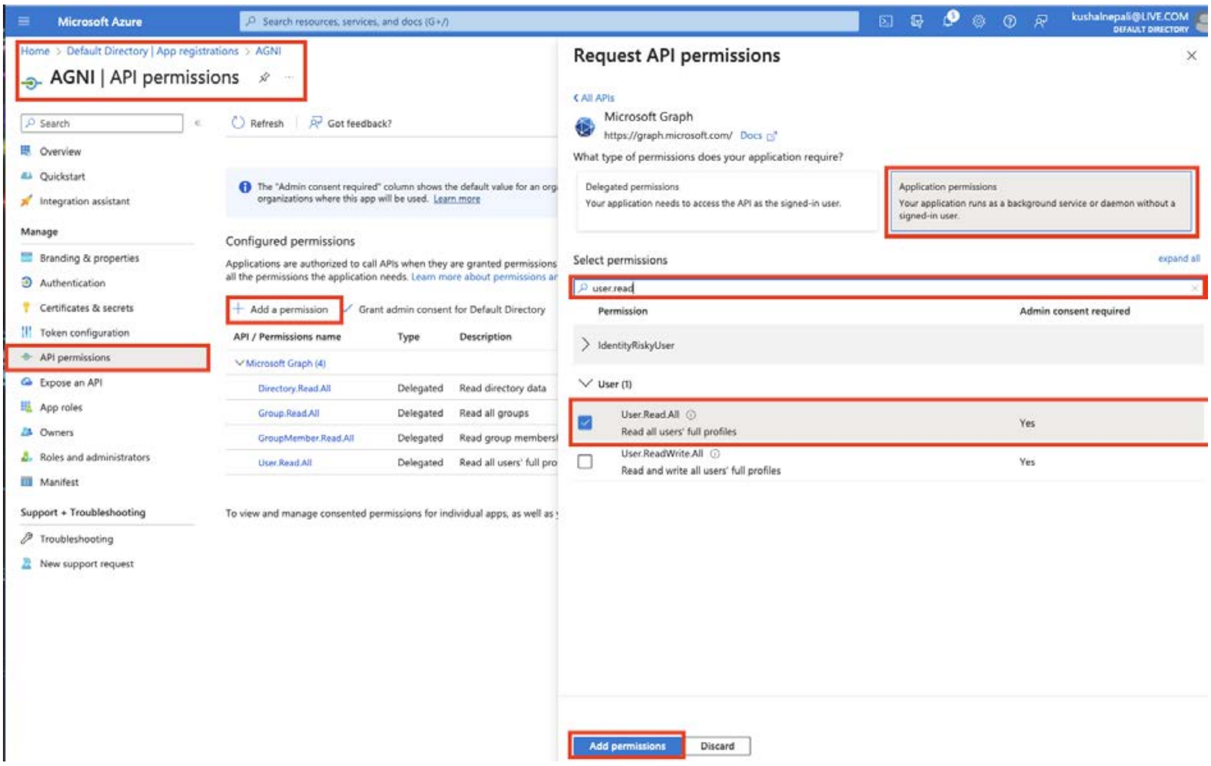
- SAML is an old standard and hard to use for modern application use cases because of the complexity surrounding the protocol.
- OIDC is a newer and well-maintained protocol built on top of OAuth 2.0 framework. OIDC uses industry-standard mechanisms to define the rules to securely transfer claims between the involved parties.
- OIDC is designed to be a modern replacement of SAML and replicates most of the fundamental SAML use cases. This reduces the complexity and overhead caused by XML and SOAP-based messages used in SAML.
- As SAML uses XML, the vulnerabilities associated with XML should be avoided during SAML implementation. This introduces further complexities in the implementation and differs from vendor to vendor.
- As OIDC is based on OAuth 2.0, it incorporates a lot of the documented threat model and security considerations.

Identity Providers

Microsoft Azure Active Directory

- Log in to Azure Active Directory instance.
- Create a New Registration by navigating to **Home→Manage** → **App Registrations**
- Click on the newly created registration. Note the values for:
    - **Application (client) ID**: This should be used for the Client ID field in AGNI
    - **Directory (tenant) ID**: This should be used for the Tenant ID field in AGNI
- Navigate to **Manage** → **Certificates & Secrets**. Add a **New Client Secret**.
    - Note the value of the newly created secret.
    - This value should be used for the Client Secret value in AGNI

- Navigate to **Manage** → **API Permissions**. Set the following permissions.



The "Admin consent required" column shows the default value for an org… organizations where this app will be used. Learn more

Configured permissions

Applications are authorized to call APIs when they are granted permissions… all the permissions the application needs. Learn more about permissions ar…

API / Permissions name	Type	Description
Microsoft Graph (4)		
Directory.Read.All	Delegated	Read directory data
Group.Read.All	Delegated	Read all groups
GroupMember.Read.All	Delegated	Read group membersl
User.Read.All	Delegated	Read all users' full pro

To view and manage consented permissions for individual apps, as well as y…

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

user.read

	Permission	Admin consent required
	IdentityRiskyUser	
	User (1)	
☑	User.Read.All Read all users' full profiles	Yes
□	User.ReadWrite.All Read and write all users' full profiles	Yes

Figure: API Permissions

API Permission	Type	Admin Consent	Status
Directory.Read.All	Application	Yes	Grant admin consent
Group.Read.All	Application	Yes	Grant admin consent
GroupMember.Read.All	Application	Yes	Grant admin consent
User.Read.All	Application	Yes	Grant admin consent

Google Workspace

- Log in to Google Workspace
- Note the following entities from Google Console
  - Customer ID
  - Domain
  - Account Email - The username of the Google Workspace account that has minimum permissions to read the User and Group objects. Normally, this is the account that is used to configure or manage the GWS configuration objects.
  - Service Account
- Reading Customer ID and Domain
  - Log in to https://admin.google.com
  - Navigate to **Account** → **Account Settings**
  - Note down **Customer ID** displayed in the **Profile** section.

    - Navigate to **Domains** → **Manage Domains**
    - Note down the primary domain name as **Domain.**
- Configuring Service Account
    - Log in to https://console.cloud.google.com
    - Create a new project for AGNI
    - Navigate to **APIs & Services** → **Credentials**
    - Create a new **Service Account** and download the JSON file
- Scopes for Service Account
    - Log in to https://admin.google.com
    - Select **Enable Google Workspace** domain-wide delegation for the Service Account
    - Enter the following common OAuth scopes separately:
        - https://www.googleapis.com/auth/admin.directory.user,
        - https://www.googleapis.com/auth/admin.directory.user.readonly,
        - https://www.googleapis.com/auth/admin.directory.user.security,
        - https://www.googleapis.com/auth/admin.directory.group,
        - https://www.googleapis.com/auth/admin.directory.group.readonly,
        - https://www.googleapis.com/auth/admin.directory.group.member,
        - https://www.googleapis.com/auth/admin.directory.group.member.readonly,
        - https://www.googleapis.com/auth/admin.directory.rolemanagement,
        - https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
        - https://www.googleapis.com/auth/cloud-platform

OneLogin

- Log in to OneLogin administration interface
- Navigate to **Applications** → **Applications** and add new **OpenId Connect** (OIDC) application
- Note down the **Client ID** and **Issuer URL** under SSO section of the application
- Navigate to **Developers** → **API Credentials**
- Add New Credentials and the privileges set to Read users
- Note down **Client ID** and **Client Secret**

Okta

- Log in to Okta administration interface
- Navigate to **Applications** → **Applications** and add new **Create App Registration**
- Choose **Client Authentication** as **None**
- Choose **Proof Key for Code Exchange** (PKCE)
- Set the **Application Type** as **Single Page App** (SPA)
- Set the **Grant Type** to **Client Acting on behalf of a user**
    - Authorization Code
    - Refresh Token
- Specify the Sign in redirect URLs (AGNI's cluster details as documented)

- Set **Login initiated** by App Only
- Once created note down the **Client ID**
- Navigate to **Security** → **API**
- Create a new token and note down the:
    - Issuer URI
    - API Key