

ARISTA

Arista Guardian for Network Identity (AGNI) User Guide

Arista Networks

www.arista.com

*Arista NetVisor Version 2024.1.0
DOC-06557-03*

Introduction.....	7
Accessing the UI.....	7
Viewing Licensing Details.....	8
User Interface (UI) Theme.....	9
Third-Party Integrations.....	10
CV-CUE Integration.....	10
CloudVision Integration.....	11
Adding Multiple CVaaS Instances in AGNI.....	13
Configuring CVaaS Instances.....	13
MSS-G Integration.....	16
Integrating MSS-G with AGNI.....	17
Arista NDR Integration.....	19
Configuring Arista NDR.....	20
Configuring Segment Policies.....	24
Using Risk Action in Segment Policies.....	27
External Integrations.....	29
Palo Alto Cortex XDR Integration.....	29
Medigate Integration.....	30
Microsoft Intune Integration.....	32
Jamf Integration.....	32
Splunk Integration.....	33
Sumo Logic Integration.....	34
CrowdStrike Integration.....	35
Event Notification.....	36
Workspace ONE integration.....	37
Downloading Issuer and Root Certificates for AGNI CA.....	39
Configuring Various Entities in AGNI.....	40
Configuring the Devices.....	41
Adding an Access Device.....	41
Importing Devices in Bulk to AGNI.....	42
Importing Devices to AGNI.....	42
Configuring TACACS+ with AGNI.....	44
Configuring Arista Cloud Gateway on Arista Switches.....	45
Configuring Arista Cloud Gateway on AGNI.....	48
Configuring TACACS+ on Arista Switches.....	51
Debug commands on Arista Cloud Gateway.....	52
Enabling Device Administration on AGNI.....	53
Configuring TACACS+ on AGNI.....	54

Monitoring TACACS+ on AGNI.....	57
Accessing Self Service Portal on AGNI.....	58
Configuring Cloud Gateway for Integrating AGNI & On-Premises.....	62
Configuring Cloud Gateway in AGNI.....	62
Installing Cloud Gateway.....	64
Debugging Workflow.....	65
Generating Client Certificates.....	66
Viewing the Certificates.....	69
Configuring Device Groups.....	69
Configuring Identity Providers (IDPs).....	71
Microsoft 365 (Azure).....	71
OneLogin.....	74
Okta.....	76
Google Workspace.....	78
Local.....	80
Guest Onboarding Features.....	81
Guest Onboarding Using AGNI.....	81
Guest User in AGNI.....	81
Portal Users.....	81
UPSK Users.....	84
Guest Operator.....	86
Guest Sponsor.....	87
Guest Onboarding Offerings in AGNI.....	87
Portal Based Guest Onboarding.....	87
Clickthrough Portal-based Method.....	88
Organizational User Login.....	89
Guestbook Based Onboarding.....	92
Guestbook Method.....	92
Self-Registration.....	93
Host Approval.....	96
UPSK Based Guest Onboarding.....	101
Configuring UPSK for Onboarding Guest (Wireless).....	102
Configuring AGNI.....	102
Configuring CV-CUE.....	105
Onboarding the User.....	107
Configuring Guest Portal Using Guestbook (Wireless).....	108
Configuring the Portal on AGNI.....	108
Configuring Network.....	114
Configuring CV-CUE.....	115
Configuring Role Profile.....	115
Configuring SSID.....	117
Configuring Guest Portal Using Guestbook-Host Approval (Wireless).....	121
Configurations on AGNI.....	121

Configuring the Network.....	126
Configuring CV-CUE.....	126
Configuring Role Profile.....	126
Configuring SSID.....	128
User Onboarding.....	132
Configuring Guest Portal Using Self-Registration (Wireless).....	136
Configuring the Portal on AGNI.....	136
Configuring Network.....	140
Configuring CV-CUE.....	141
Configuring Role Profile.....	141
Configuring SSID.....	142
User Onboarding.....	146
Networks.....	150
802.1X.....	150
Prerequisites.....	151
Configuring the Networks.....	151
Authenticating Users with Email Codes (as against IDP).....	154
Network Settings.....	158
Unique PSK (UPSK) Settings.....	158
Prerequisites.....	158
Configuration.....	158
Configuring the Device Count Limit for Authentication.....	161
Wireless Captive Portal.....	163
Prerequisites.....	163
Configuration.....	163
Configuring Guest Portal in AGNI for Wireless Clients.....	166
Configuring AGNI.....	166
Configuring CV-CUE.....	169
Configuring Role Profile.....	169
Configuring SSID.....	170
Wireless MAC Authentication.....	174
Prerequisites.....	174
Configuration.....	174
Wired 802.1X.....	175
Prerequisites.....	175
Configuration.....	176
Wired MAC Authentication.....	179
Prerequisites.....	179
Configuration.....	180
Wired Captive Portal.....	182
Prerequisites.....	182
Configuration.....	182
Configuring Guest Portal in AGNI for Wired Clients.....	184

Configuring AGNI.....	184
Configuring EOS.....	188
Segments.....	188
Status.....	188
Conditions.....	189
Actions.....	189
Configuration.....	189
Sample Segments.....	190
User Configurations.....	194
Users.....	194
External Users.....	194
Local User.....	195
User Groups.....	196
Local User Groups.....	196
Client Configuration.....	197
Clients.....	200
Client Details.....	201
Creating Client Certificates Manually in AGNI.....	202
System.....	207
Portal Settings.....	208
RadSec Settings.....	209
Support Logs.....	209
System Events.....	210
Sessions.....	210
On-Demand Disconnecting a Client from the Network.....	211
Troubleshooting.....	214
Monitoring.....	214
Dashboards.....	215
Sessions.....	216
Appendix.....	219
OIDC Vs SAML.....	219
Identity Providers.....	219
Microsoft Azure Active Directory.....	219
Google Workspace.....	220
OneLogin.....	221
Okta.....	222

Introduction

This document provides information about Arista Networks' Arista Guardian for Network Identity (AGNI) software and 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

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. Access the 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).

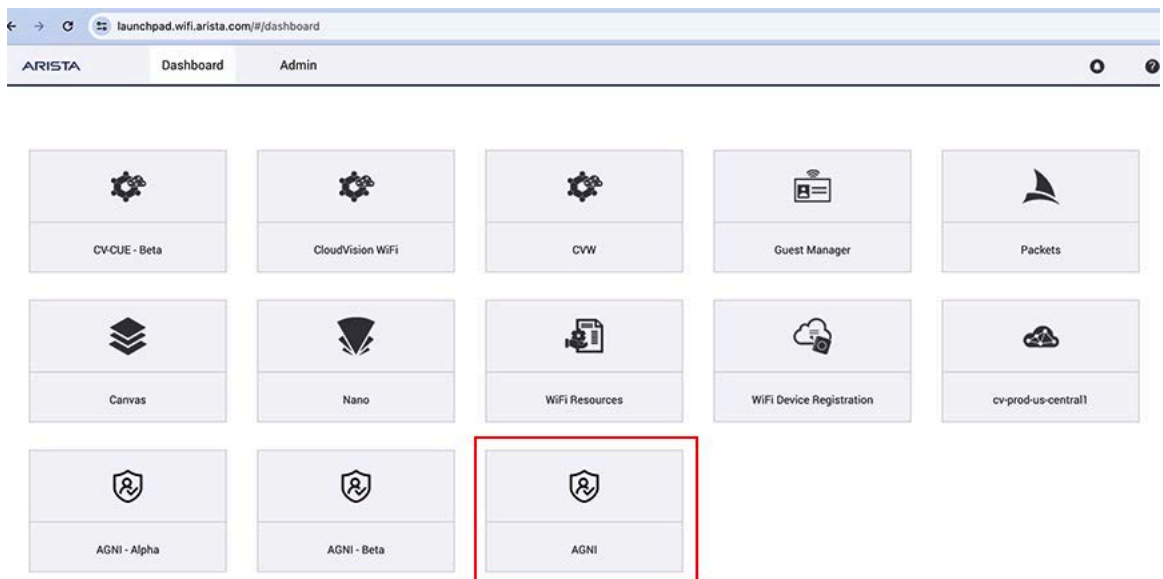


Figure: Arista Launchpad Displaying AGNI and Other Applications

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.

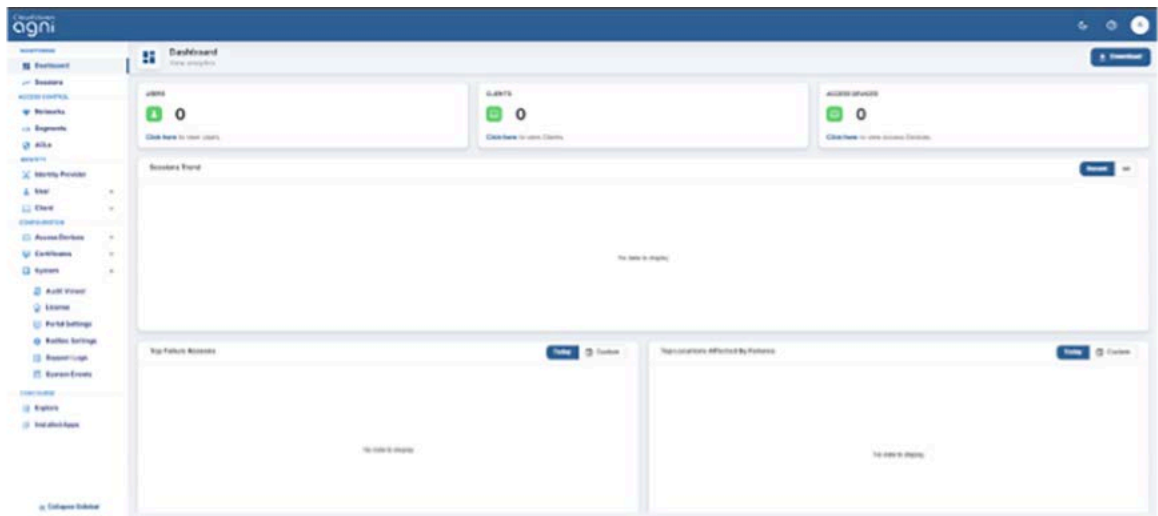


Figure: AGNI Dashboard

Viewing Licensing Details

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

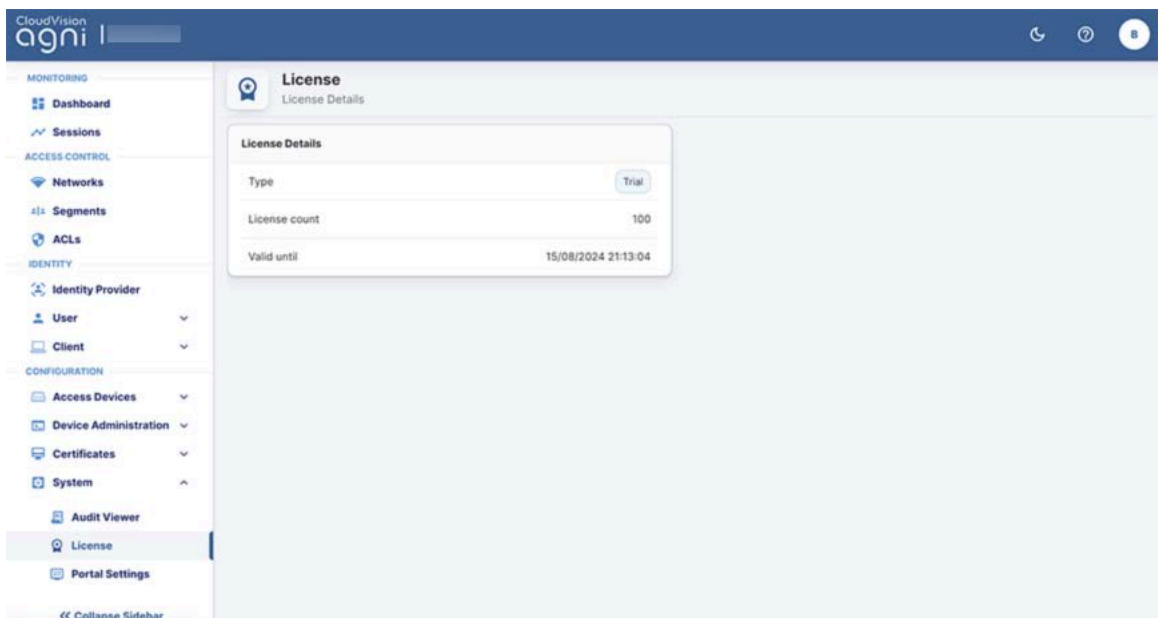


Figure: AGNI License Details

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).

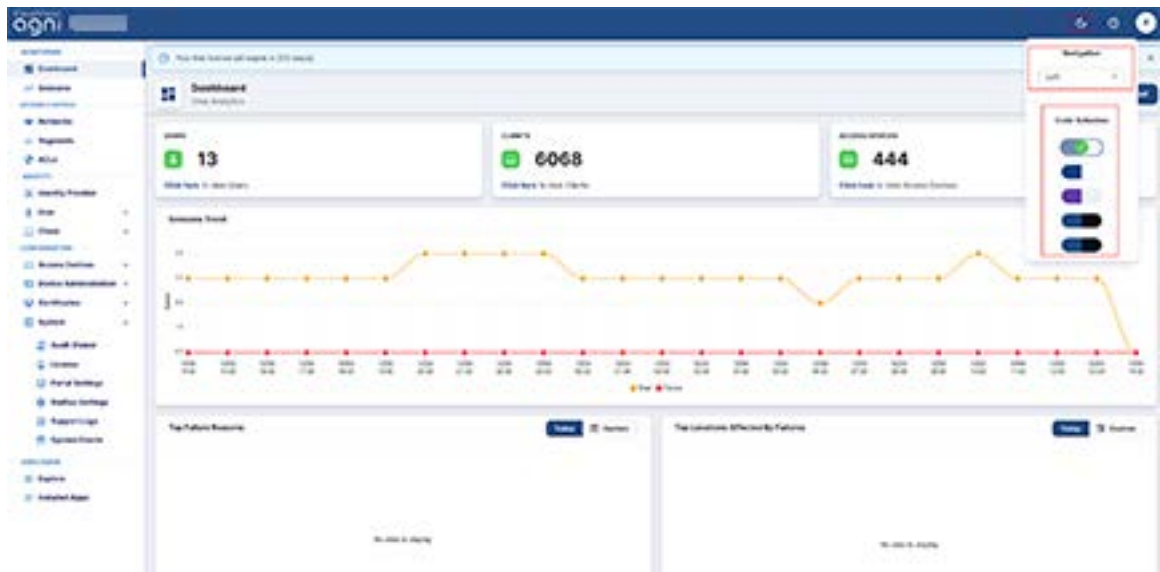


Figure: AGNI UI Theme (Navigation & Color) Settings

Third-Party Integrations

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

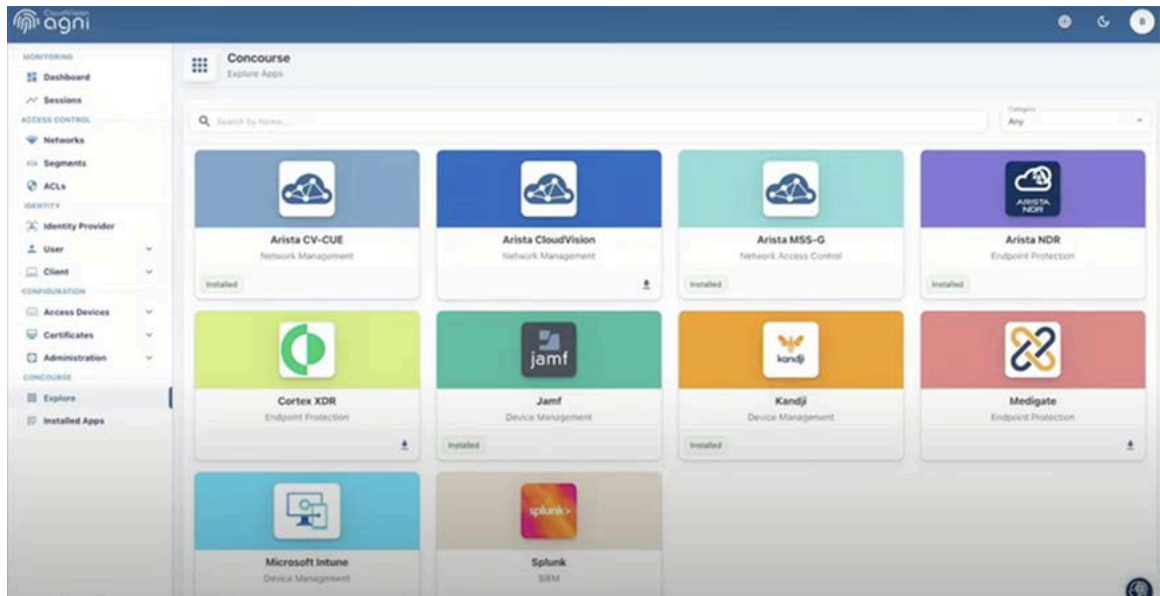


Figure:AGNI Concourse Applications

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

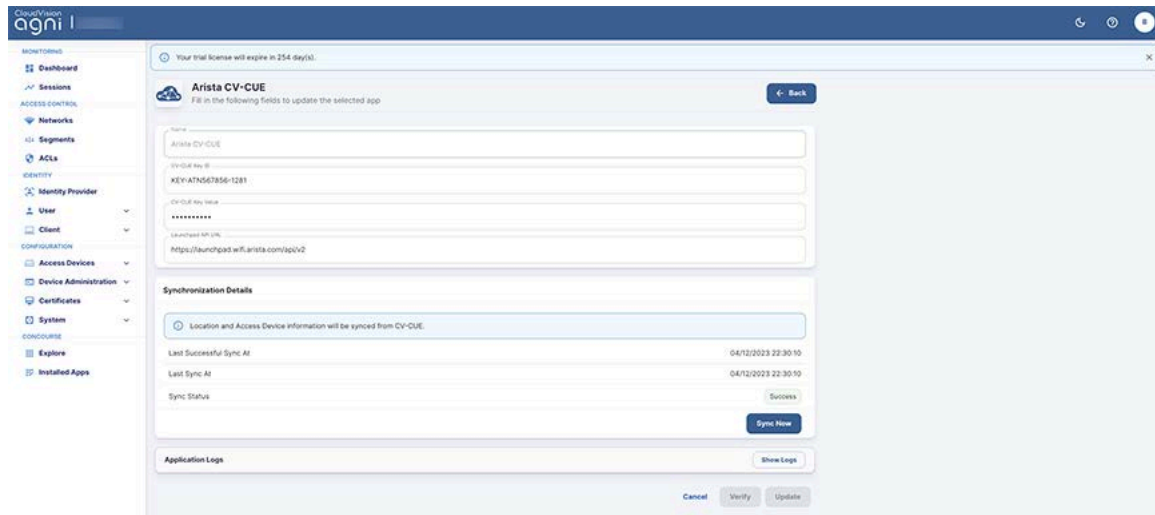


Figure: Installing Arista CV-CUE Concourse Application

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

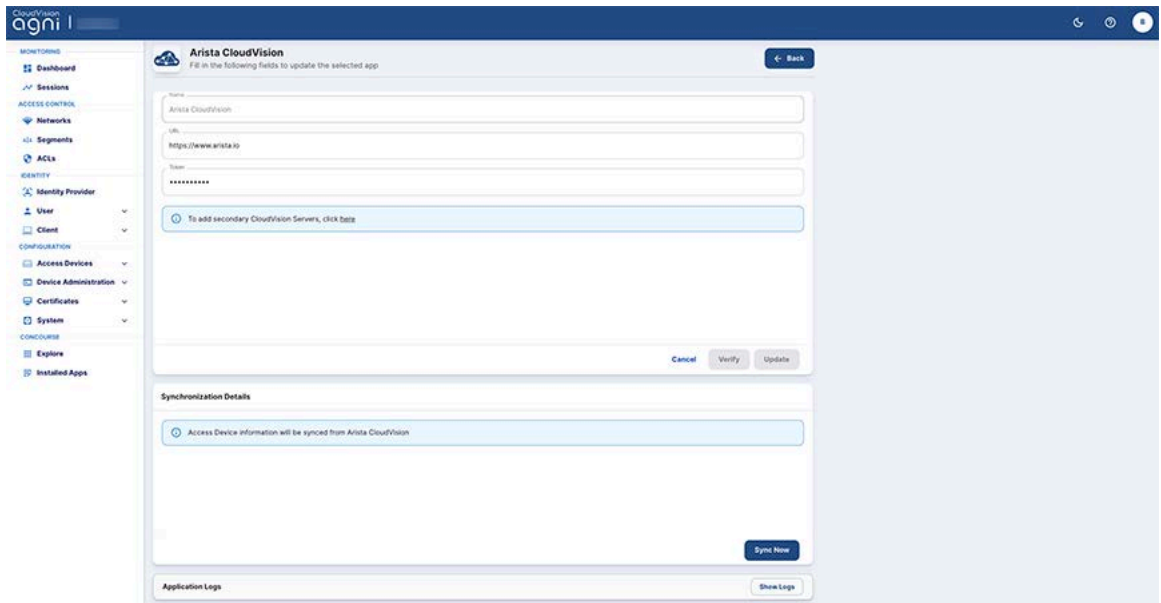


Figure: Installing Arista CloudVision Concourse Application

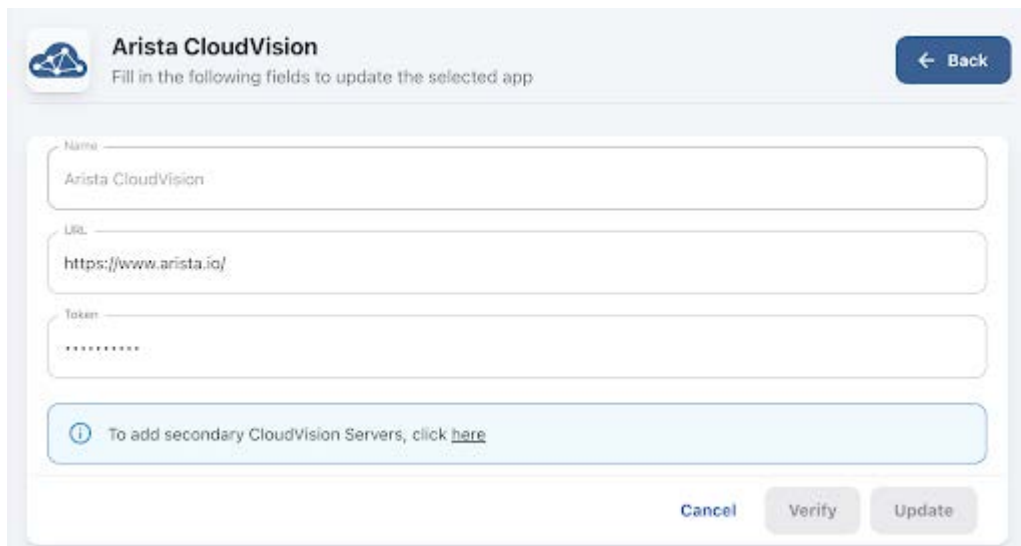
3. Enter the following parameters:
 - a. Arista CloudVision in the **Name** field
 - b. The URL of the CloudVision application
 - c. API Token value
 4. Click the **Verify** button to validate the credentials
 5. Click the **Install** button to complete the installation process.
The CloudVision application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



The screenshot shows a web form titled "Arista CloudVision" with a subtitle "Fill in the following fields to update the selected app". A "Back" button is in the top right. The form contains three input fields: "Name" with the value "Arista CloudVision", "URL" with the value "https://www.arista.io/", and "Token" with a masked value "*****". Below these fields is a light blue box containing an information icon and the text "To add secondary CloudVision Servers, click [here](#)". At the bottom right are three buttons: "Cancel", "Verify", and "Update".

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).

Figure: Adding Secondary Servers

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

Figure: Adding CloudVision Server

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

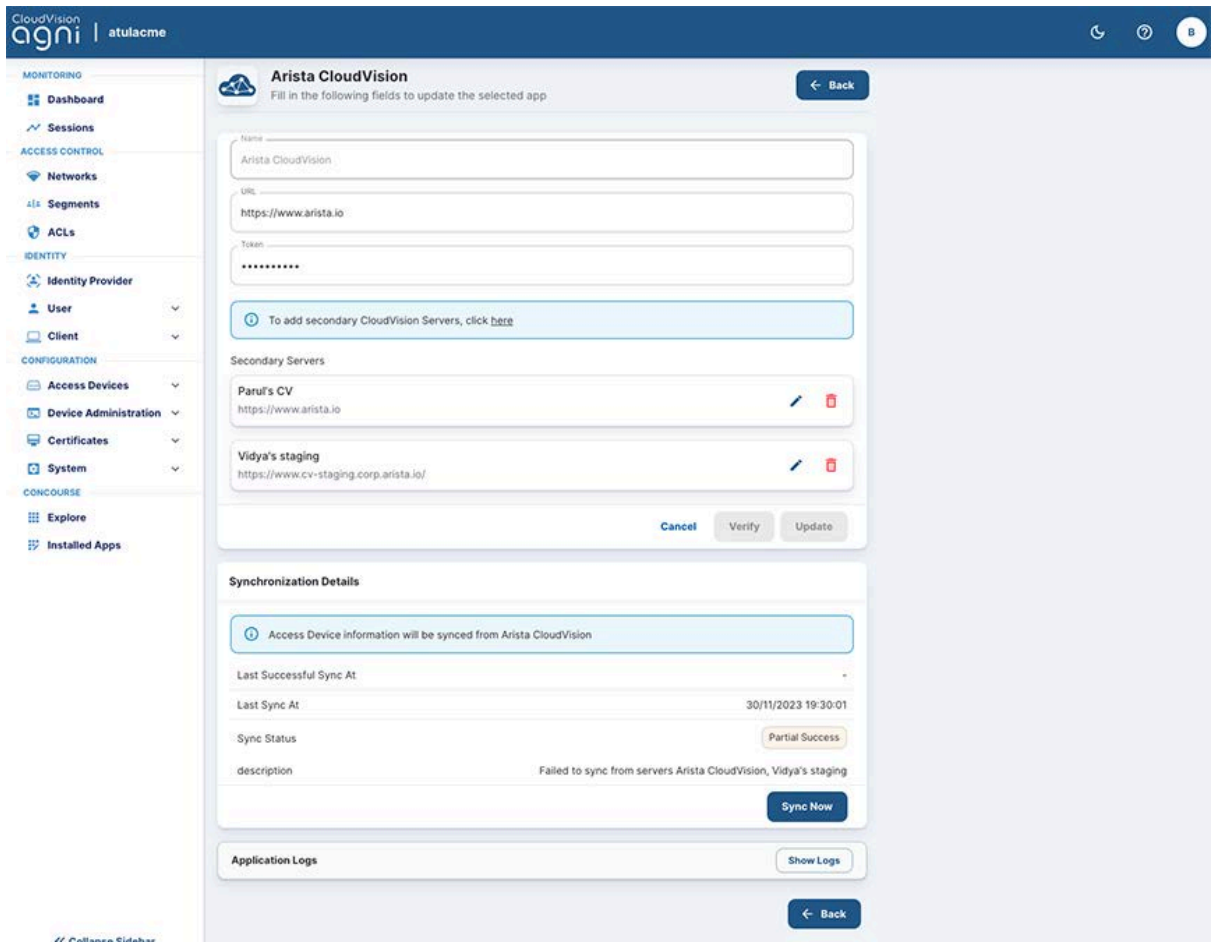


Figure: CVaaS Synchronization Details

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						
Search by Name, MAC Address or Location ...						Vendor All Devices
#	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:8f	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.

Integrating MSS-G with AGNI

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

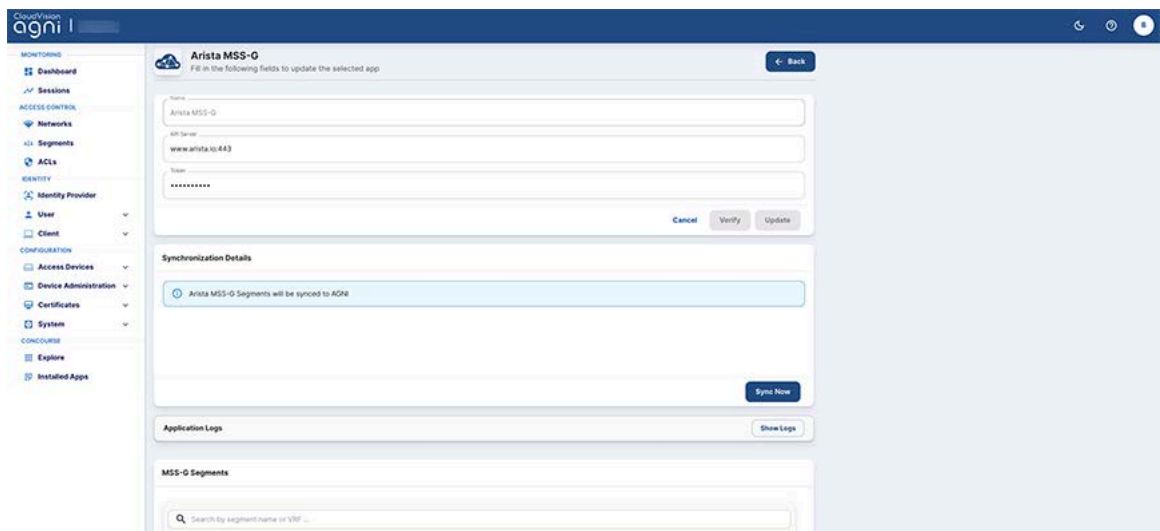


Figure: Installing Arista MSS-G Concourse Application

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).

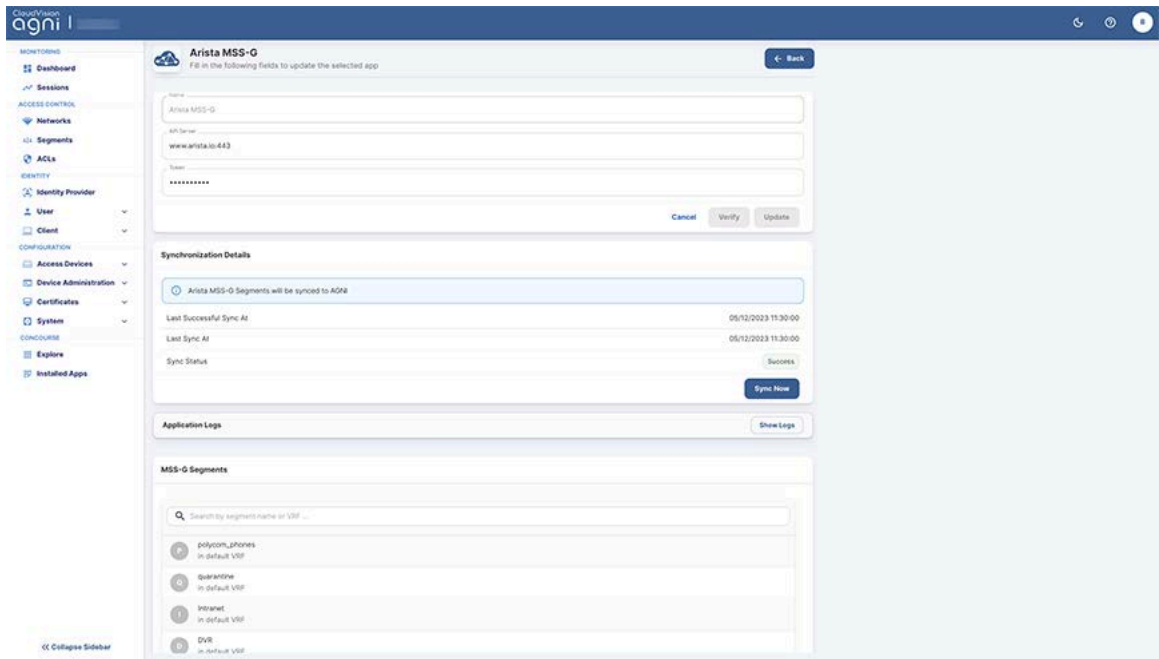


Figure: Installed Arista MSS-G Concourse Application

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.

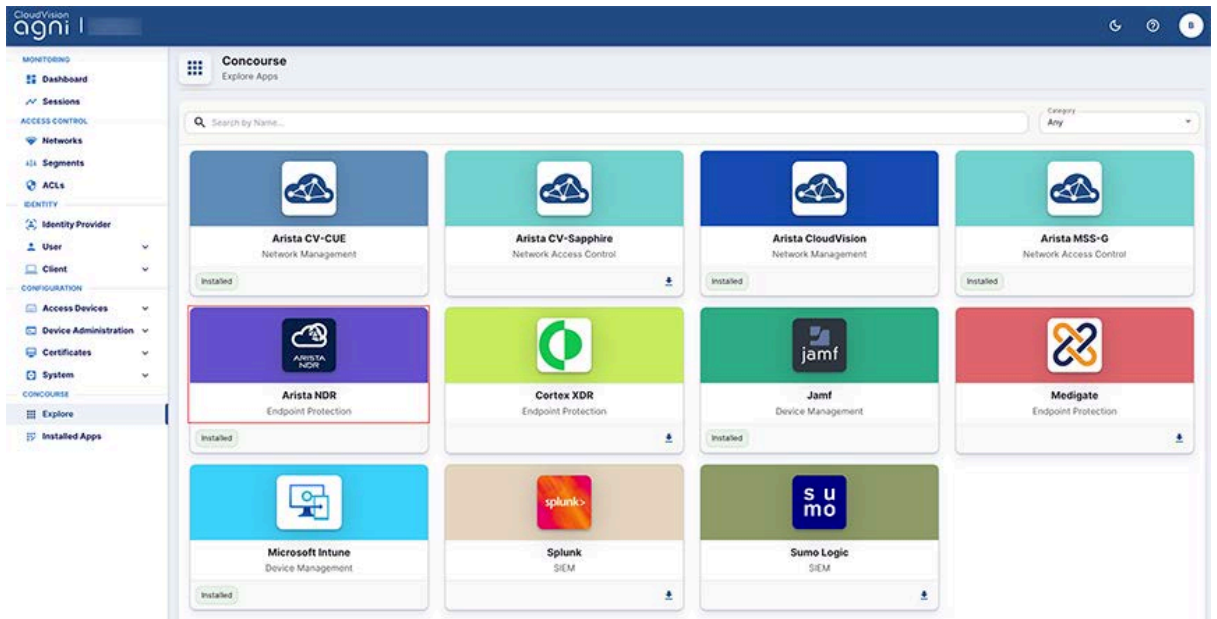


Figure : Arista NDR in Concourse App

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

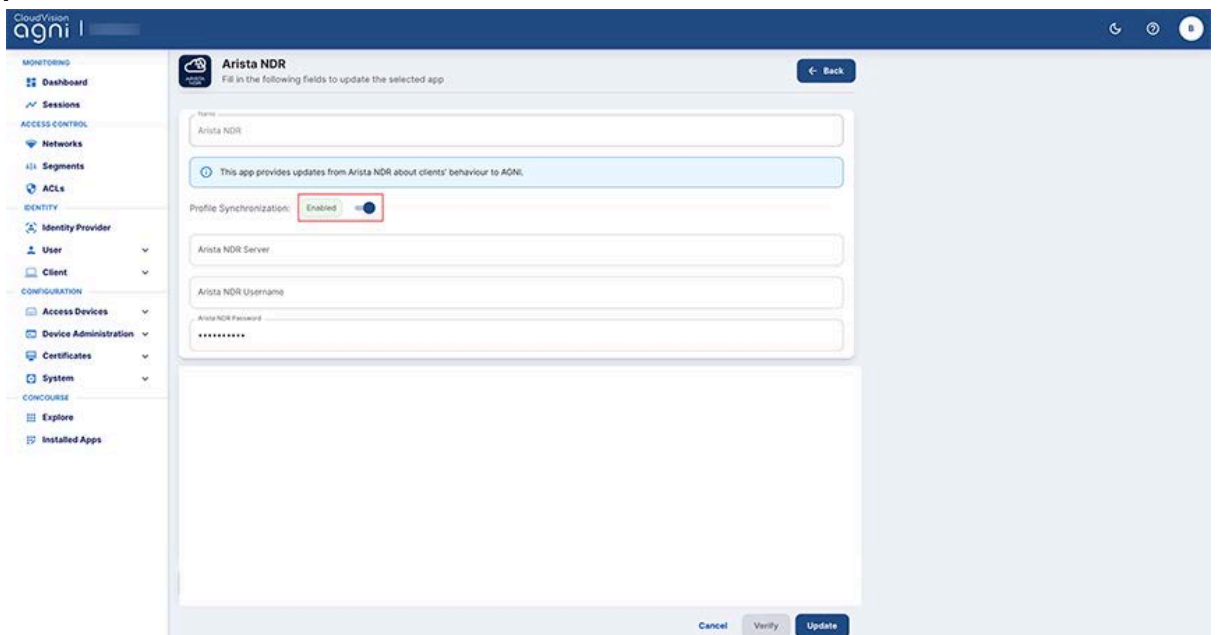


Figure: Arista NDR Integration

- 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.

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).

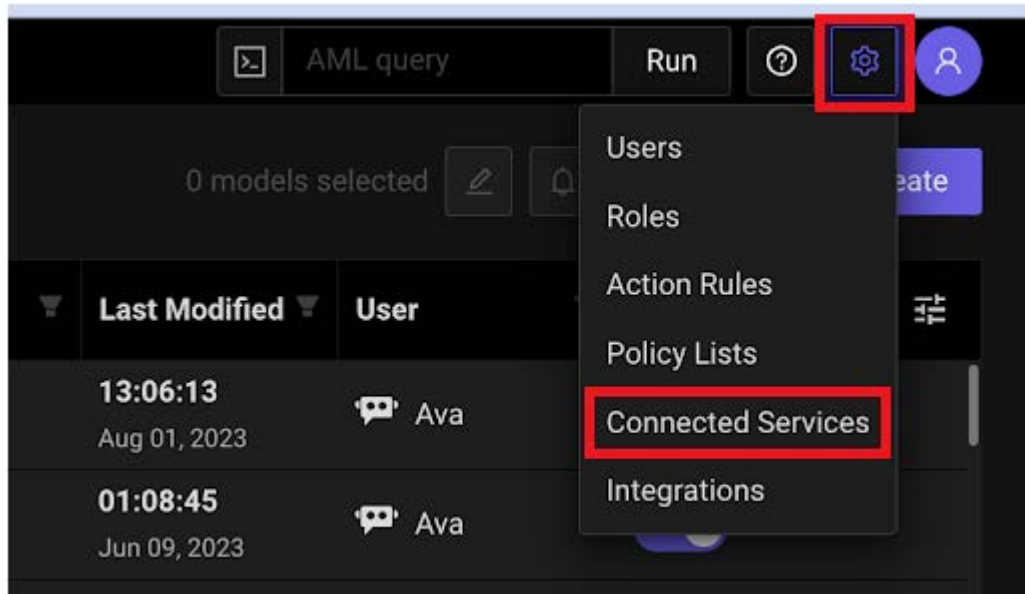


Figure: Arista NDR Configuration Settings Page

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

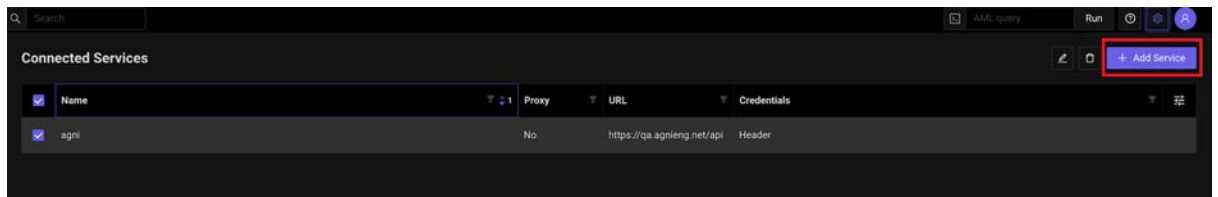


Figure: Arista NDR Configuration - Add Service

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

Edit Service

* Name
agni

* URL
https://qa.agnieng.net/api

* Header Name
Authorization

* Header Value
Bearer eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IklU0NWZlZWNmMi04OGNhLT...

* Proxy

Discard Changes Save

Figure: Arista NDR Configuration Details

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

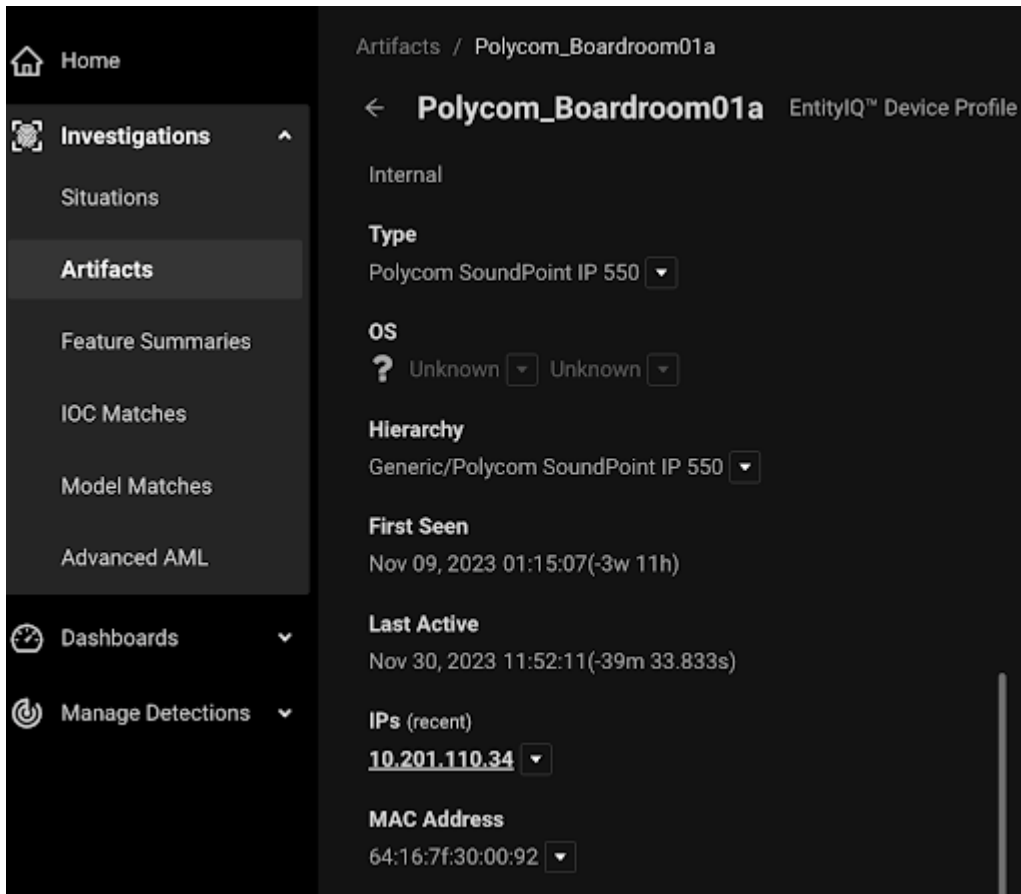


Figure: Arista NDR Configuration Artifacts Details

- 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.

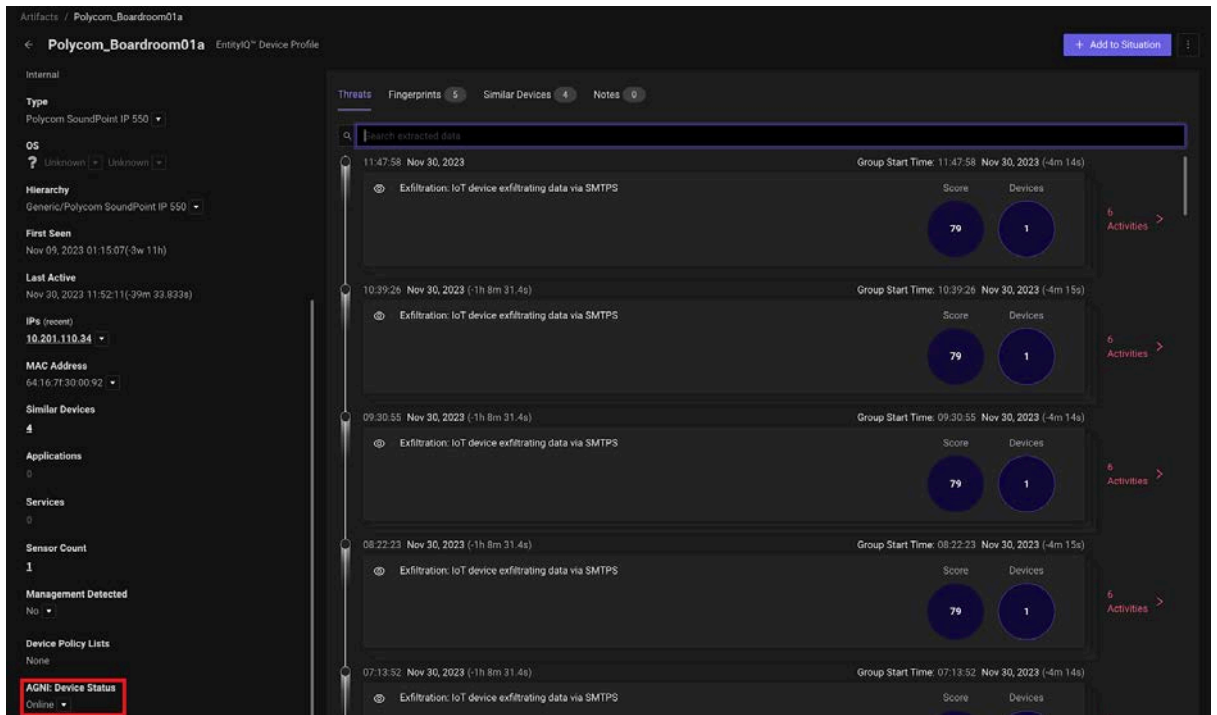


Figure: Arista NDR - AGNI Integration Status

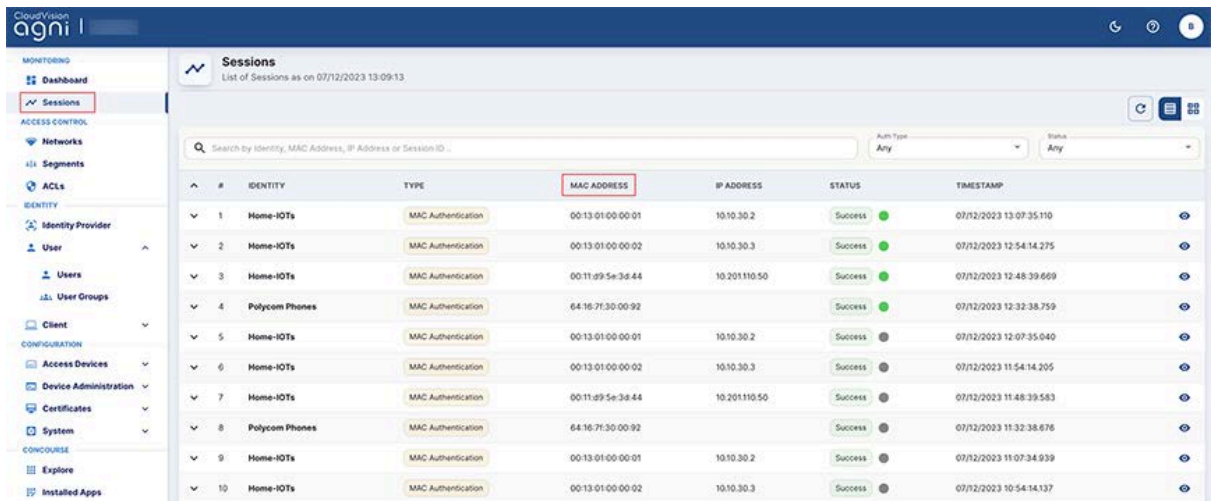
Configuring Segment Policies

After the successful integration of AGNI with Arista NDR, as a network 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.



The screenshot shows the AGNI interface with the 'Sessions' tab selected. The table displays the following data:

#	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:3e:44	10.201.110.50	Success	07/12/2023 12:48:39.669
4	Polycorn 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:3e:44	10.201.110.50	Success	07/12/2023 11:48:39.583
8	Polycorn 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:

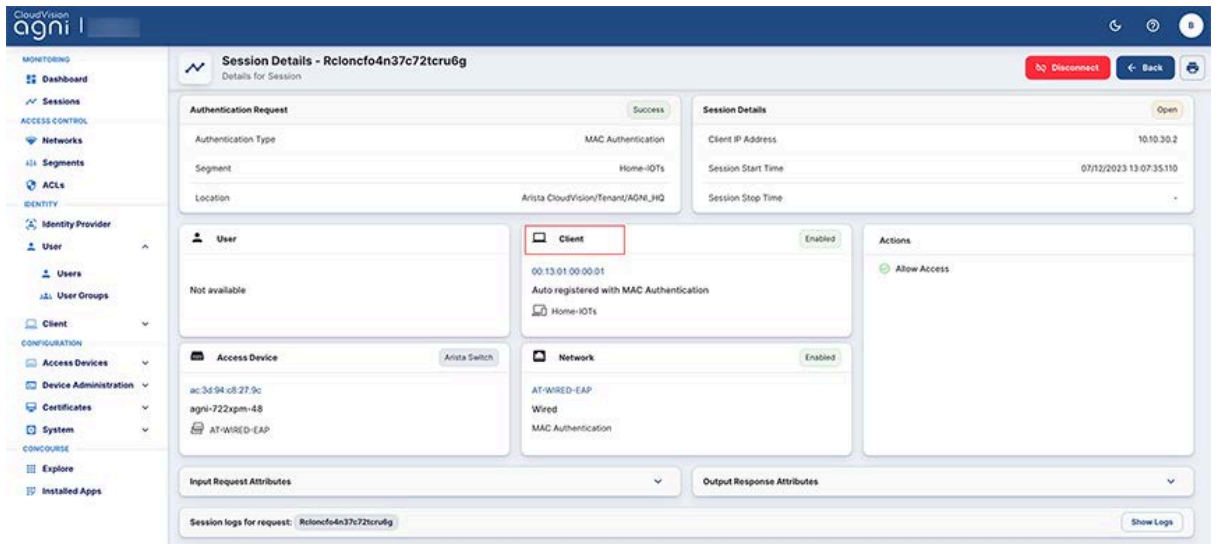


Figure: Sessions Client Details

- Add the details and click Update Client:



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

Disable | Monitor

Conditions MATCHES ALL

Client: Arista NDR: ×

- Device Brand
- Device Hierarchy
- Device Type
- Risk Action ✓

⊞ Add Condition

Actions

⊞ Add Action

Action cannot be empty

Cancel

Add Segment

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 Disable | Monitor

Conditions MATCHES ALL

Client: Arista NDR: Risk Action is quarantine ✕

≡ Add Condition

Actions

Assign VLAN Assign VLAN through RADIUS response ✕

VLAN Quarantine VLAN

+

≡ Add Action

Cancel Add Segment

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	X
Arista NDR: Device Type	=	Polycom SoundPoint IP 550	X
Arista NDR: Risk Action	=	deQuarantine	X

≡ Add Attribute

Cancel **Update Client**

Client Details

Device Type

Machine Authenticated

Added At

Updated At

Client Fingerprint

Last Session Details

IP Address

Location

Segment

Authentication Status

Network Client Certificate

AT-WIRED-EAP
Wired

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

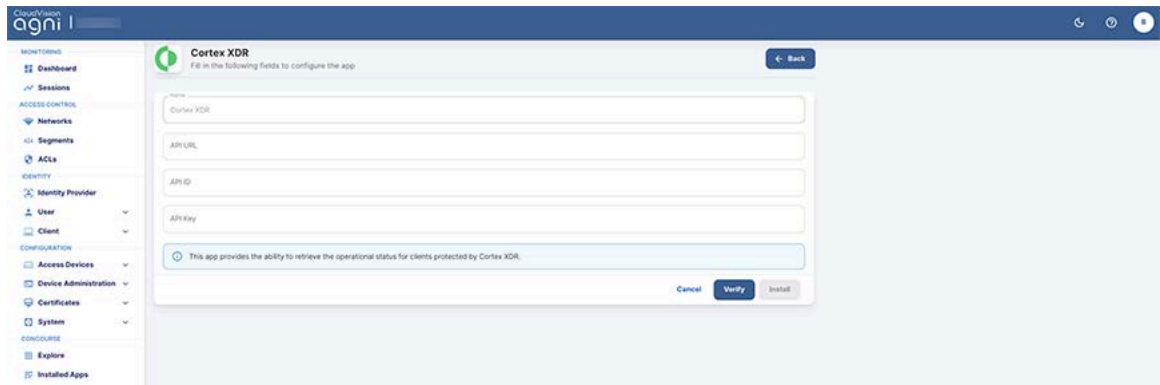


Figure: Installing Palo Alto Cortex XDR Concourse Application

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)

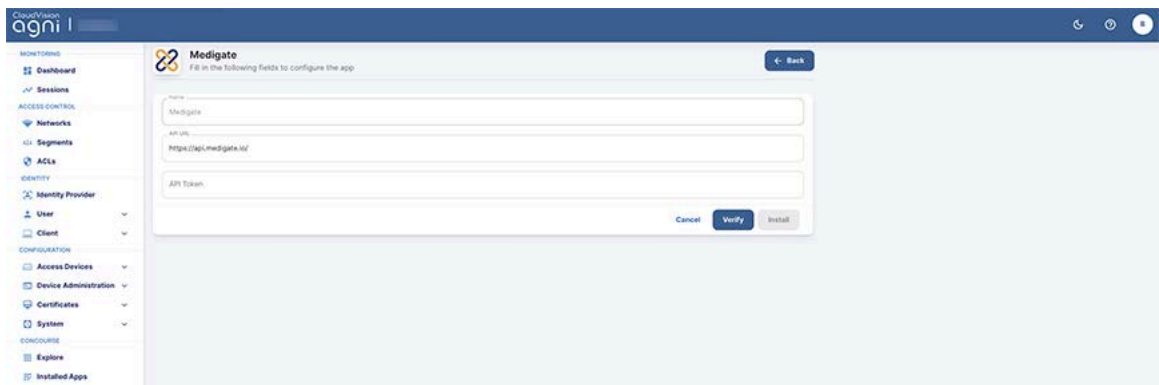


Figure: Installing Medigate Concourse Application

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).

The screenshot displays the Agni dashboard interface. On the left is a sidebar with a navigation menu. The main content area is titled "Medigate" and contains a form for updating the application. Below the form is a "Synchronization Details" section with a table of sync events and a "Sync Now" button. At the bottom, there is an "Application Logs" section with a "Show Logs" button.

Monitoring

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
 - Users
 - User Groups
- Client
 - Clients
 - Client Groups

CONFIGURATION

- Access Devices
 - Devices
 - Device Groups
 - Administration
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

Medigate
Fill in the below fields to update the selected app

← Back

Name: Medigate

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

API Key: [REDACTED]

Cancel Verify Update

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

Sync Now

Application Logs

Show Logs

← Back

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)

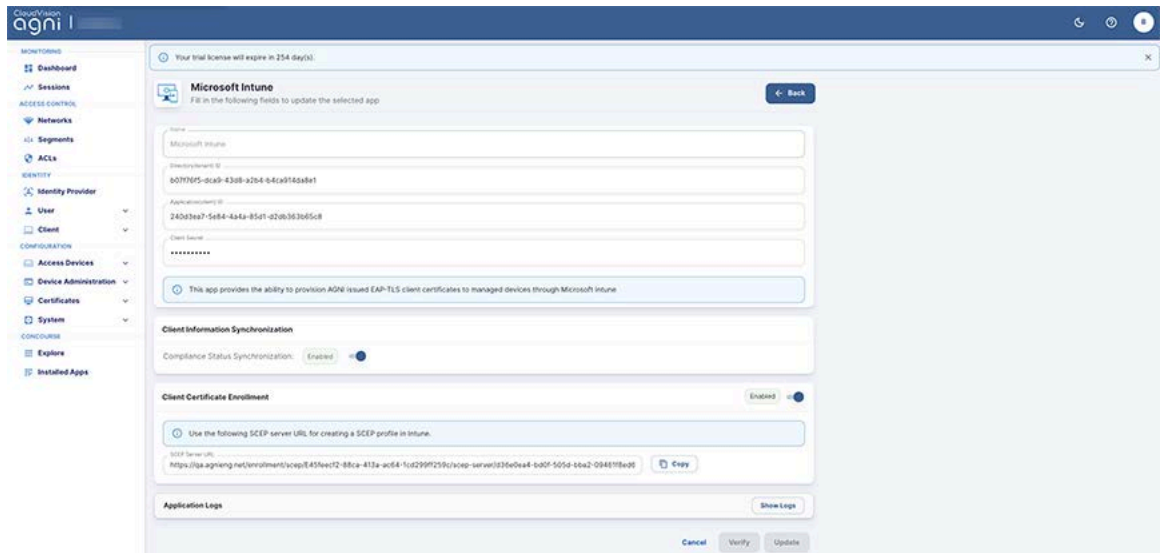
The image shows a screenshot of the AGNI portal interface. On the left is a navigation sidebar with categories like MICROSERVICES, ACCESS CONTROL, IDENTITY, CONFIGURATION, and CONSCORE. The main content area is titled 'Microsoft Intune' and contains a form for installation. The form includes fields for Name, Directory (Tenant) ID, Application (Client) ID, and Client Secret. Below these fields, there are sections for 'Client Information Synchronization' and 'Client Certificate Enrollment', both with 'Enabled' toggle switches. A 'SCEP Server URL' is displayed with a 'Copy' button. At the bottom, there are 'Cancel', 'Verify', and 'Update' buttons.

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)

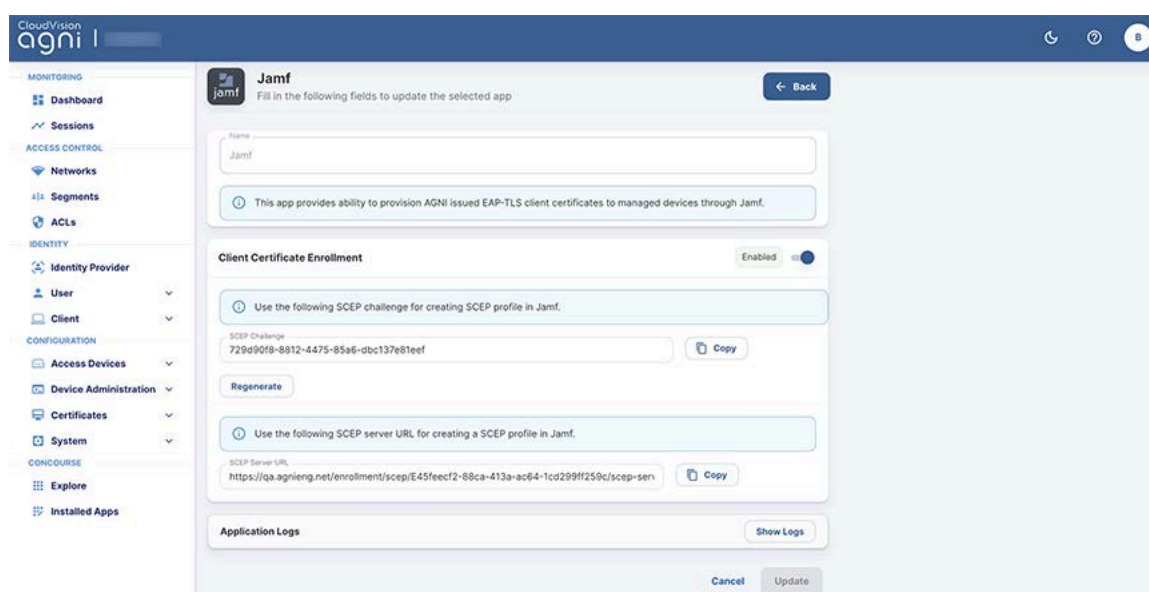


Figure: Installing Jamf Concourse Application

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)

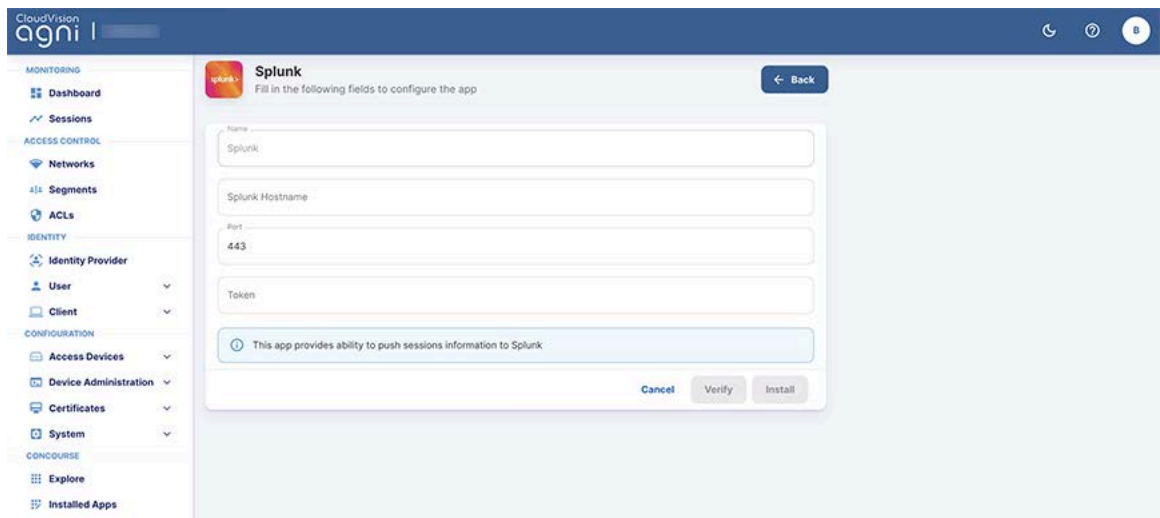


Figure: Installing Splunk Concourse Application

3. Enter the following parameters:
4. Splunk in the **Name** field
5. Splunk Hostname
6. Port (default is 443)
7. 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)

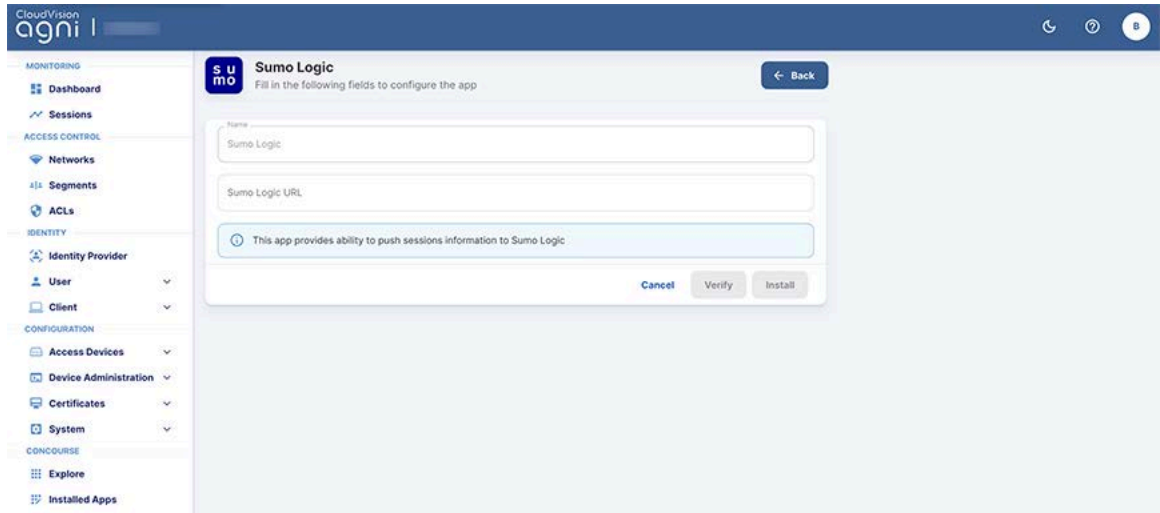


Figure: Installing Sumo Logic Concourse Application

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.

CrowdStrike Integration

CrowdStrike is an Enterprise Endpoint Protection solution for managing corporate-owned devices. AGNI works with CrowdStrike using the Concourse App Framework. CrowdStrike provides the functionality to create credentials to access the APIs.

For details on CrowdStrike, see the vendor documentation.

To install CrowdStrike on AGNI:

1. Access the **AGNI** tile from the CV-CUE launchpad.
2. Navigate to **Concourse > Explore**, click the **CrowdStrike** tile to install the application.
3. Add the **API URL**, **API CLIENT ID**, and **API Client Secret** code configured in **CrowdStrike** Server in the previous section and click the **Verify** button to verify the application.

Event Notification

- The Event Notification enables AGNI to receive notification status from CrowdStrike whenever the device details change.
Copy and save the **Notification URL** and **Notification Secret** (required while configuring CrowdStrike Falcon Console).

Workspace ONE integration

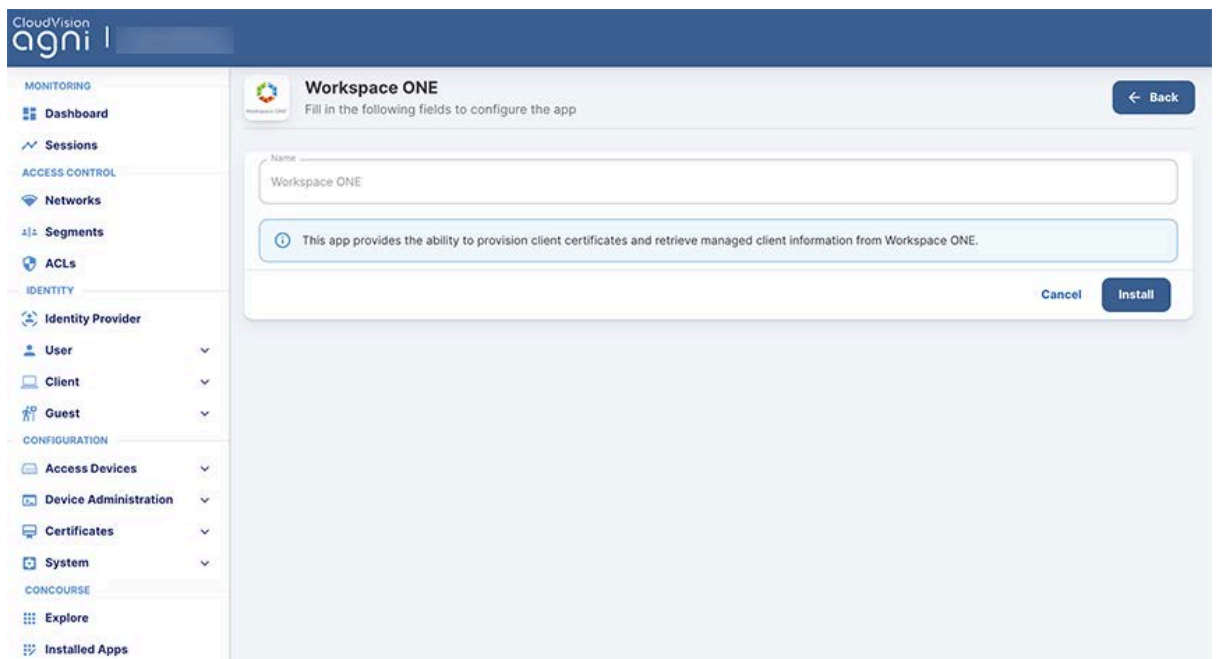
Workspace ONE is an enterprise Mobile Device Management (MDM) solution to manage corporate owned devices. Arista Guardian for Network Identity (AGNI) integrates with Workspace ONE by using the Concourse App framework.

The integration of Workspace ONE with AGNI provisions the certificates and Wi-Fi profiles of the managed clients for connecting to an EAP-TLS network.

Pre-Requisite: To configure Workspace ONE, first generate a client ID or Secret key. Workspace ONE provides the functionality to create credentials for accessing the APIs. For details, see the vendor documentation.

To install the Workspace ONE application:

1. Access the **AGNI** tile from the CV-CUE launchpad.
2. Go to **Concourse > Explore**, and click the **Workspace ONE** card to install the application.
3. Click the **Install** button.

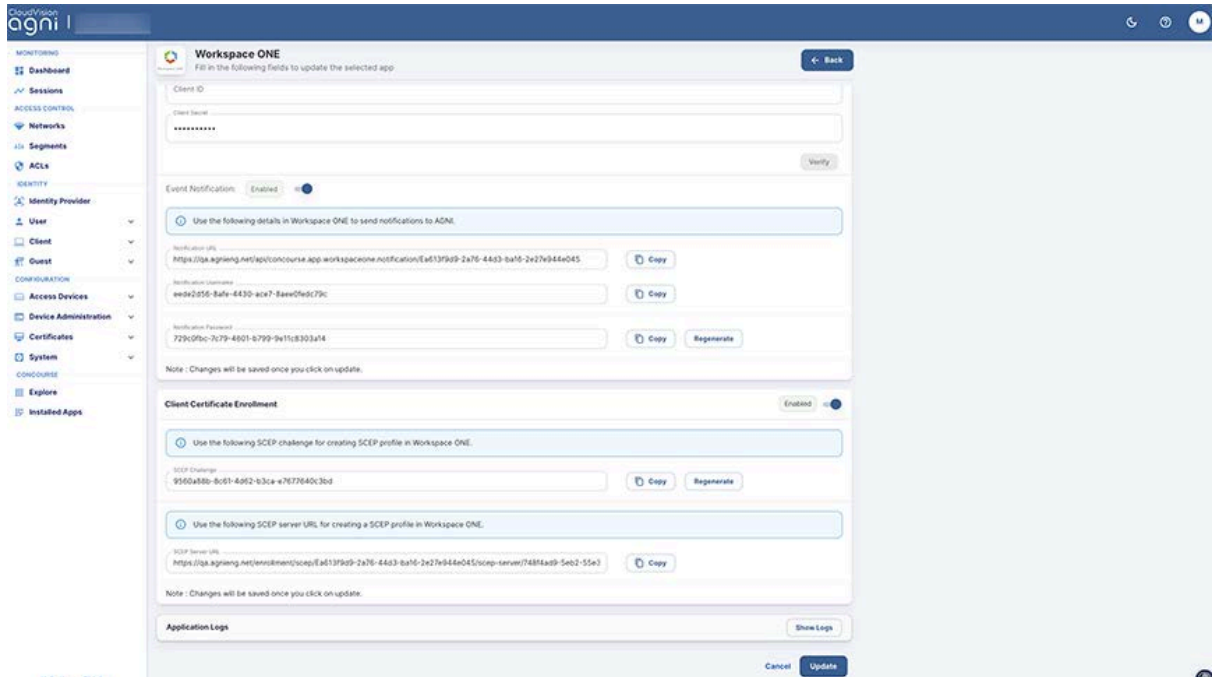


4. Enable the **Client Information Synchronization** if you use compliance policies with *Workspace ONE*. This enables AGNI to retrieve the compliance status and compromised status for each managed device upon authentication.
5. Add the **API URL**, **CLIENT ID**, and **Client Secret** to verify and install Workspace ONE on AGNI. This information was saved while configuring

Workspace ONE earlier. See the Generating ClientID/Secret Key section above.

The screenshot shows the AGNI console interface for configuring a Workspace ONE application. The left sidebar contains navigation menus for Monitoring, Access Control, and Identity. The main content area is titled "Workspace ONE" and includes a "Back" button. Below the title, there is a "Name" field containing "Workspace ONE" and a descriptive note: "This app provides the ability to provision client certificates and retrieve managed client information from Workspace ONE." The "Client Information Synchronization" section has a toggle switch set to "Enabled" and fields for "API URL", "Client ID", and "Client Secret". A "Verify" button is located below the "Client Secret" field. The "Event Notification" section has a toggle switch set to "Disabled" and a note: "Enable to allow Workspace ONE to send notifications to AGNI for managed clients." The "Client Certificate Enrollment" section has a toggle switch set to "Disabled". At the bottom, there is an "Application Logs" section with a "Show Logs" button and "Cancel" and "Update" buttons.

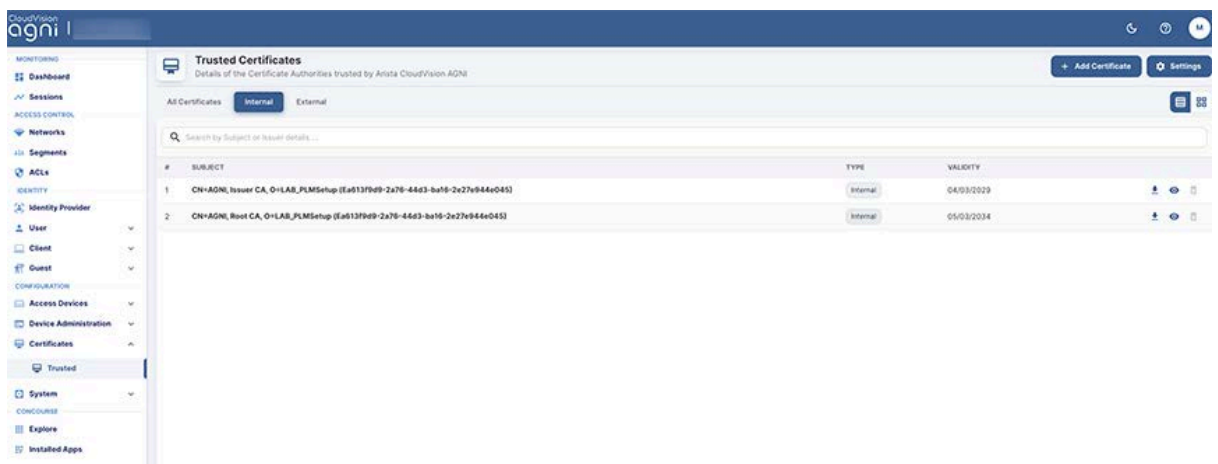
6. Within the Client Information Synchronization settings, enable **Event Notification**. This enables AGNI to receive compliance status & Compromised status from *Workspace ONE* whenever the device details change.
Note: Save the **Notification URL**, **Notification Username**, and **Notification Password**, which is configured on Workspace ONE Settings.
7. Enable the **Client Certificate Enrollment** and copy and save the **SCEP URL** and **SCEP Challenge** to be required later for configuring Workspace ONE.



Downloading Issuer and Root Certificates for AGNI CA

To download the Issuer and Root certificates:

1. Navigate to **Configuration > Certificates > Trusted** from the AGNI dashboard. Click the **Internal** tab (see image below).



2. Download the Agni Issuer certificate and save it as **agni-Issuer.cer**.
3. Download the Agni Root certificate and save it as **agni-Root.cer**.

For complete details on the Workspace ONE integration and configuration, see the How to document on Arista Community Central.

Configuring 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.

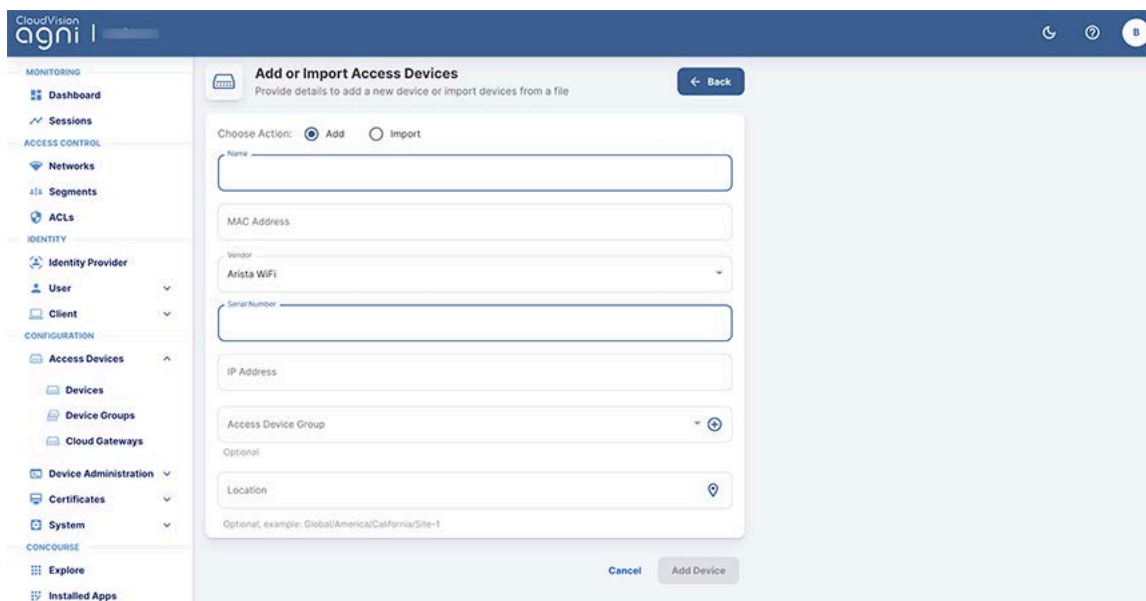
For details on the concourse plugin installation, see the [Third-party Integrations](#) section.

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.



The screenshot shows the 'Add or Import Access Devices' form in the AGNI portal. The form is titled 'Add or Import Access Devices' and includes a subtitle 'Provide details to add a new device or import devices from a file'. There is a 'Back' button in the top right corner. The form has two radio buttons for 'Choose Action': 'Add' (selected) and 'Import'. The form fields are: 'Name' (text input), 'MAC Address' (text input), 'Vendor' (dropdown menu with 'Arista WiFi' selected), 'Serial Number' (text input), 'IP Address' (text input), 'Access Device Group' (dropdown menu), and 'Location' (text input with a location pin icon). Below the 'Location' field, there is a note: 'Optional, example: Global/America/California/Site-1'. At the bottom of the form, there are 'Cancel' and 'Add Device' buttons. The left sidebar of the portal shows a navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Devices, Device Groups, Cloud Gateways, Device Administration, Certificates, System), and CONCOURSE (Explore, Installed Apps).

Figure: Adding a Device

Importing Devices in Bulk to AGNI

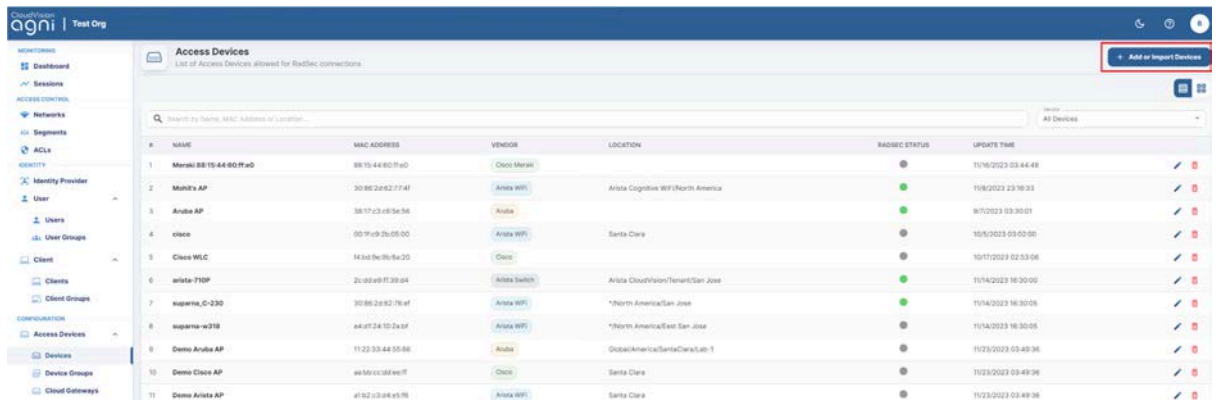
This section describes the steps to import Network Access Devices (NAD) in bulk to AGNI. The network access devices are added under the **Access Devices** tab.

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:

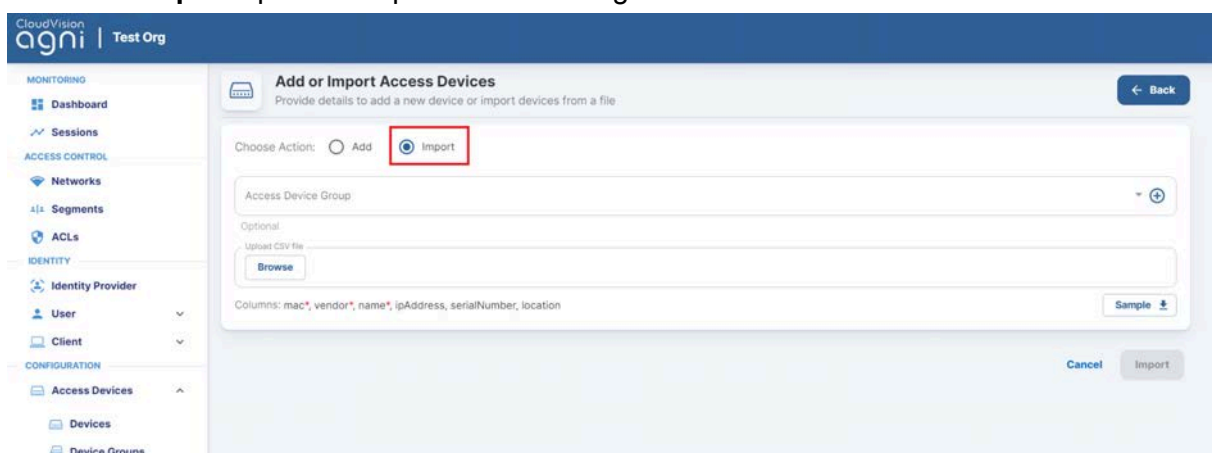
1. Log in to AGNI and Navigate to **Access Devices-> Devices**. Click the **Add or Import Devices** option (see image below).



#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADIUS STATUS	UPDATE TIME
1	Meraki 8810-44-8011a0	8810448011a0	Cisco Meraki		●	11/16/2023 03:44:48
2	Mobily AP	30862462774f	Arista WFI	Arista Cognitive WFI(North America)	●	11/16/2023 23:16:33
3	Aruba AP	3817c3a85e5d	Aruba		●	9/10/2023 03:30:01
4	cisco	001f492b0500	Arista WFI	Santa Clara	●	10/6/2023 09:03:00
5	Cisco WLC	143d8e9c6a35	Cisco		●	10/11/2023 02:53:06
6	arista-710P	2c00a9113904	Arista Switch	Arista CloudVision/Tenant/San Jose	●	11/14/2023 16:30:00
7	superna_C-230	30862462774f	Arista WFI	*North America/San Jose	●	11/14/2023 16:30:06
8	superna-w216	4d47124102af	Arista WFI	*North America/San Jose	●	11/14/2023 16:30:06
9	Demo Aruba AP	112233445566	Aruba	Global/America/Santa Clara/lab-1	●	11/23/2023 03:49:36
10	Demo Cisco AP	4d36cc38aef8	Cisco	Santa Clara	●	11/23/2023 03:49:36
11	Demo Arista AP	4f82c388a576	Arista WFI	Santa Clara	●	11/23/2023 03:49:36

Figure: Importing Devices

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



CloudVision agni | Test Org

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client

CONFIGURATION

- Access Devices
 - Devices
 - Device Groups

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: [Dropdown]

Optional

Upload CSV file: [Browse]

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

[Sample]

[Cancel] [Import]

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).

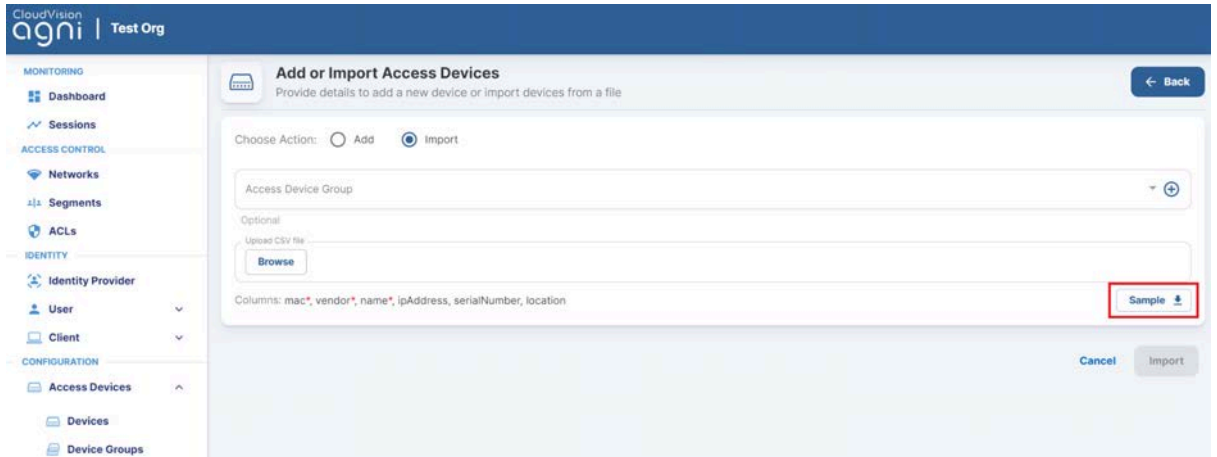


Figure: Add or Import Devices-2

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).

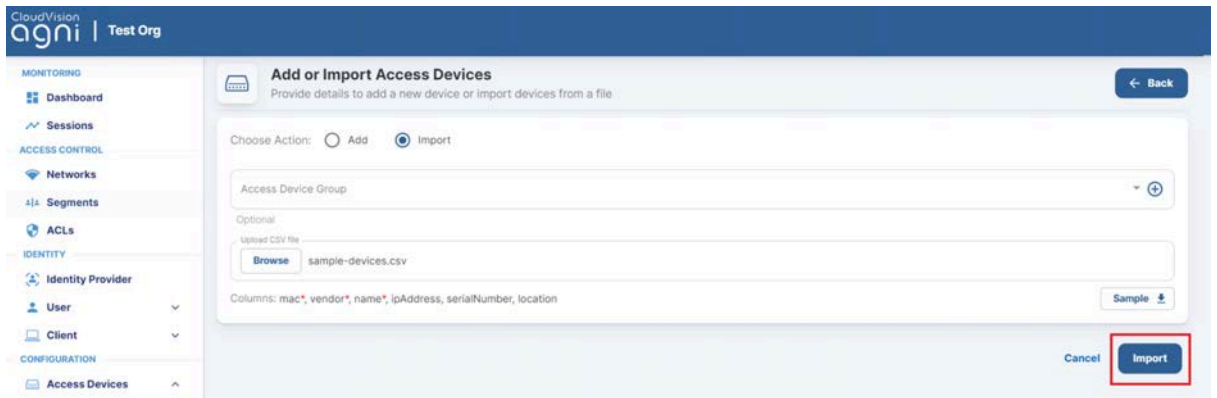


Figure: Add or Import Devices-3

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.

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADIUS STATUS	UPDATE TIME
1	Meraki 8815-44-801f-a0	8815.44.801f.a0	Cisco Meraki		●	11/16/2023 03:44:48
2	Mubury AP	30.85.2a62.77.4f	Arista WFI	Arista Cognitive WFI/North America	●	11/8/2023 13:16:33
3	Arista AP	3817.13.18.54.36	Arista		●	9/7/2023 03:30:01
4	cisco	001f.92b.05.00	Arista WFI	Santa Clara	●	10/5/2023 09:02:00
5	Cisco WLC	163d.9e.9b.84.20	Cisco		●	10/17/2023 02:13:06
6	arista-710P	20.89.a9f1.39.04	Arista Switch	Arista CloudVision/Tenant/San Jose	●	11/14/2023 16:30:00
7	superna_c-230	30.86.2a62.76.4f	Arista WFI	*North America/San Jose	●	11/14/2023 16:30:06
8	superna-w318	a4.0f.24.10.2a.8f	Arista WFI	*North America/East San Jose	●	11/14/2023 16:30:05
9	Demo Arista AP	11.22.33.44.55.66	Arista	GlobalAmerica/SantaClara-1	●	11/23/2023 03:49:38
10	Cisco AP	a4.0f.24.10.2a.8f	Cisco	Santa Clara	●	11/24/2023 15:29:33
11	Arista AP	a782.13.08.a5.16	Arista WFI	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	a4.0f.24.10.2a.8f	Demo	San Jose	●	11/23/2023 03:49:36
14	Demo Cisco Meraki	a4.0f.24.10.2a.8f	Cisco Meraki	Mountain View	●	11/23/2023 03:49:36
15	Arista C-75	0011.14.1f.4d.0f	Arista WFI	GlobalAmerica/SantaClara-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 article explains the process of configuring TACACS+ with AGNI. Before configuring TACACS+ with AGNI the network administrator should first configure the Arista Cloud Gateway (ACG) solution, which provides greater security in accessing the public internet. The Arista Cloud Gateway solution integrates with AGNI over secure web sockets.

The image below illustrates that 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 or 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 the below sections.

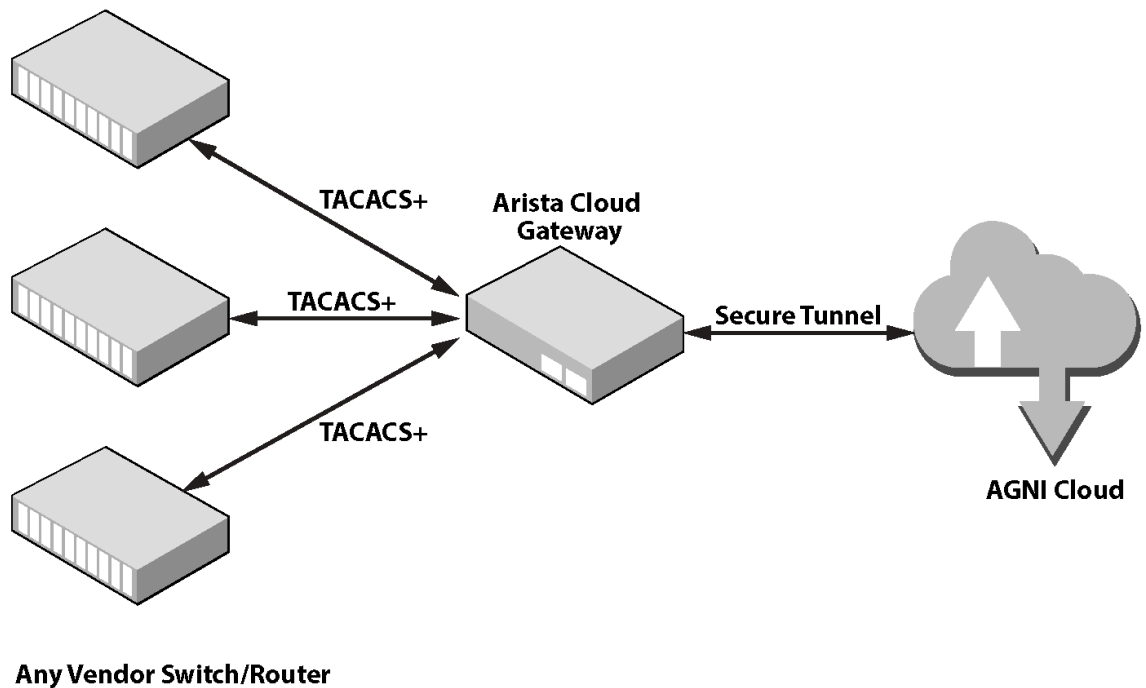


Figure: Arista Cloud Gateway Solution

Configuring Arista Cloud Gateway on Arista Switches

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

```

Copy the Arista Cloud Gateway file to the system flash:
  scp .\AristaCloudGateway-1.0.0-1.swix
  admin@192.168.1.10:/mnt/flash

copy flash:AristaCloudGateway-1.0.0-1.swix extension:
extension AristaCloudGateway-1.0.0-1.swix

show extensions

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



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

The below snapshot displays 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 5: Running TACACS+ on non-Standard Port

Note: If you want to change the default VRF option, use the CLI command below:

```
option AGNI_ACG_VRF value <vrf_name>
```

```
[agni-720dp-24-1(config-daemon-AristaCloudGateway)#
[agni-720dp-24-1(config-daemon-AristaCloudGateway)#
[agni-720dp-24-1(config-daemon-AristaCloudGateway)#option AGNI_ACG_VRF value management
[agni-720dp-24-1(config-daemon-AristaCloudGateway)#no shutdown
This is an EosSdk application
Full agent name is 'acg-AristaCloudGateway'
[agni-720dp-24-1(config-daemon-AristaCloudGateway)#trace monitor acg
```

```
agni-720dp-24-1(config-daemon-AristaCloudGateway)#trace monitor acg
--- Monitoring /var/log/agents/acg-AristaCloudGateway-14082 ---
2024/01/10 21:21:26 INFO [nad=10.81.204.5] tacacs(AGNI) - send-recv completed, reply(17 bytes) in 48.893659ms
2024/01/10 21:21:26 INFO [nad=10.81.204.5] tacacs - conn closed by remote end
2024/01/10 21:21:26 INFO [nad=10.81.204.5] tacacs - closed tcp conn after 49.521013ms
2024/01/10 21:21:26 DEBUG [swix] restricting port [49] on vrf [management]
2024/01/10 21:21:26 DEBUG [swix] restricted port [49] on vrf [management]
2024/01/10 21:21:26 DEBUG [swix] acg service stopped
2024/01/10 21:21:28 DEBUG [swix] handling agent shutdown/no shutdown: True
2024/01/10 21:21:28 DEBUG [swix] allowing port [49] on vrf [management]
2024/01/10 21:21:28 DEBUG [swix] allowed port [49] on vrf [management]
2024/01/10 21:21:28 DEBUG [swix] setting-up acg service. wait for 10s
2024/01/10 21:21:38 DEBUG [swix] starting acg service
```

Configuring Arista Cloud Gateway on AGNI

To configure Arista Cloud Gateway on AGNI:

- Navigate to **Configuration**→**Access Devices**→**Cloud Gateways**.
- Click **+Add Cloud Gateway** button 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 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

Cancel Add Cloud Gateway

Figure: Adding a New Cloud Gateway

- Enter a name and click **Add Cloud Gateway** button at the bottom of the page to generate a Token.
- Copy and save this token. To establish an HTTPS connection with AGNI, you must input it on the Arista Cloud Gateway running on the Arista Switch.
- Click **Update Cloud Gateway**.

Cloud Gateway-1

Provide the following details to update the selected Cloud Gateway

← Back
⋮

Name

Location

📍

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

Connection Status: Not Connected

📘
Copy the generated token into the Cloud Gateway.

Token

📄 Copy

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
<input style="width: 90%; border: none; border-bottom: 1px solid #ccc;" type="text" value="AristaSwitch"/>	<input style="width: 90%; border: none; border-bottom: 1px solid #ccc;" type="text" value="....."/> 👁️ 📄 ✕

➡ Add Secret

Cancel
Update Cloud Gateway

Figure: Updating the Cloud Gateway

Note: For security reasons, the generated token is visible only for the first time on 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.

Regenerate

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

Add Secret

Cancel **Update Cloud Gateway**

Figure: Regenerate Token

When 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, the “`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

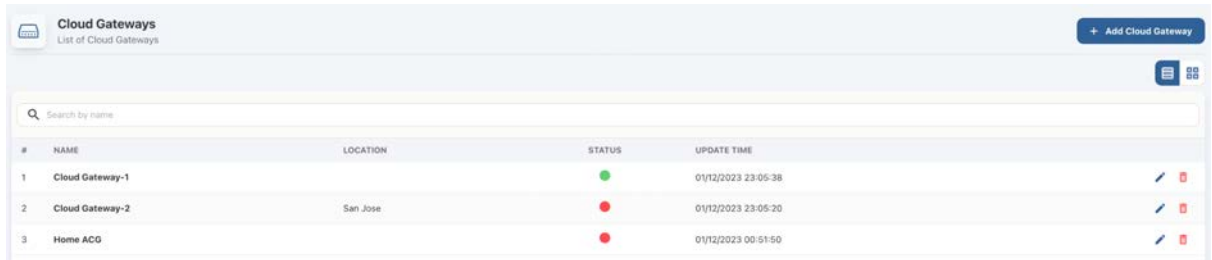
Location:

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

Connection Status: **Connected**

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

Regenerate



#	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

Note: If you are deploying multiple Arista Cloud Gateways on different EOS switches, then each of them should be added on AGNI portal. For each Cloud Gateway added in AGNI, a unique token is generated and this token should be added to the Arista Cloud Gateways running on the respective Arista Switches.

Configuring TACACS+ on Arista Switches

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

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

Note: The `shared_secret` should be the same shared secret provided while adding the Arista Cloud Gateway 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, acting as a TACACS+ Proxy.

Note: If you are using a non-default VRF, then use the following commands:

```
tacacs-server host <IP_ACG> vrf <vrf_name> key
    <shared_secret>
aaa group server tacacs+ agni-tacacs
Server <IP_ACG> vrf <vrf_name>
```

For authentication, authorization, and accounting (AAA), use the commands below:

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

Debug commands on Arista Cloud Gateway

Below are some sample debug commands that can be useful during 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
```

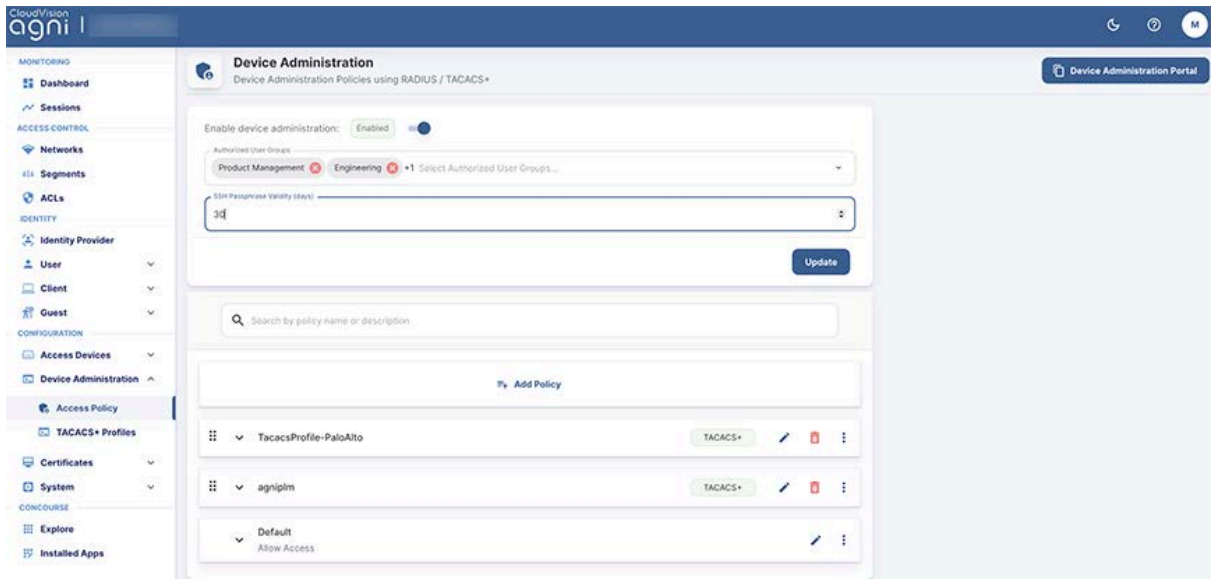
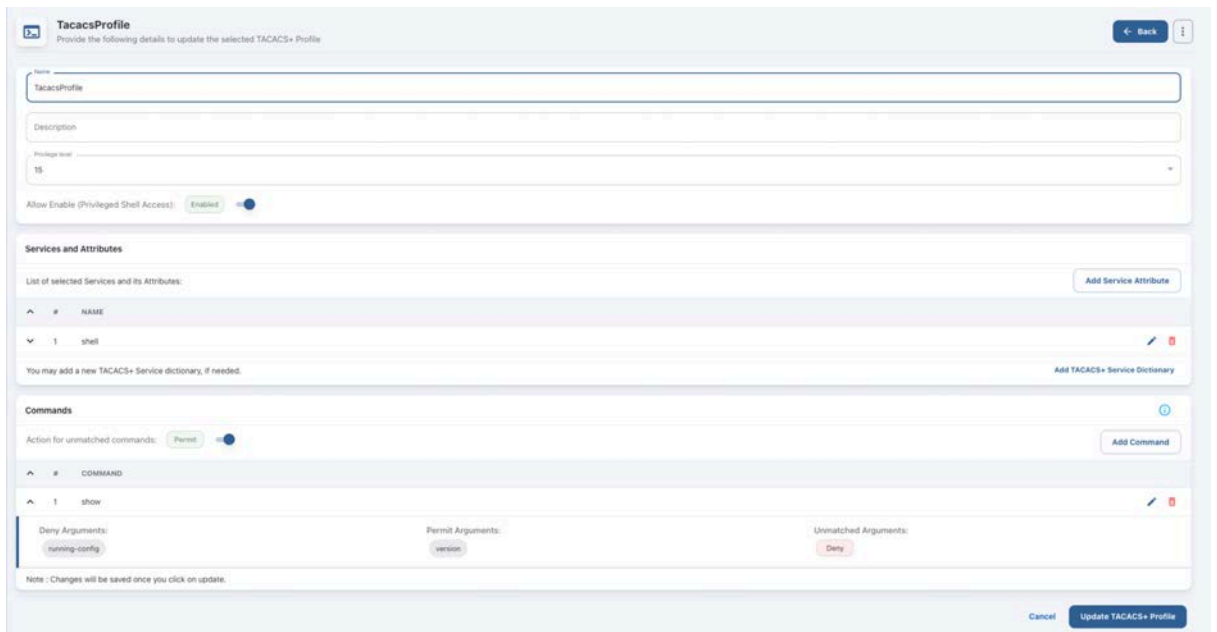



Figure: Device Administration Enabled and Passphrase Validity

Configuring TACACS+ on AGNI

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

You can create TACACS+ Profiles by navigating to **Device Administration** → **TACACS+ Profiles**. Click the **+Add TACACS+ Profile** button. The Add TACACS+ Profile page is displayed (see image below).



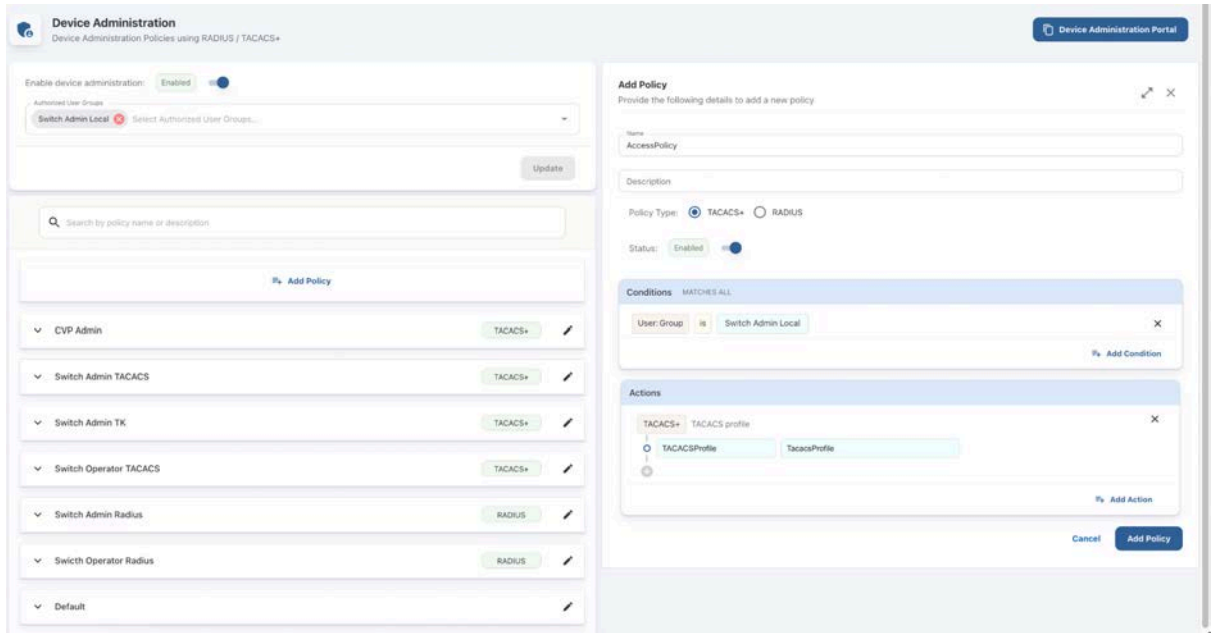


Figure: Creating TACACS+ Profiles

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

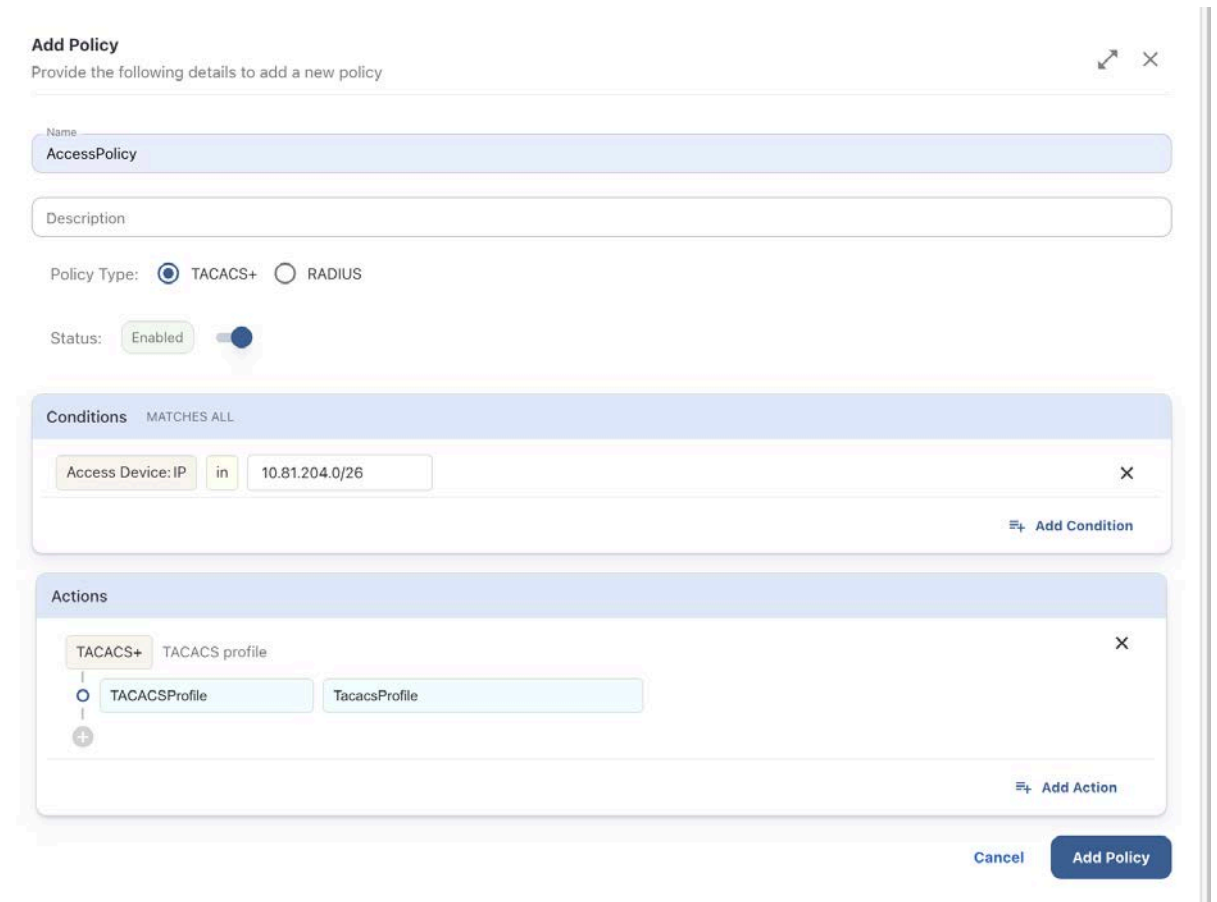


Figure: Creating TACACS+ Policy Details

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+ Policy Details-Conditions

Monitoring TACACS+ on AGNI

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

The screenshot displays the 'Session Details' interface for a TACACS+ session. The session ID is 'Tclnm60c88nsc72qekc50'. The interface is divided into several sections:

- Authentication Request:** Shows 'Success' status. Fields include Authentication Type (TACACS+), Policy (Switch Admin TACACS), and Location (San Jose).
- Request Details:** Shows NAS IP Address (10.81.204.5), Request Time (05/12/2023 23:20:57.448), and TACACS+ Profile Name (TacacsProfile).
- User:** Shows 'Enabled' status and the username 'tarun'.
- Access Device:** Shows 'Not available'.
- Cloud Gateway:** Shows 'Connected' status and details: CloudGateway - 10.81.204.7, San Jose.
- Input Request Attributes:** A dropdown menu.
- Output Response Attributes:** A dropdown menu.
- TACACS+ Activity:** A section with a 'Show Activity' button.
- Session logs for request:** A section with a 'Show Logs' button.

The second screenshot shows the same session details but with the 'TACACS+ Activity' section expanded to show a table of activity:

#	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

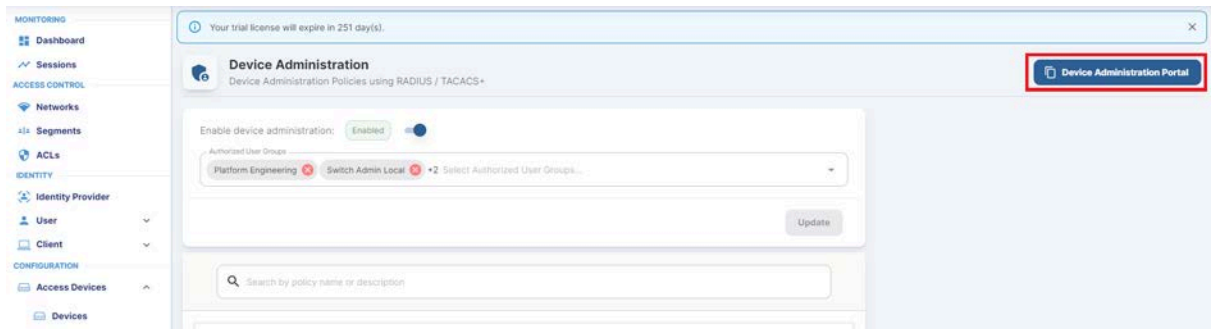
The 'Input Request Attributes' section is also expanded, showing:

- TACACS:AuthnPrivLevel: 1
- TACACS:AuthnService: Login
- TACACS:AuthnType: AuthnTypeASCII

Figure: TACACS+ Session Details

Accessing Self Service Portal on AGNI

To access the Self-Service Portal, the network administrator should navigate to **Device Administration-> Access Policy** and click on the **Device Administration Portal** button.



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 for SSH connection to devices* that should be managed. End users can add a list of frequently accessed devices for device management in the self-service portal by specifying following details:

- **Name** - 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 can be downloaded from the self-service portal.

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

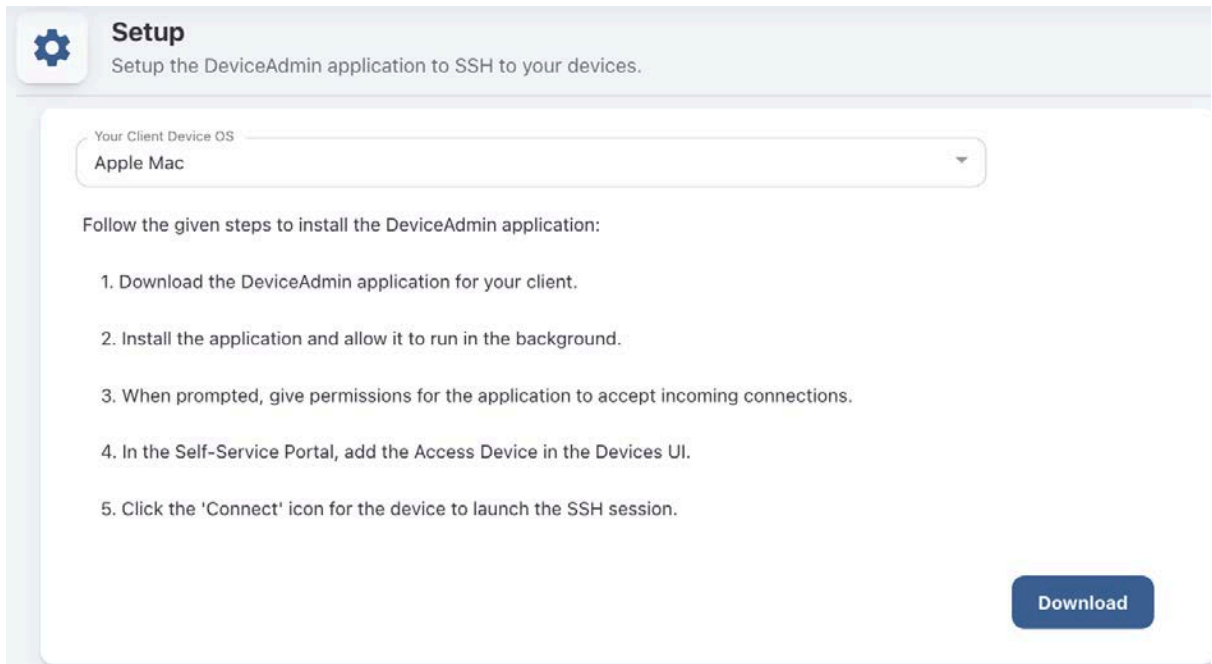


Figure: Self-Service Portal for Mac OS

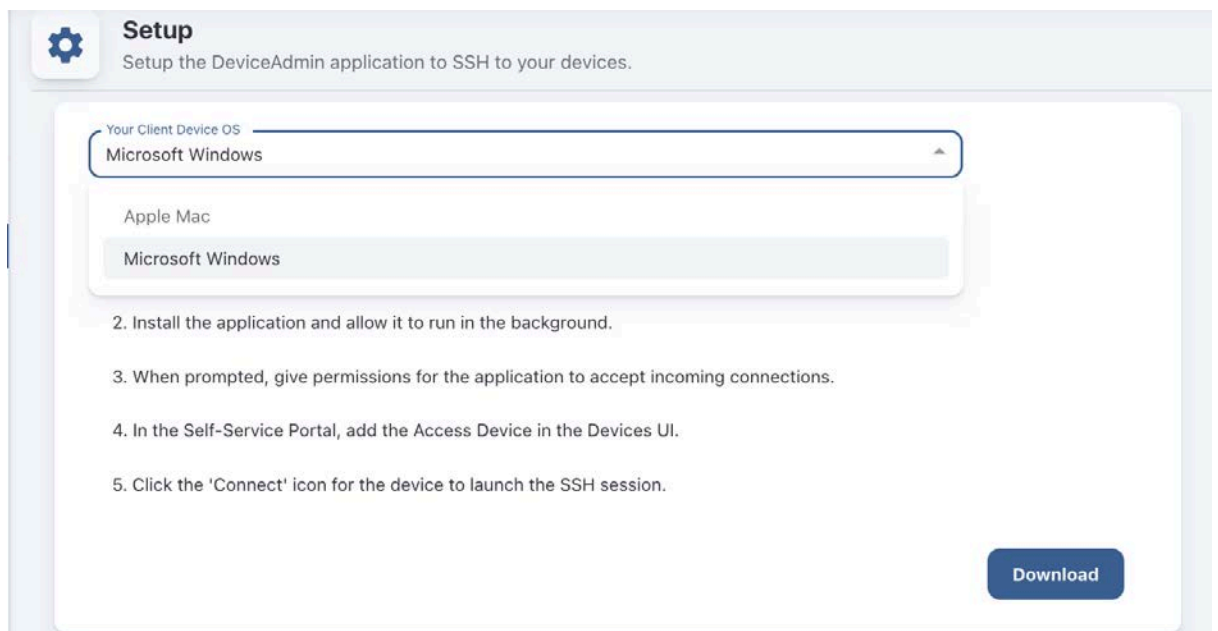


Figure: Self-Service Portal for Windows

After the AGNI app is installed on the laptop, you can add the Devices. Also, you can use the **Import** option to import the devices to AGNI as a .csv file.

Note: The system administrator can initiate SSH sessions from local SSH clients installed on the laptop, such as *PUTTY*, *SecureCRT*, or any other terminal, by navigating to SSH credentials and getting the Session password or TACACS token. If the administrator is using their local SSH clients, then there is no need to add the devices to be managed to the self-service portal.

In cases where end-users have access to the Device Administration feature, they can generate an SSH passphrase that is valid for the duration allowed by the administrator (see the [Enabling Device Administration on AGNI](#) section).

In earlier releases, the SSH passphrase was valid only until the web session was active. However, now the SSH credentials can work for days or even months without expiry as determined by the duration allowed by the administrator.

Generate the SSH credentials using the Self-Service portal (see images below).

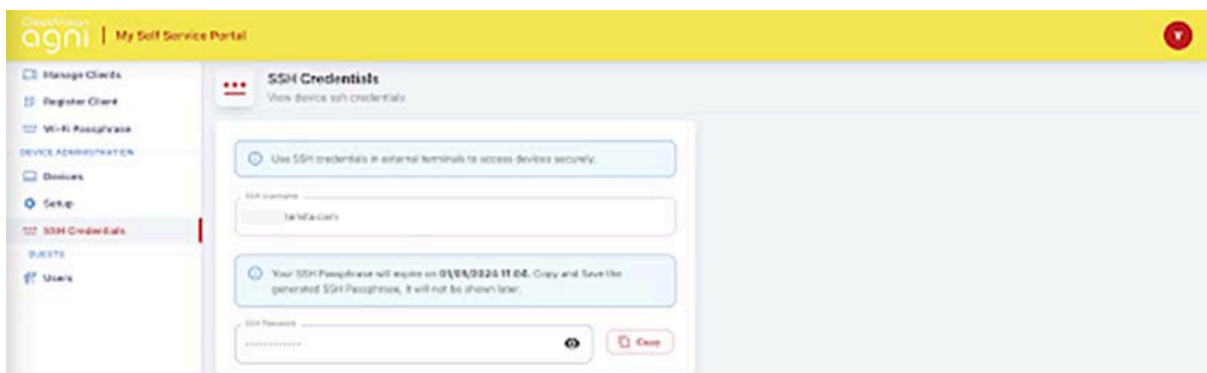
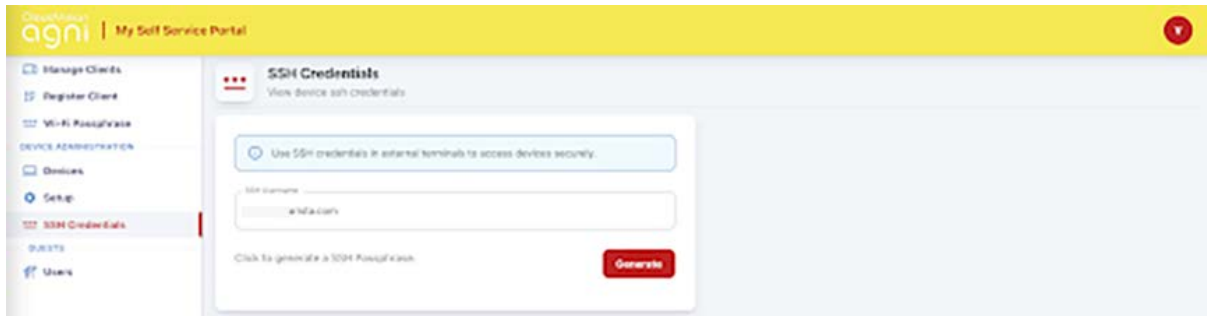


Figure: SSH Credentials

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

```
login as: shrirang@agniplm.onmicrosoft.com
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Tue Feb  6 16:56:22 2024 from 10.86.28.96
IN-MH04-PL-SW04#show interfaces status
% Authorization denied for command 'show interfaces status'
IN-MH04-PL-SW04#show running-config
% Authorization denied for command 'show running-config'
IN-MH04-PL-SW04#show version
Arista CCS-710P-16P
Hardware version: 11.04
Serial number: WTW23230216
Hardware MAC address: 2cdd.e9f6.cd13
System MAC address: 2cdd.e9f6.cd13

Software image version: 4.30.4M
Architecture: i686
Internal build version: 4.30.4M-34191138.4304M
Internal build ID: d92ce5c7-f147-4a0f-a966-5841f64dfc33
Image format version: 3.0
Image optimization: Strata-4GB

Uptime: 5 days, 23 hours and 25 minutes
Total memory: 3960752 kB
Free memory: 2495540 kB

IN-MH04-PL-SW04#
```

Figure: TACACS+ Authorization Allowed and Denied Output

Configuring Cloud Gateway for Integrating AGNI & On-Premises

This section 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.

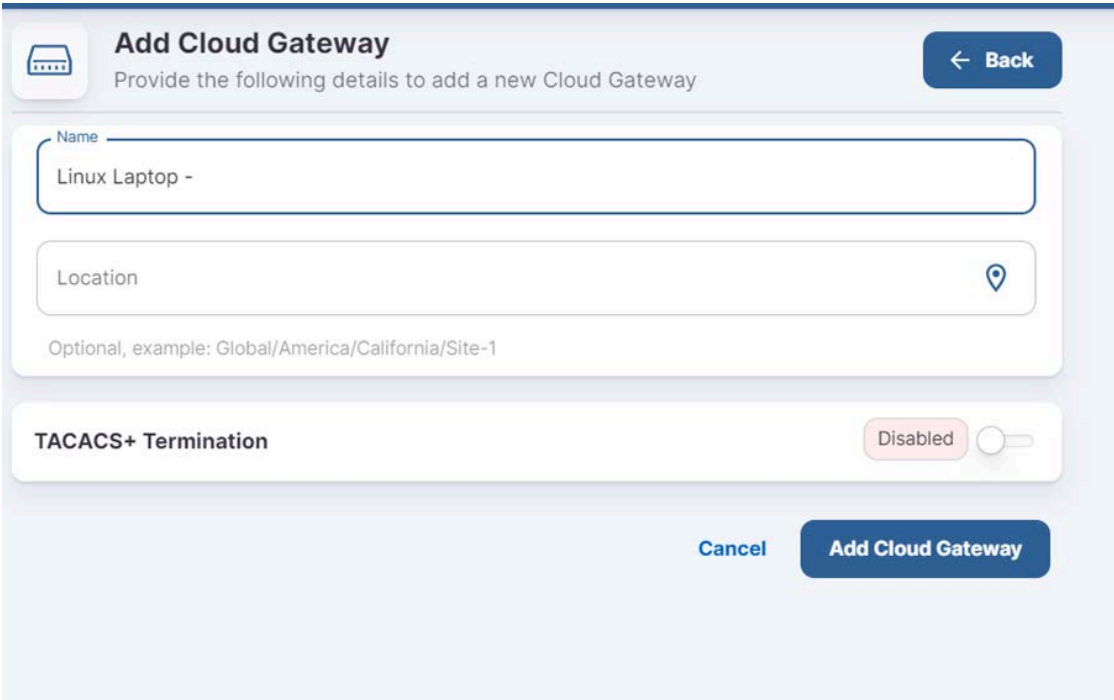
The Cloud Gateway must meet the following requirements:

- 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.



The screenshot shows the 'Add Cloud Gateway' configuration page. At the top, there is a title 'Add Cloud Gateway' and a subtitle 'Provide the following details to add a new Cloud Gateway'. A 'Back' button is in the top right. The form contains three main sections: 1. 'Name' field with the value 'Linux Laptop -'. 2. 'Location' field with a location pin icon and a note: 'Optional, example: Global/America/California/Site-1'. 3. 'TACACS+ Termination' section with a 'Disabled' toggle switch. At the bottom, there are 'Cancel' and 'Add Cloud Gateway' buttons.

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.

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.

Regenerate

TACACS+ Termination Disabled

Cancel Update Cloud Gateway

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.

The screenshot shows a web interface titled "Cloud Gateways" with a sub-header "List of Cloud Gateways". Below the header is a search bar labeled "Search by name". A table below the search bar lists the gateways. The table has columns for "#", "NAME", "LOCATION", "STATUS", and "UPDATE TIME". There is one entry in the table:

#	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
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).

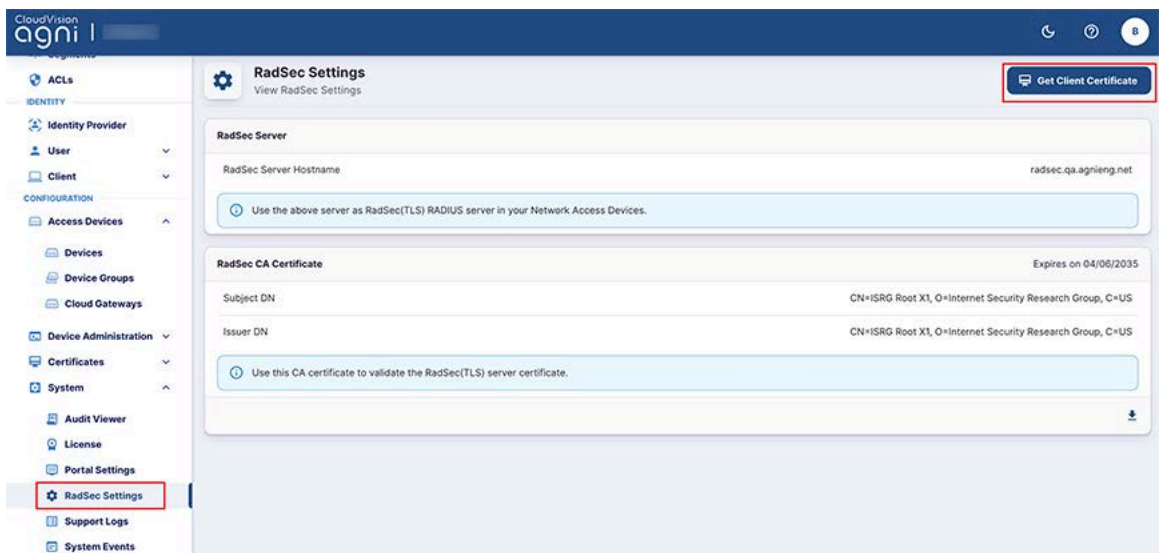


Figure: RadSec Settings Certificate Generate Page

OR

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

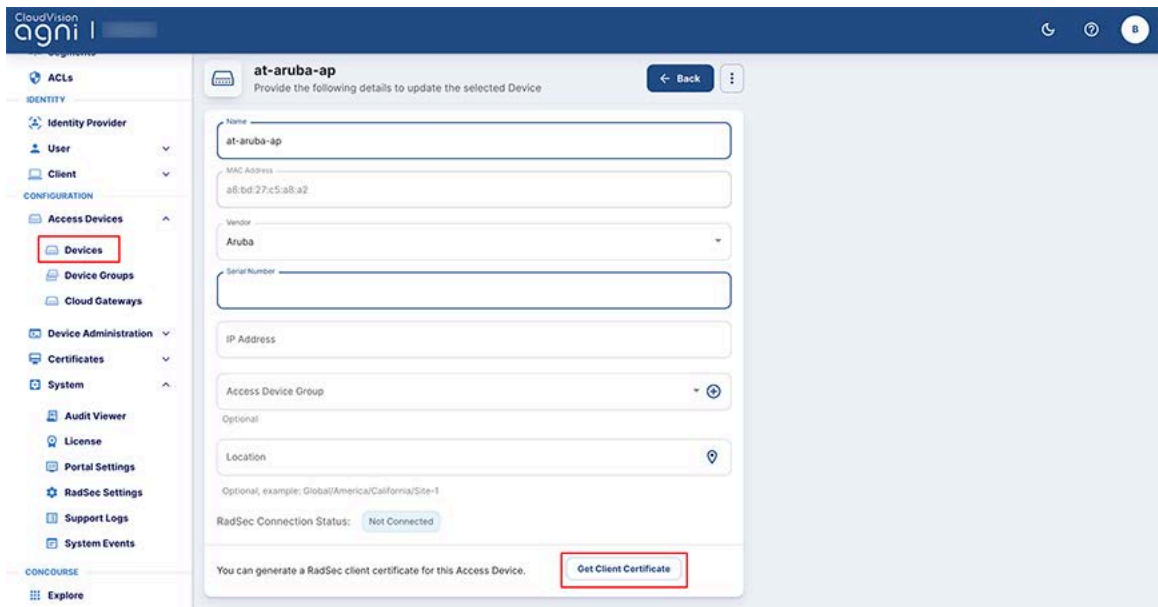


Figure: Device Settings Certificate Generate Page

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.
Note: By default, the generated certificate for Network Access Devices (NAD) is valid for a period of three years (previously valid for one year only).
- 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.

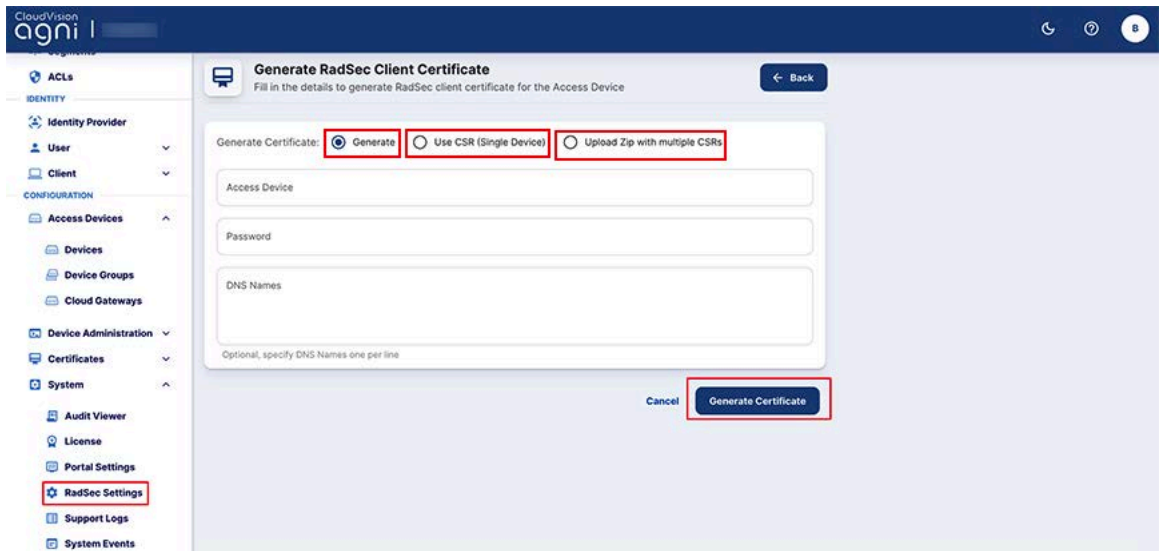


Figure: RadSec Client Certificate Generating Options

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

- o Name of the device
- o MAC address of the device
- o Select the Vendor
- o Enter Serial Number of the device (mandatory for Cisco Meraki devices)
- o 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.

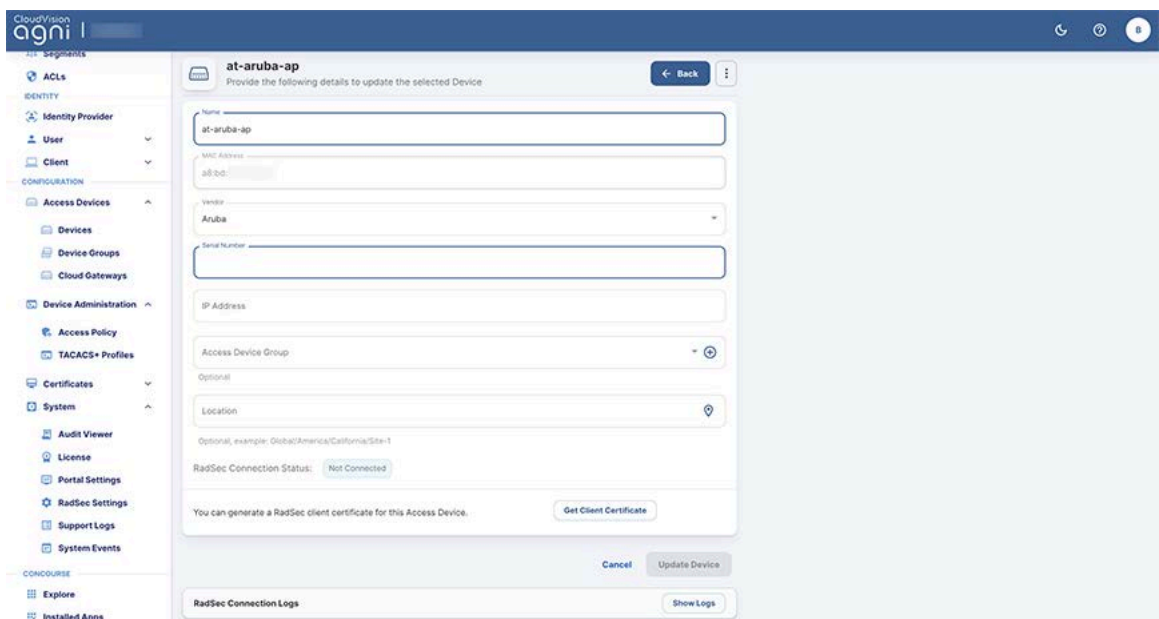


Figure: Device Details

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.

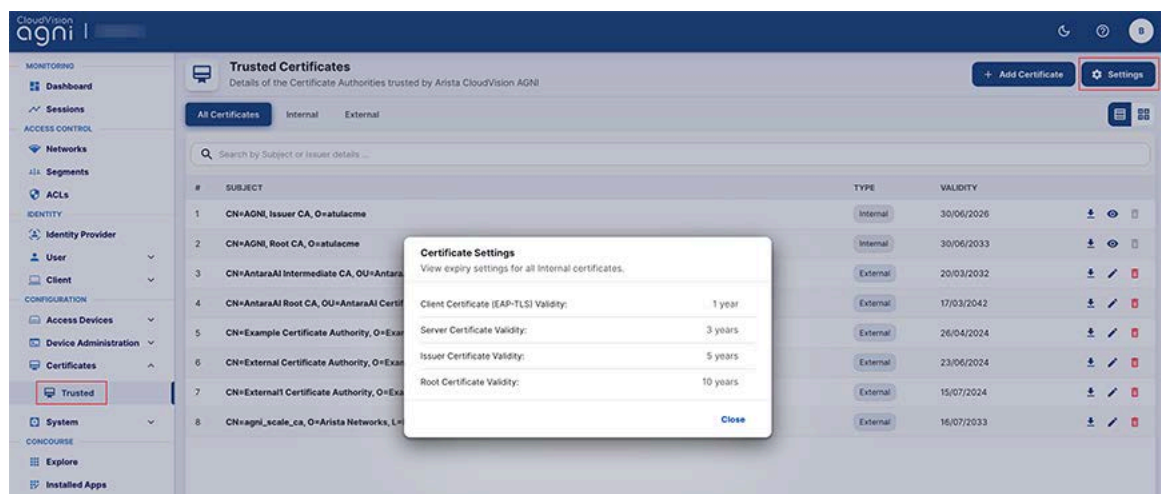


Figure: Trusted Certificates

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)

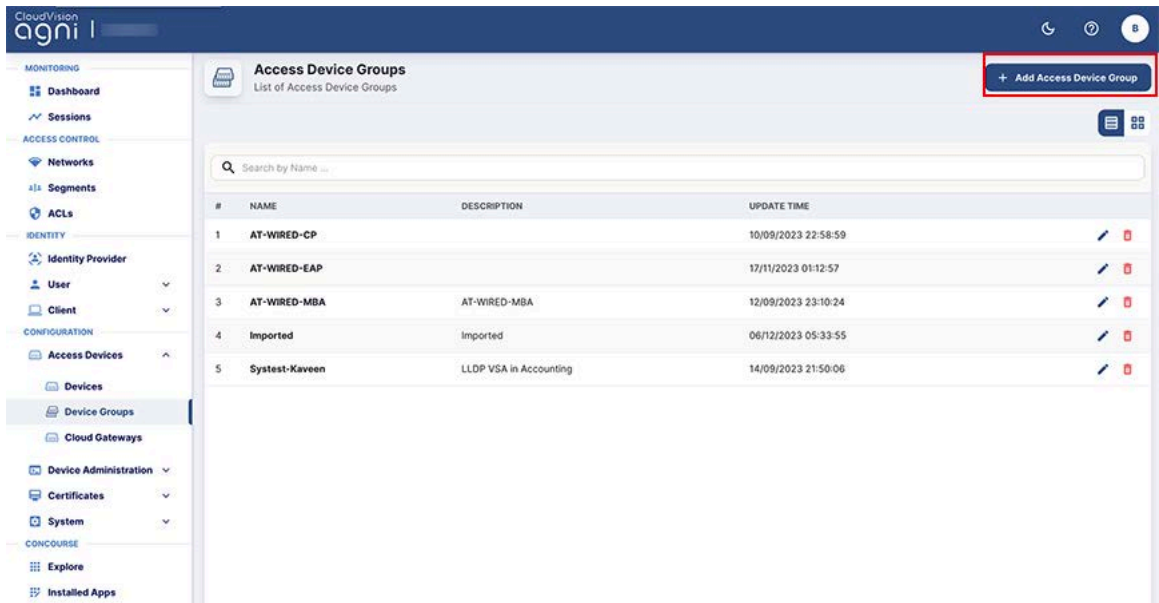


Figure: Access Device Groups

- 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.

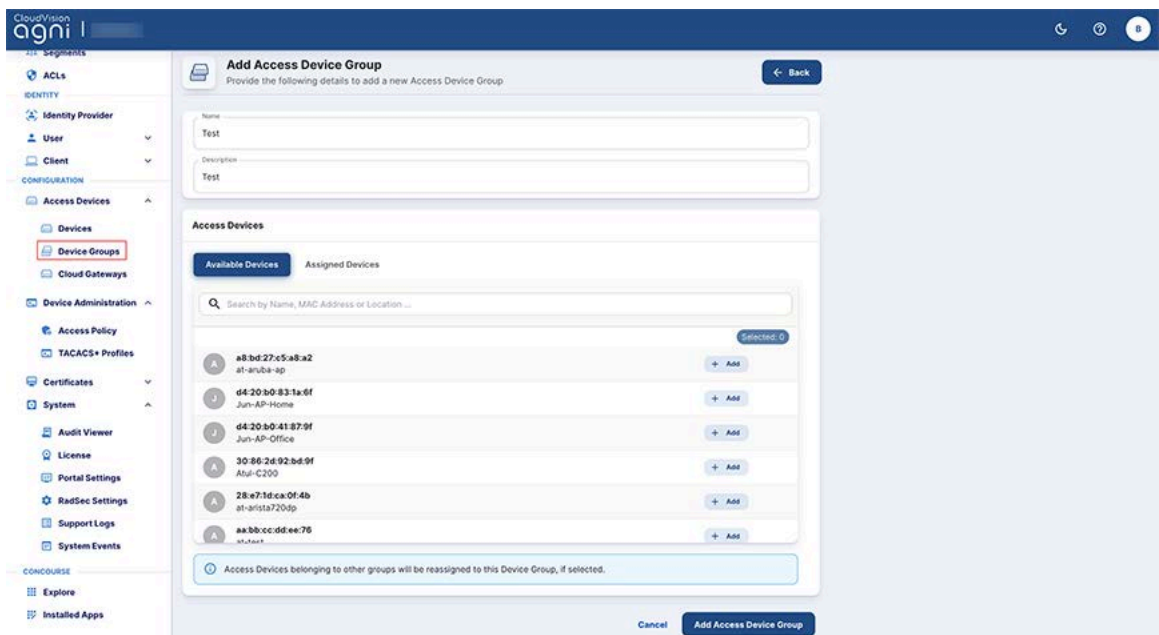


Figure: Adding Access Device Groups

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.

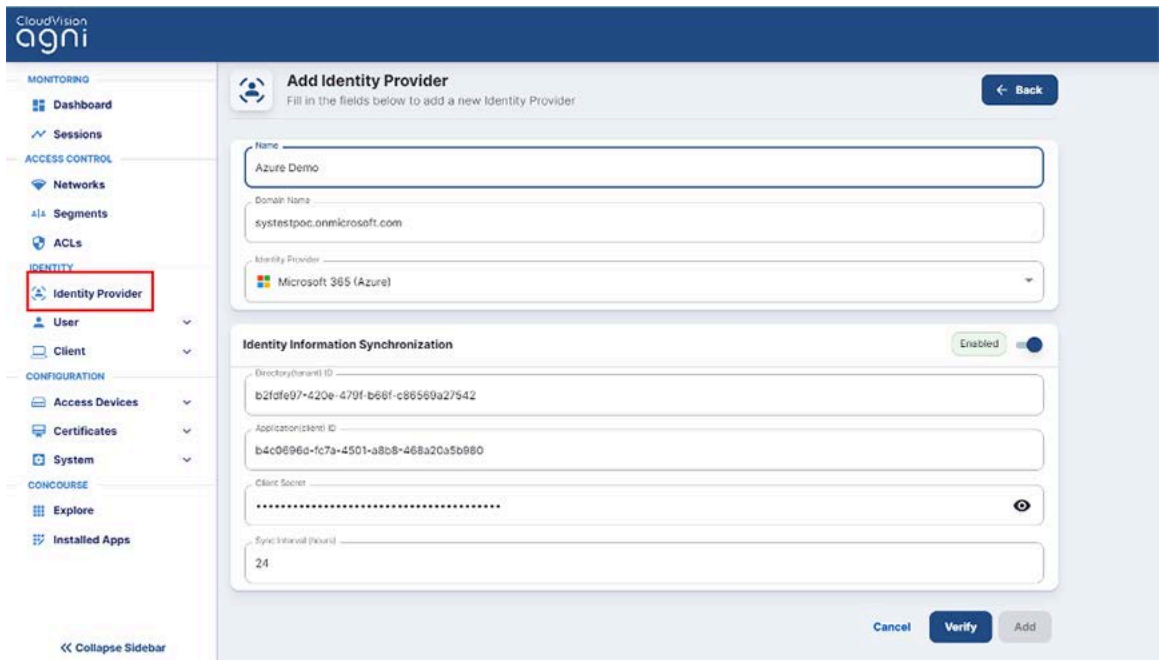


Figure: Adding Identity Provider

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

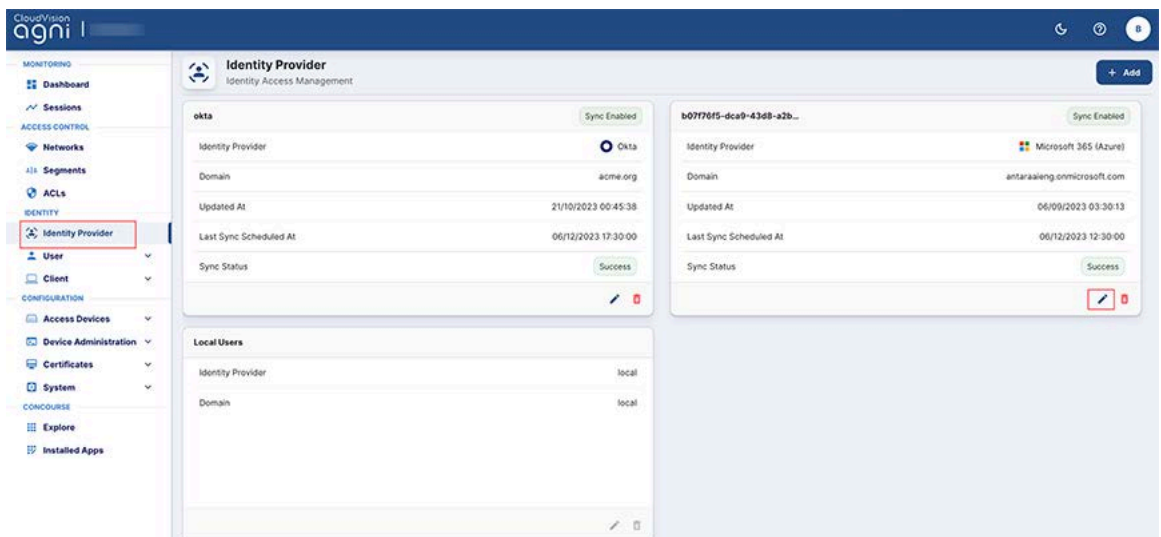


Figure: Edit or Update Identity Provider

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.

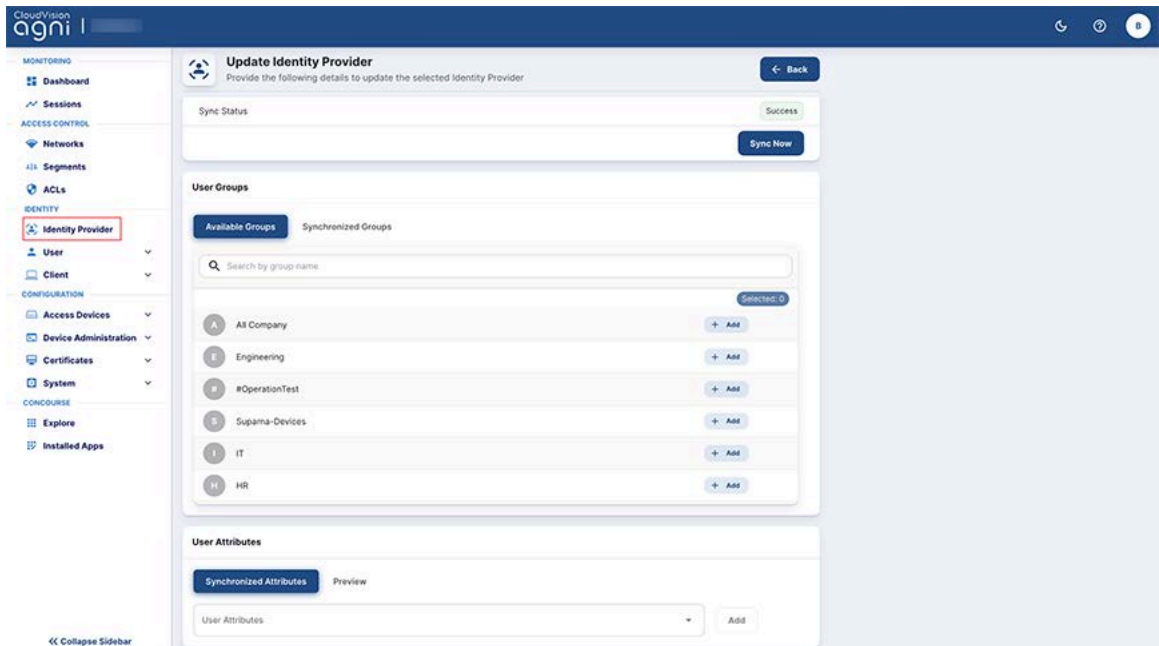


Figure: Identity Provider Available Groups

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.

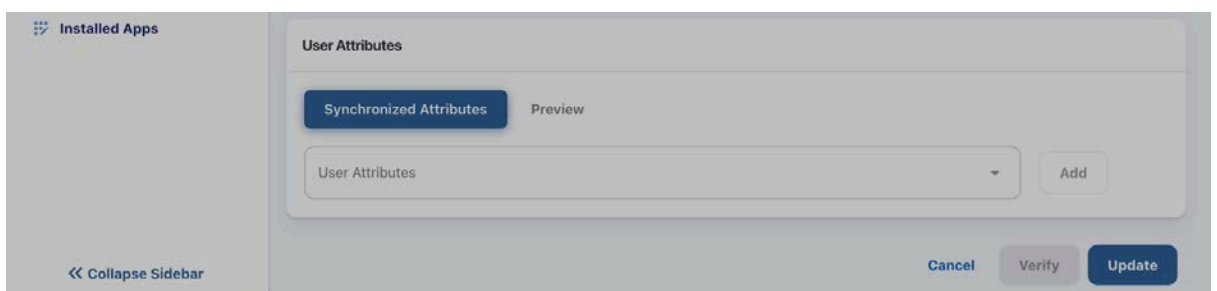


Figure: Identity Provider and User Attributes

- **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.

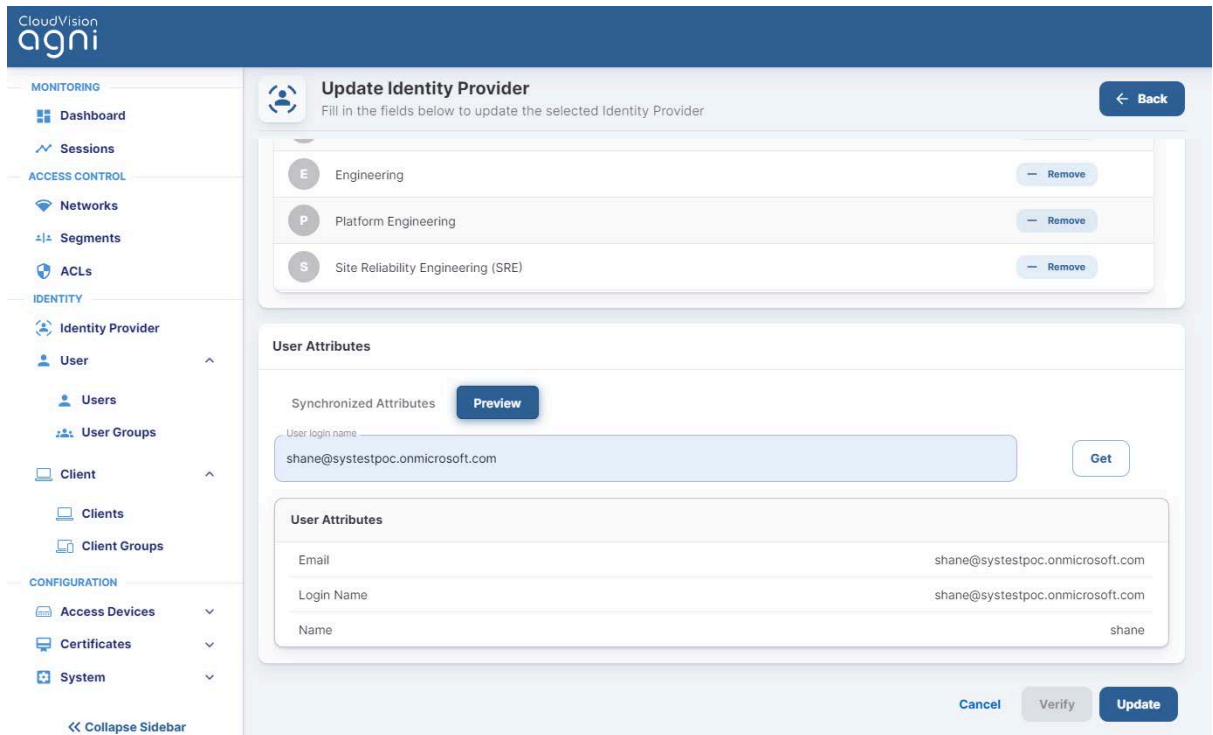


Figure: Identity Provider and User Preview

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**

The screenshot displays the 'Add Identity Provider' configuration interface in the CloudVision agni dashboard. The interface is organized into several sections:

- Form Fields:**
 - Name:** One-Login Demo
 - Domain Name:** myorg1.com
 - Identity Provider:** OneLogin (selected from a dropdown menu)
- Identity Information:**
 - OIDC Issuer URL:** https://antara.onelogin.com/oidc/2
 - OIDC Client ID:** 1bc7f213411e5336d6b845ca1d7a8227ab387ba62d574f9075db44e8dcd34df8
- Redirect URL Configuration:**
 - A blue box prompts: "Add the below URL in the redirect URI's for OIDC application."
 - A text input field contains: https://beta.agni.arista.io/sso/login/callback
 - A "Copy" button is located to the right of the input field.
- Identity Information Synchronization:**
 - A toggle switch is currently set to "Disabled".
- Navigation:**
 - A "Back" button is in the top right corner.
 - "Cancel", "Verify", and "Add" buttons are at the bottom right.

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).

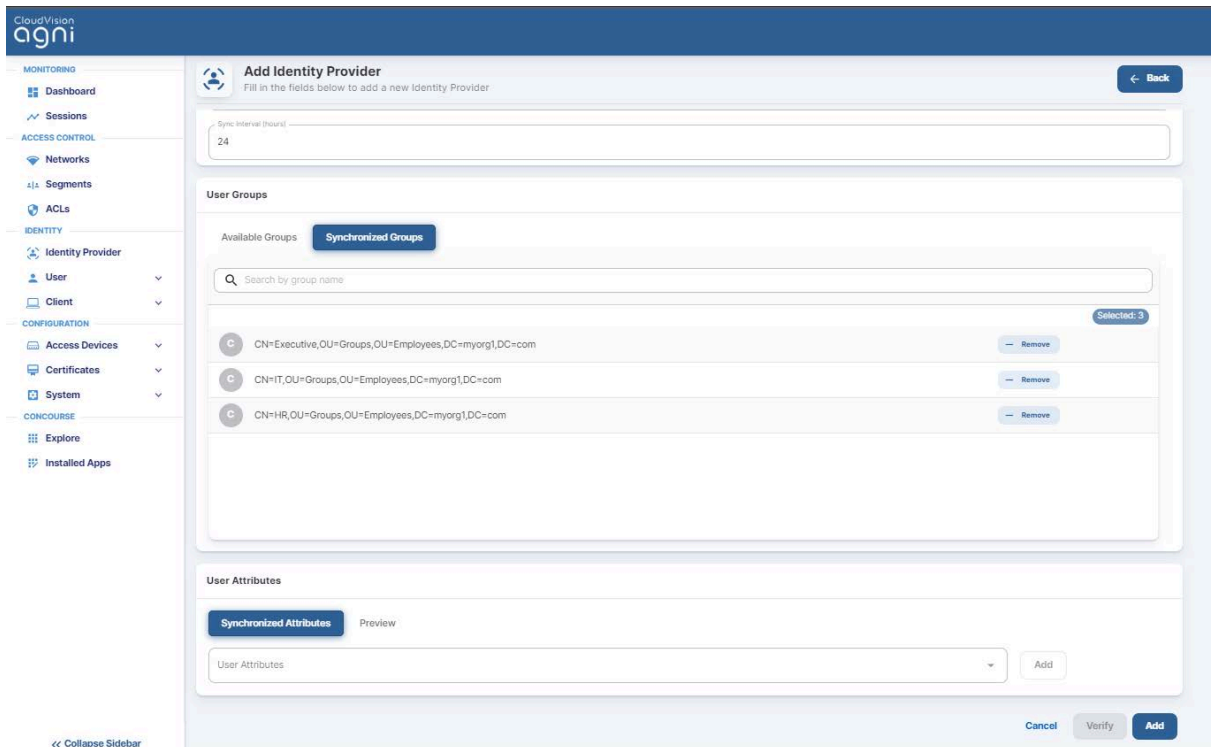


Figure: OneLogin Identity Provider Synchronization

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**

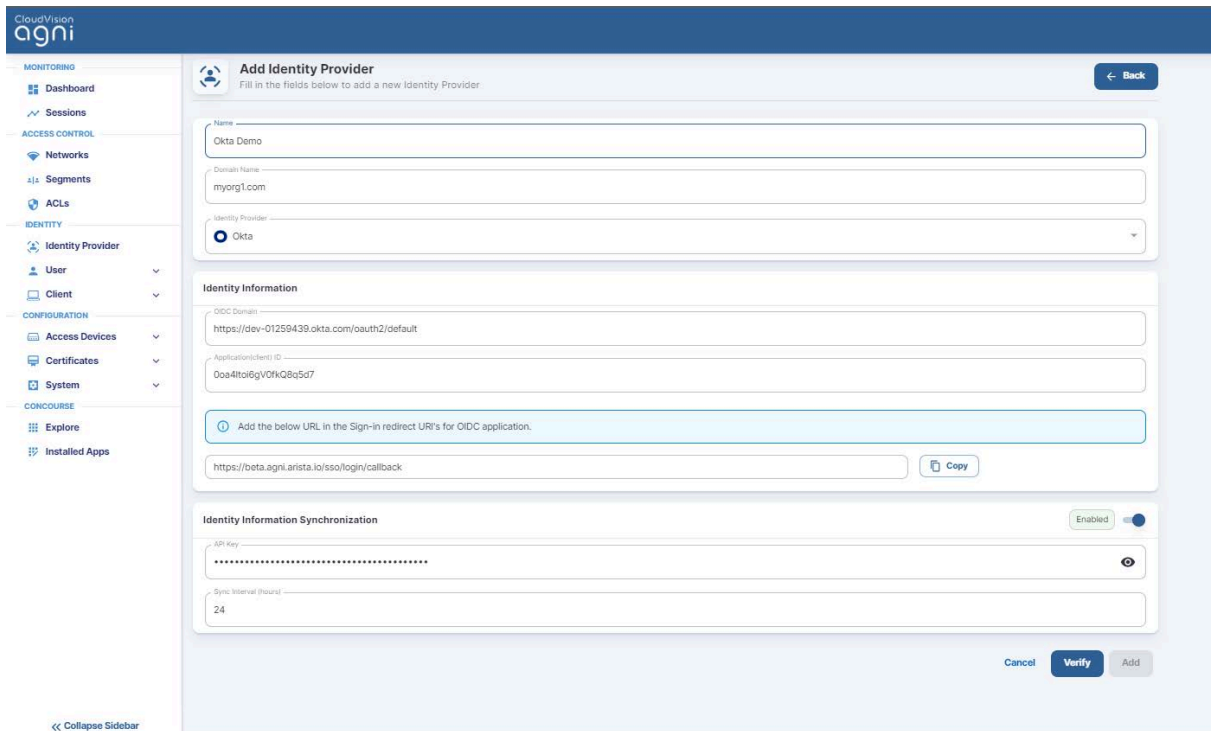


Figure: Okta Identity Provider Configuration

- **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).

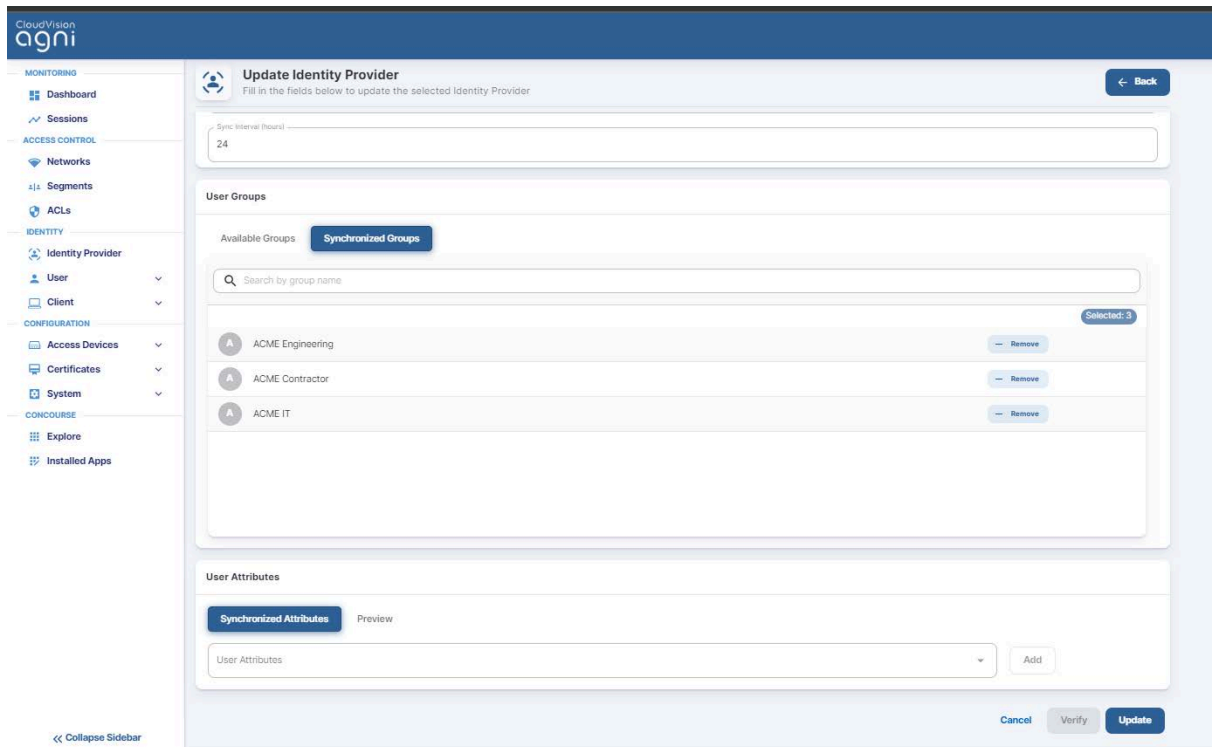


Figure: Okta Identity Provider Synchronization

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).

The screenshot shows the 'Update Identity Provider' configuration page in the CloudVision interface. The page is titled 'Update Identity Provider' and includes a 'Back' button. A notification at the top states 'Your trial license will expire in 346 day(s)'. The configuration fields are as follows:

- Name:** AntaraAI
- Domain Name:** antaraai.net
- Identity Provider:** Google Workspace
- Identity Information Synchronization:** Enabled
- Customer ID:** C03qemvr
- Account Email:** bhagya2@antaraai.net
- Upload Service Account Credentials:** Includes an 'Update Service Account' button and a note: 'Upload the file in JSON format. Updating this will overwrite existing Service Account.'
- Sync Interval (hour):** 24
- Synchronization Details:**
 - Last Sync At:** 8/1/2023 23:32:01
 - Sync Status:** Success

A 'Sync Now' button is located at the bottom right of the page.

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.

The screenshot displays the CloudVision AGNI interface for Identity Provider management. The left sidebar contains a navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Certificates, System), and CONCOURSE (Explore, Installed Apps). The main content area is titled 'Identity Provider' and 'Identity Access Management'. It features a 'Local Users' table with two entries: 'Identity Provider' and 'Domain', both associated with the 'local' provider. Edit and delete icons are visible at the bottom right of the table.

Local Users	
Identity Provider	local
Domain	local

Figure: Local IDP Configurations

Guest Onboarding Features

The Guest Onboarding topics include:

- Guest Onboarding Using AGNI
- Guest Onboarding Offerings in AGNI
- Configuring UPSK for Guest Onboarding (Wireless)
- Configuring Guest Portal Using Guestbook (Wireless)
- Configuring Guest Portal Using Guestbook-Host Approval (Wireless)
- Configuring Guest Portal Using Self-Registration (Wireless)

Guest Onboarding Using AGNI

Arista Guardian for Network Identity (AGNI) offers various ways to onboard guests onto the network. AGNI allows the network admin to host the guest portal page in AGNI and supports customization of the portal page. This document describes the guest onboarding offerings.

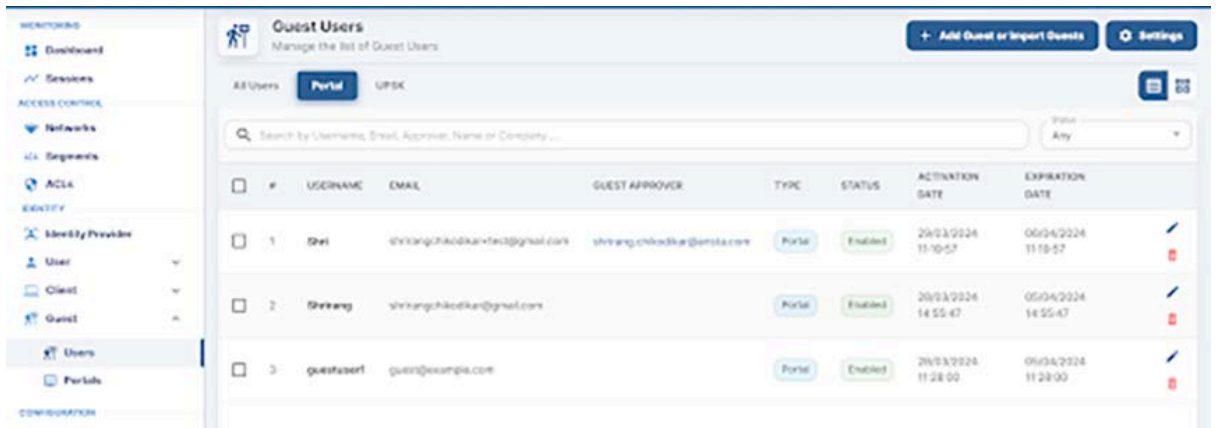
Guest User in AGNI

AGNI has introduced a few user categories to provide the guest onboarding experience. They include:

- Portal Users
- UPSK Users
- Guest Operator
- Guest Sponsor

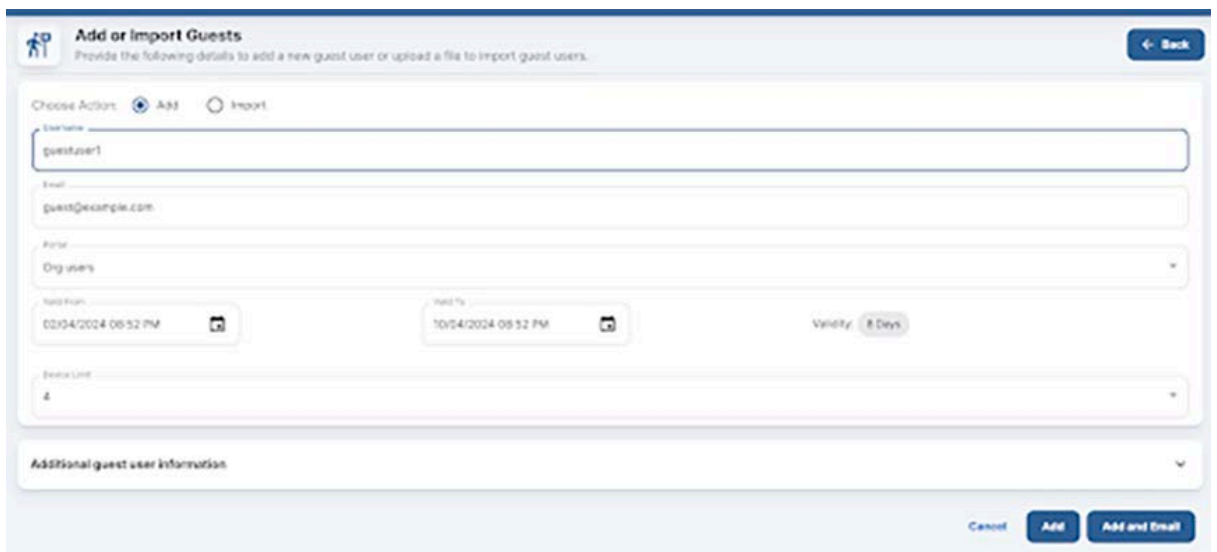
Portal Users

The portal users are guest users who are enrolled in the AGNI via guestbook, self-registration, and host approval methods. The Admin or Guest Operator can pre-populate these users. AGNI can also dynamically add them based on the input from guest users.



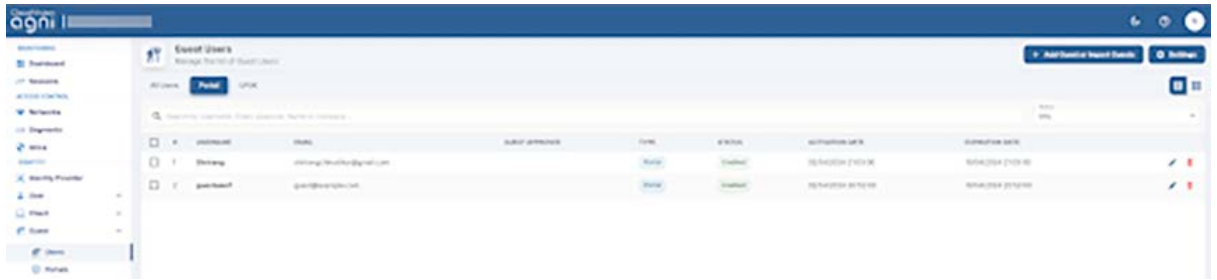
The admin or guest operator can add portal users and share their credentials with the guests in advance. To add the portal users, navigate to **Identity > Guest > Users**. The guest operator must log into the Self-Service Portal and navigate to **Guests > Users**.

Add the Portal Users by Clicking the **Add Guest** or **Import Guest** button. Admin/Guest Operator needs to add a user with the username, email address, Portal with Guestbook plugin, user validity, and Device Limit. Click the **Add** button to add the portal user.

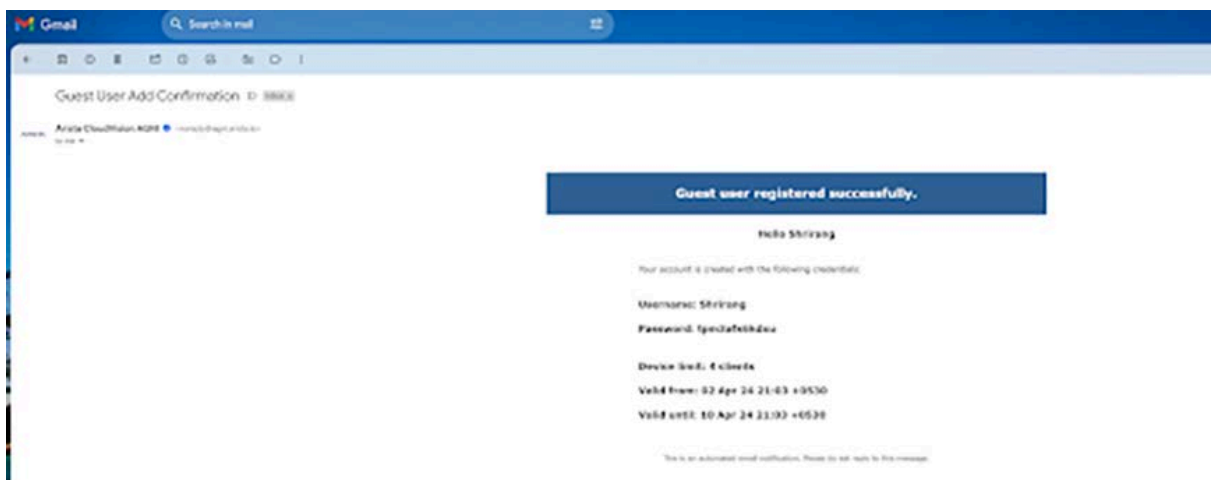


As an Admin or Guest operator, click the **Add and Email** button to add the portal user and send an email to the guest email address with the username, password, validity, and device limit.

Once the portal user is added, it gets displayed in the Portal User listing.



The following screenshot is an example of an email received when a portal user is added.



You can locally add portal users and export them for distribution purposes or use the email functionality.

Admin/guest operators can also add portal users using the Import option. In this flow, the admin/guest operators must import the CSV file in a certain format. See the sample CSV file.

The imported users are listed in the portal user listing.

#	USERNAME	EMAIL	GUEST APPROVER	TYPE	STATUS	ACTIVATION DATE	EXPIRATION DATE
1	user01	user01@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
2	user02	user02@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
3	user03	user03@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
4	user04	user04@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
5	user05	user05@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
6	user06	user06@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
7	user07	user07@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00
8	user08	user08@org.com	admin	Portal	Enabled	2024-04-01 09:33:00	2024-04-09 09:33:00

If the admin or guest operator uses the **Import and Email** option, an email (similar to previous image) is sent to the email address mentioned in the CSV file. Guest users added using self-registration and host approval portal methods are also listed here. In the case of the Host-Approval method, the guest sponsor username is listed in the Guest Approver column.

UPSK Users

Apart from Portal users, AGNI also introduces the concept of UPSK users. Only a Guest Operator can add, update, or delete the UPSK users. The guest can use the identity lookup method to onboard other devices for the same UPSK user.

To add UPSK users, the Guest Operator must log in to the self-service portal and:

- Navigate to **Guest > Users > UPSK**.
- Click the **Add Guest** or **Import Guest** button.
- Select the **Add UPSK user** option, and add email, user validity, and device limit (mandatory fields). You can also add optional guest information, including name, company, phone number, address, and notes.

Note: A UPSK network allowing UPSK guests is mandatory for adding UPSK users.

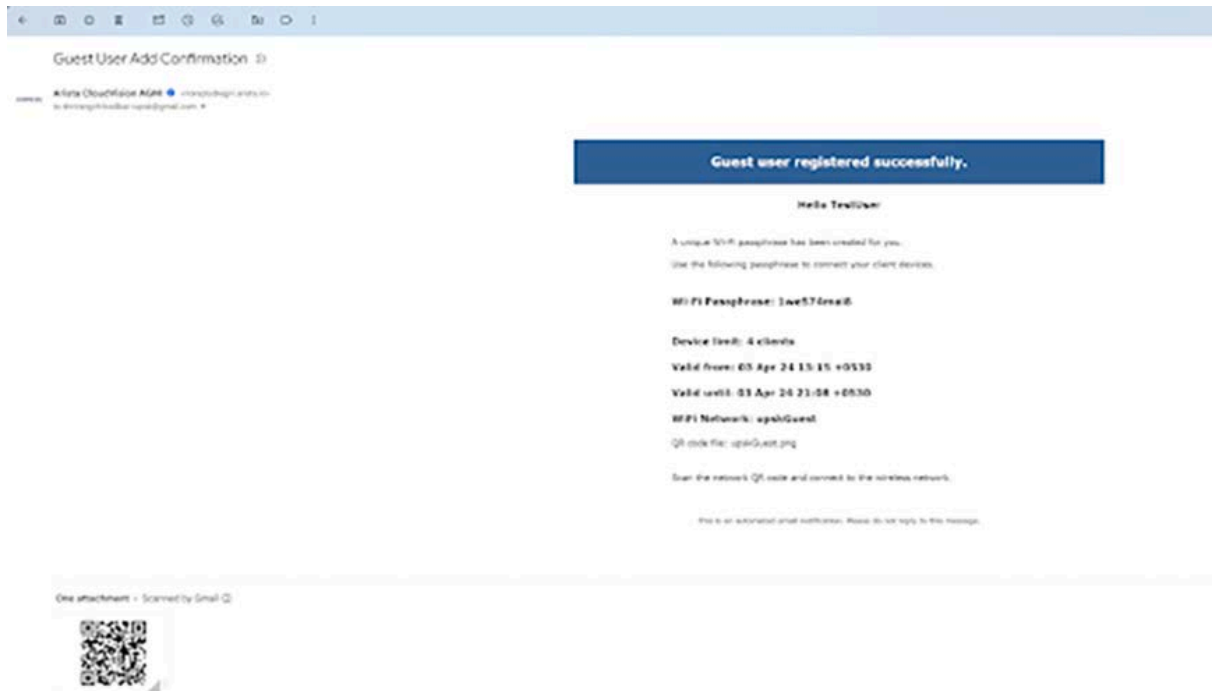
The screenshot shows the 'Add or Import Guests' page. At the top, there's a title 'Add or Import Guests' and a subtitle 'Provide the following details to add a new guest user or upload a file to import guest users.' Below this, there are three radio buttons for 'Choose Action': 'Add portal user', 'Add UPSK user' (which is selected), and 'Import'. The 'Email' field contains 'shirangchikodkar+upsk@gmail.com'. There are 'Validity' and 'Device Limit' fields, both with a value of '4'. Below these is an 'Additional guest user information' section with fields for 'Name' (TestUser), 'Company' (Example LLC), 'Phone', 'Address', and 'Notes' (Test account). At the bottom right, there are three buttons: 'Cancel', 'Add', and 'Add and Email'.

- Click the **Add** button to add the UPSK user. The UPSK user details, along with the QR code, are displayed, and the Guest Operator is mentioned as the approver for the UPSK users.

The screenshot shows the 'Update Guest User' page. It has a title 'Update Guest User' and a subtitle 'View guest user details and update the selected guest user.' The 'Email' field contains 'shirangchikodkar+upsk@gmail.com'. There are 'Validity' and 'Device Limit' fields, both with a value of '4'. A blue box indicates 'This is a UPSK based guest user.' Below this is a 'Network QR code for this user' section with a QR code. At the bottom right, there are three buttons: 'Cancel', 'Update', and 'Add and Email'.

- Click the **Add and Email** button. An email is sent to the configured email address with the following details: UPSK user name, passphrase, user validity, device limit, and QR code of the network.

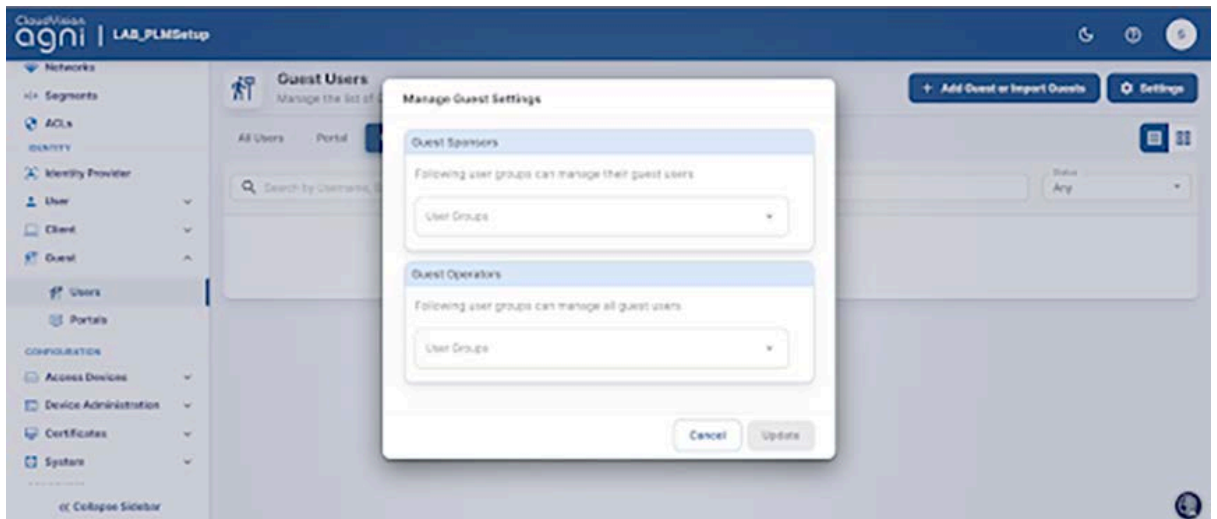
The UPSK Guest user can onboard the devices to the network by scanning the QR code or by using a system-generated passphrase.



Guest Operator

Guest Operators are users who belong to a specified user group. They have the right to add, update, and delete portal and UPSK users and have access to all guest users in the organization.

The admin can configure particular user groups as guest operators by selecting the **Identity > Guest > Users > Settings** option.



Guest Sponsor

Guest sponsors are users who belong to a specified user group and have the right to add portal users. Guest Sponsors can only manage the portal users they add.

The admin can configure particular user groups as guest sponsors by selecting the **Identity > Guest > Users > settings** option.

Guest Onboarding Offerings in AGNI

AGNI offers different guest onboarding methods. These methods include portal-based guest onboarding and UPSK-based guest onboarding methods.

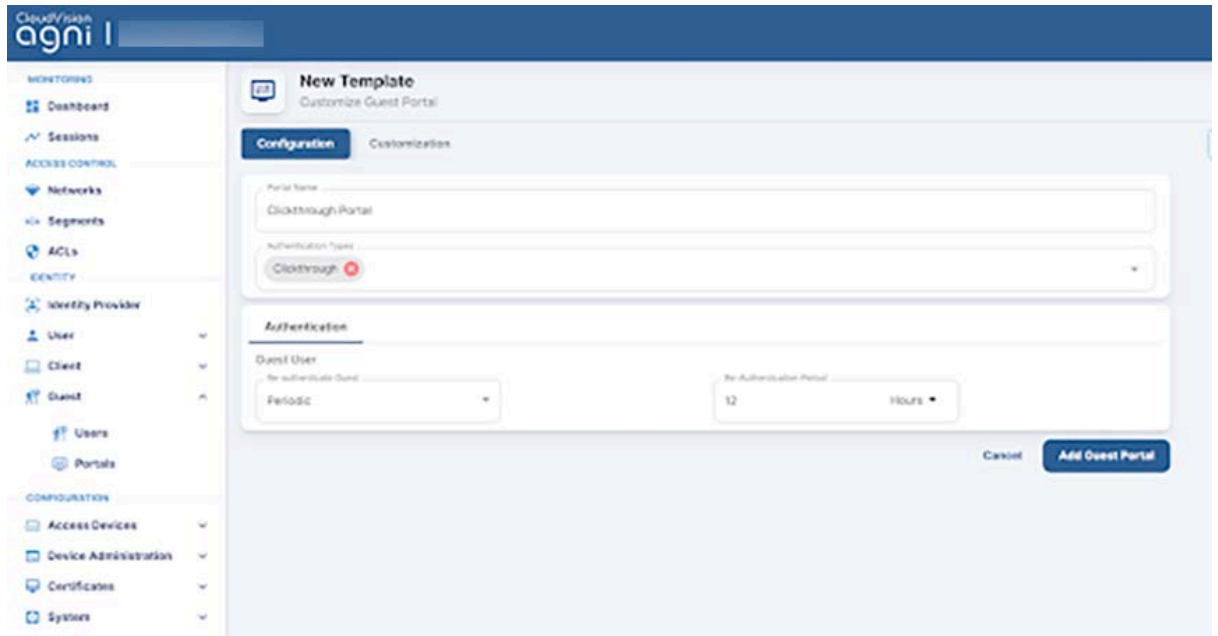
Portal Based Guest Onboarding

AGNI hosts the portal during portal-based onboarding. With admin login, navigate to **Identity > Guests > Portals** to configure the portal page using the appropriate onboarding method. In the portal-based method, AGNI uses roles to redirect the guests to the captive portal. AGNI sends the captive portal URL and role information in Access-Accept messages to the access point. AGNI opens a new session once the user is authenticated and onboarded.

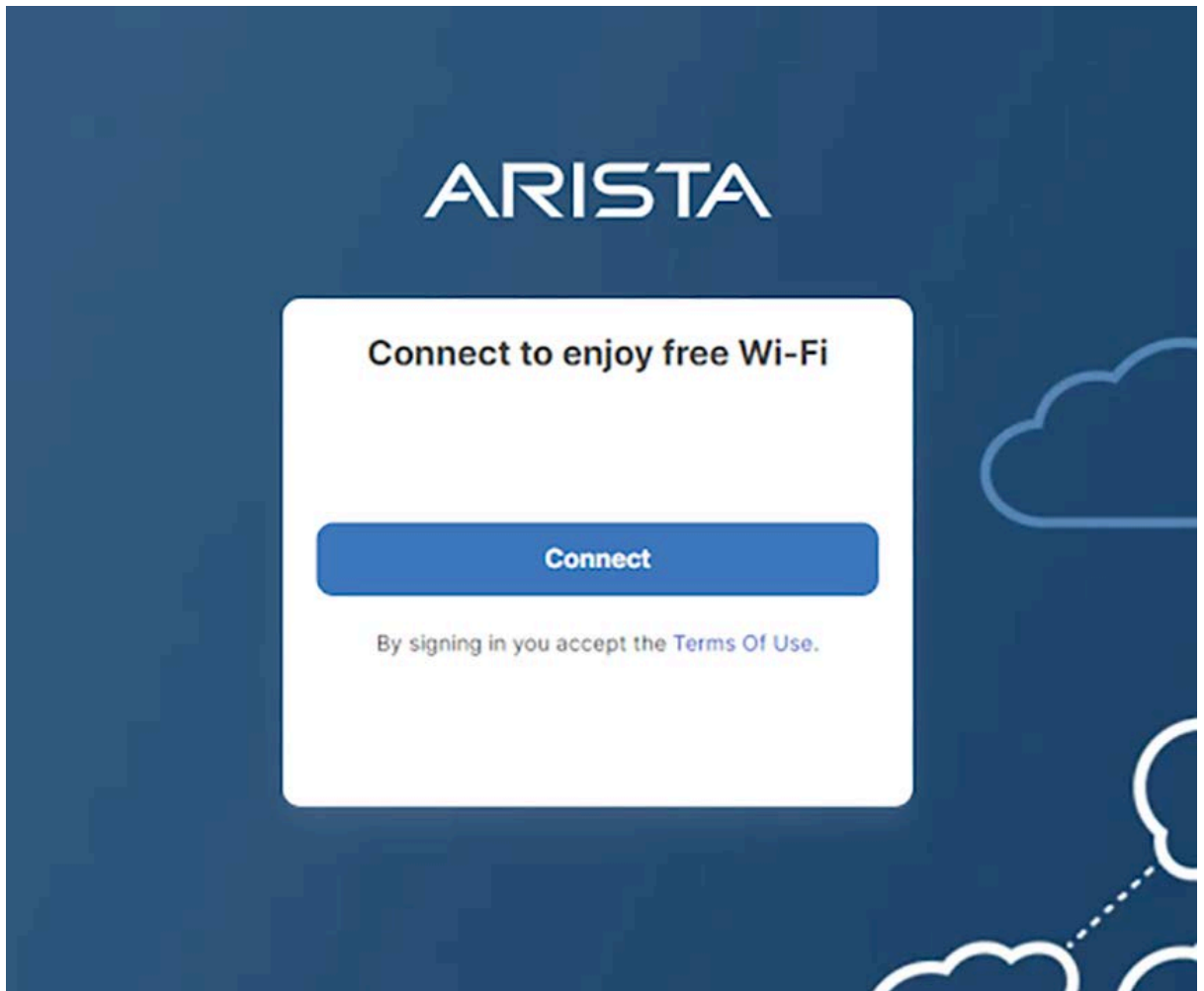
The AGNI admin can add a portal with multiple customization options and modify every field on it. The portal-based authentication method uses the following client onboarding methods:

Clickthrough Portal-based Method

In the clickthrough portal-based method, the guest users can onboard to AGNI network by clicking the **Connect** button (see sample image below). See portal configuration as follows:



See the sample portal below:



Organizational User Login

This guest onboarding method is mainly used to onboard organizational user devices onto the network. This method requires an Identity Provider. In this method, a portal is presented to the user; the user must provide his domain credentials that are verified against the configured identity Provider. If the user gets authenticated successfully then the device gets onboarded onto the network. Admin can restrict the user onboardings using the **Authorised User Groups** feature. Users belonging to these user groups are allowed to onboard the users and the rest are rejected access. The admin can configure the re-authenticate method and device limit for the guest users. The sample configuration for this portal-based onboarding method is as follows:

New Template

Customize Guest Portal

Portal Name
Org User Portal

Authentication Types
Organizational User Login ✕

Authentication

Organizational User

Re-authenticate User
Periodic

Re-Authentication Period
12 Hours

Device Limit
4

Authorized User Groups
Product Management ✕ Select Authorized User Groups...

[Cancel](#) [Add Guest Portal](#)

See the sample portal below:

ARISTA

Organization Login

Submit

By signing in you accept the [Terms Of Use](#).

Guestbook Based Onboarding

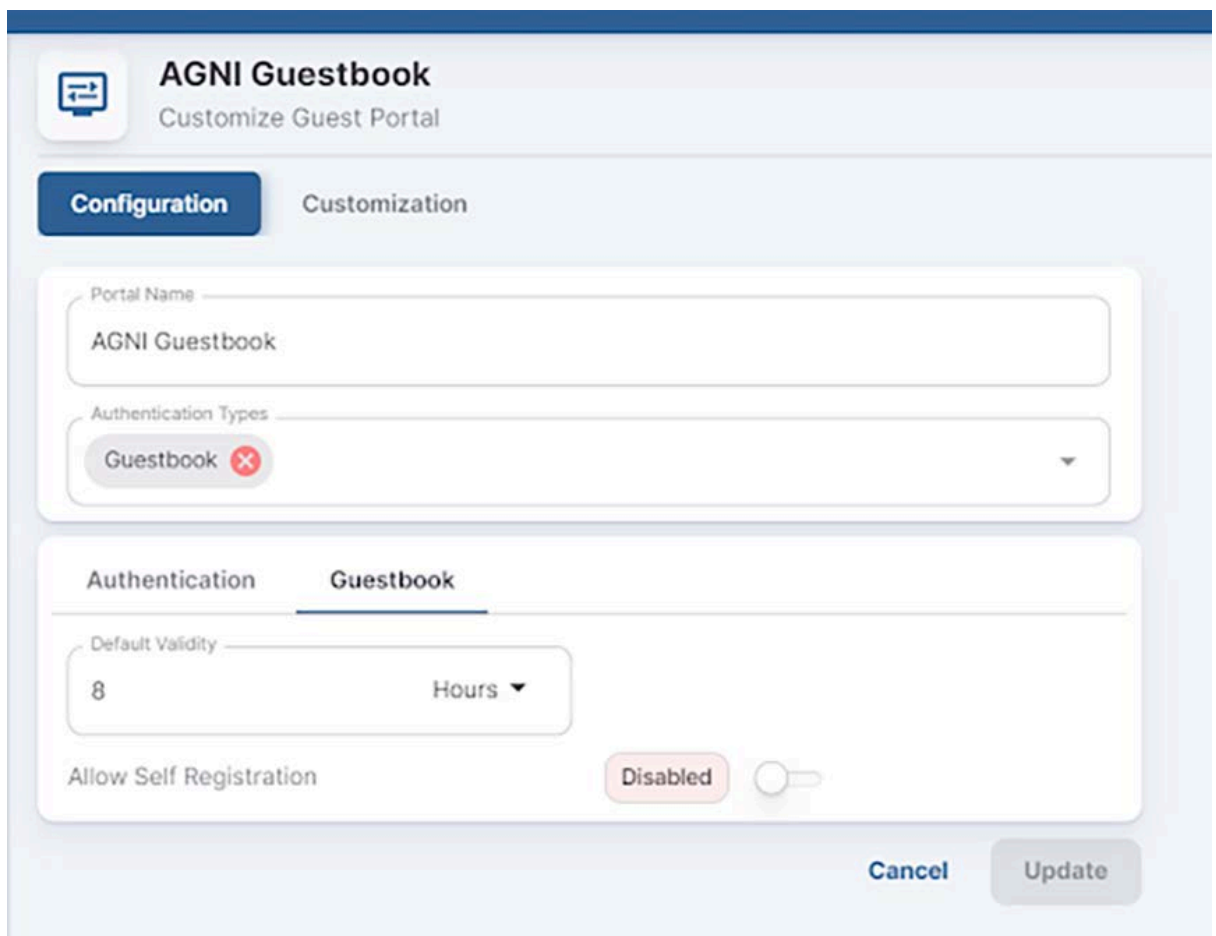
The guestbook method allows the admin to onboard guest users using username and password authentication. There are multiple ways to generate a username and password. Based on the username and password generation, there are three onboarding methods under Guestbook.

Guestbook Method

In this method, the admin or guest operator can add or import users into the system on behalf of the guest user. These guest user details are emailed to guest users from AGNI or exported from AGNI and distributed to users by other means of communication. The admin can configure the portals using the Guestbook method and configure the re-authentication type, device limit, and account validity.

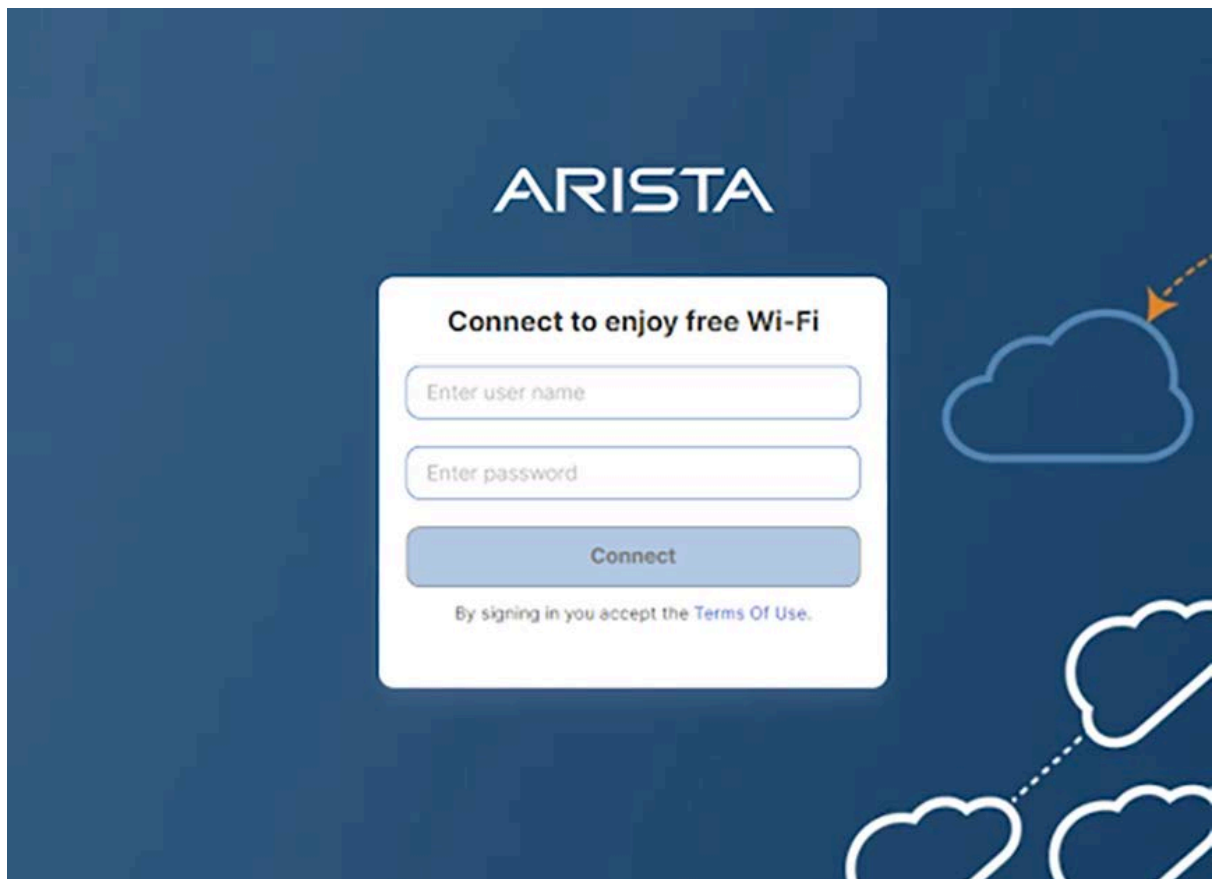
Note: In any guestbook method, the periodic re-authentication time should be less than the account validity. The default account validity is 8 hours.

Below is the screenshot of a sample configuration of the guestbook method:



The screenshot displays the 'AGNI Guestbook' configuration page. At the top, there is a header with the title 'AGNI Guestbook' and the subtitle 'Customize Guest Portal'. Below the header, there are two tabs: 'Configuration' (which is active) and 'Customization'. The main configuration area is divided into two sections. The first section contains a 'Portal Name' field with the value 'AGNI Guestbook' and an 'Authentication Types' dropdown menu with 'Guestbook' selected. The second section, titled 'Authentication', has a sub-tab 'Guestbook' and contains a 'Default Validity' field with the value '8' and a unit dropdown set to 'Hours'. Below this, there is a toggle switch for 'Allow Self Registration' which is currently 'Disabled'. At the bottom right of the configuration area, there are 'Cancel' and 'Update' buttons.

The sample portal is as follows:



Self-Registration

In this method, the admin can allow the guest users to enroll themselves into the system using the portal-based form and receive the credentials in an email. The admin must enable the self-registration toggle to access this method. The admin can decide on the input list to take from the guest users before creating credentials. Later, the guest user can configure the list by using the **Customized Guest User Fields** option. Name and email are the mandatory fields on the list. The sample config is as follows:



AGNI Guestbook

Customize Guest Portal

Configuration

Customization

Portal Name

AGNI Guestbook

Authentication Types

Guestbook

Authentication

Guestbook

Default Validity

8

Hours

Allow Self Registration

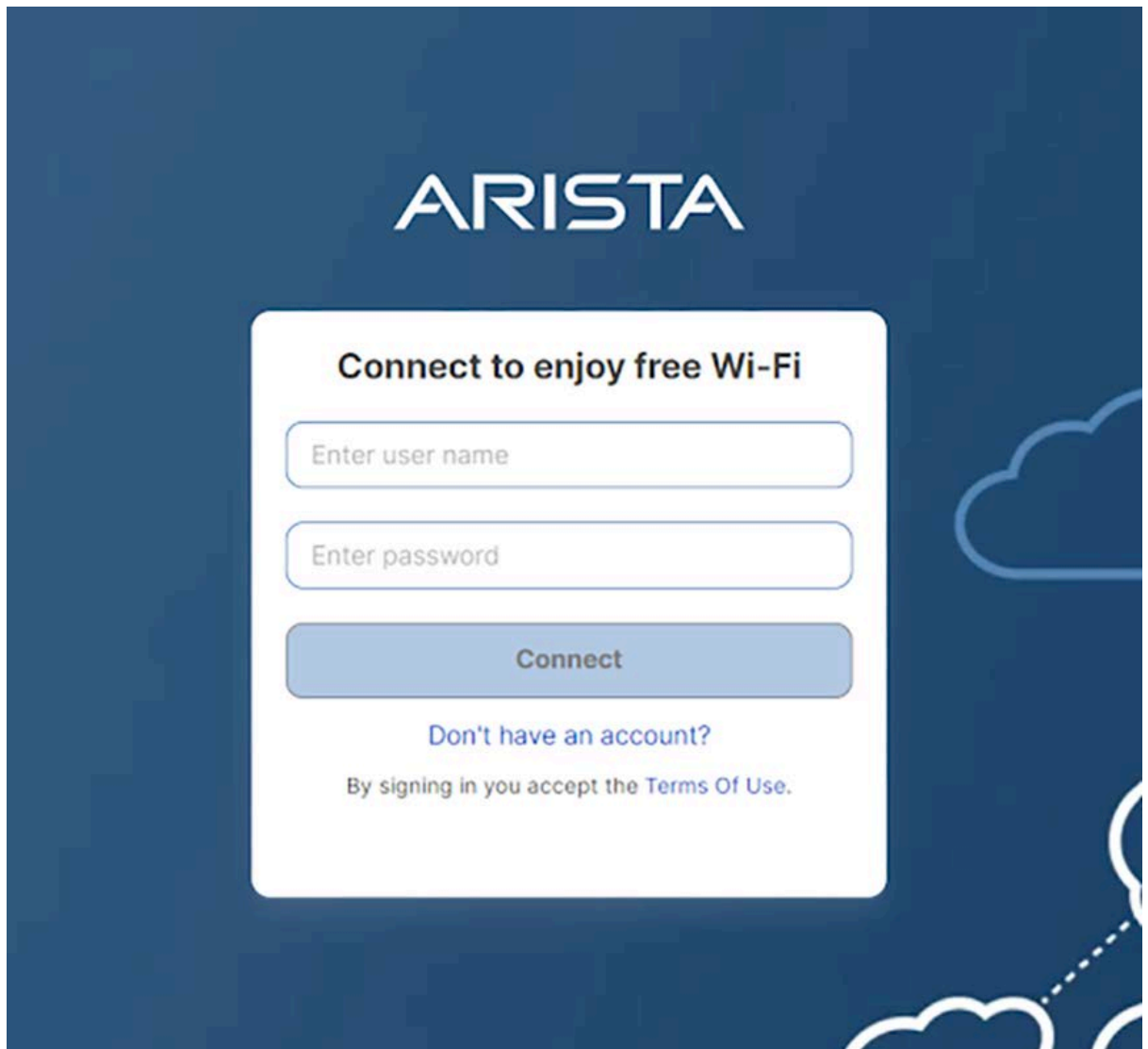
Enabled

Approval required for guest access

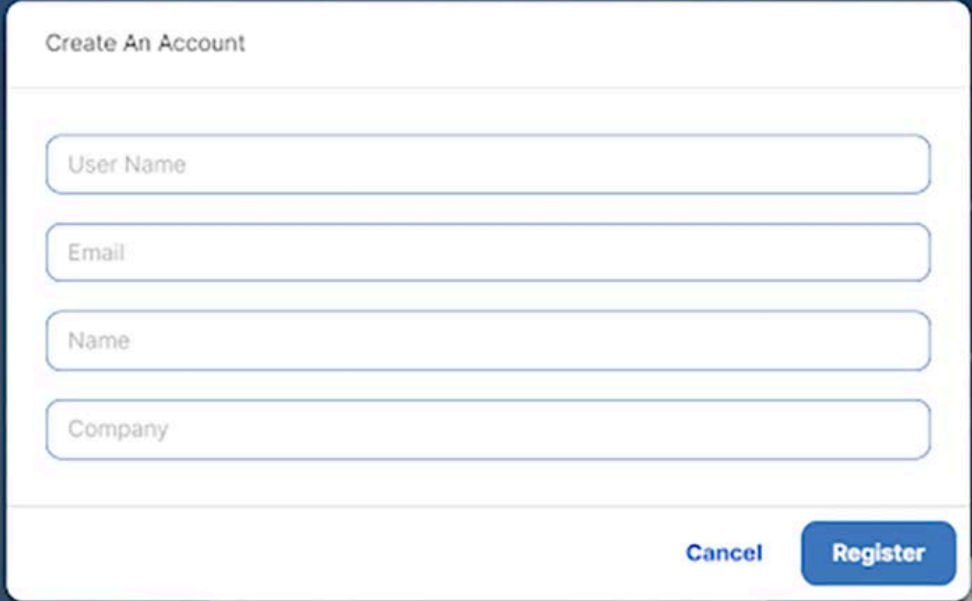
Disabled

Customize Guest User Fields

Below is a sample portal:

A sample login portal for ARISTA. The background is dark blue with white cloud outlines. At the top center, the word "ARISTA" is written in a white, bold, sans-serif font. Below it, a white rounded rectangle contains the text "Connect to enjoy free Wi-Fi" in bold. There are two input fields: "Enter user name" and "Enter password", both with light blue borders. Below the fields is a blue button with the text "Connect" in white. Underneath the button, the text "Don't have an account?" is displayed in blue. At the bottom of the white box, it says "By signing in you accept the Terms Of Use." in a smaller font, with "Terms Of Use" being a link.

The users can generate their own credentials by using the **Don't have an account** option. A form is displayed when you click this option. Below is a sample form:



The image shows a 'Create An Account' form on a dark blue background. The form is white with rounded corners and contains four input fields: 'User Name', 'Email', 'Name', and 'Company'. At the bottom right of the form, there are two buttons: a blue 'Register' button and a 'Cancel' button. The background features a stylized cloud graphic with a dashed arrow pointing towards the form.

Click the **Register** button. A portal user gets added to the AGNI using the information given, and details are emailed to the guest. If the email is incorrect, then the portal user gets added, and the admin or guest operator can help the guests with the username and password.

Guests can use these credentials to log into the portal.

Host Approval

The Host-approval method allows the admin to configure the portal so that the host can approve the guest access requests. Once the host approves the guest request, the guest credentials are generated and sent to the guests via email.

This type of guest onboarding method is common in enterprises.

See the image below for the sample configuration:



AGNI Guestbook

Customize Guest Portal

Authentication Types

Guestbook ✕



Authentication

Guestbook

Default Validity

8

Hours ▼

Allow Self Registration

Enabled



Approval required for guest access

Enabled



Add approvers by: User Groups Email Domains

Authorized User Groups

Engineering ✕

approver ✕

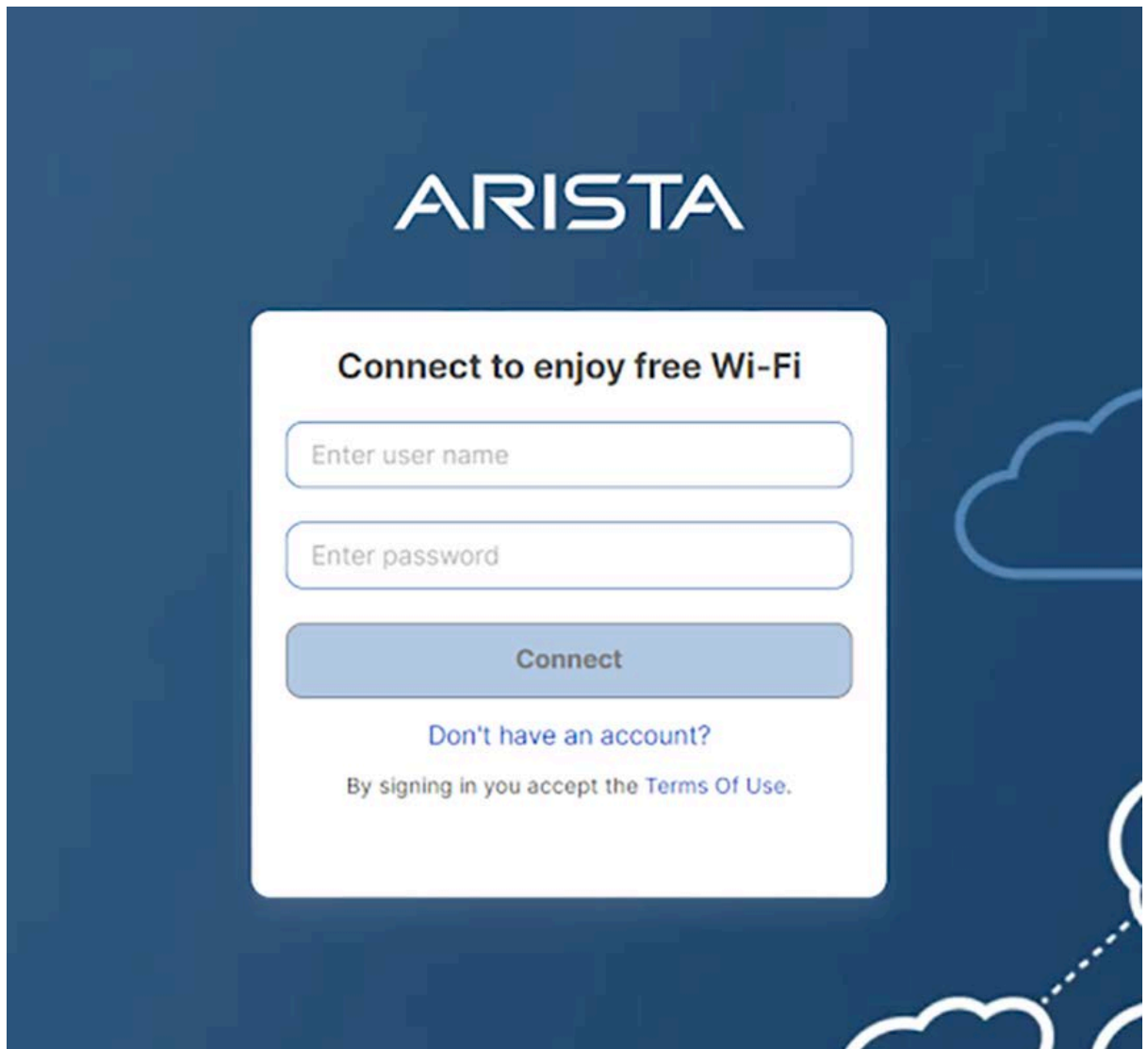
Select Authorized User Groups...



Customize Guest User Fields



Below is a sample portal:

A sample Wi-Fi login portal for ARISTA. The background is dark blue with white cloud outlines. At the top center, the word "ARISTA" is written in a white, bold, sans-serif font. Below it, a white rounded rectangle contains the text "Connect to enjoy free Wi-Fi" in bold black font. Underneath are two white input fields with rounded corners and thin blue borders. The first field contains the placeholder text "Enter user name" and the second contains "Enter password". Below the input fields is a blue button with rounded corners and the text "Connect" in white. At the bottom of the white box, the text "Don't have an account?" is displayed in blue, followed by "By signing in you accept the [Terms Of Use.](#)" in a smaller black font.

ARISTA

Connect to enjoy free Wi-Fi

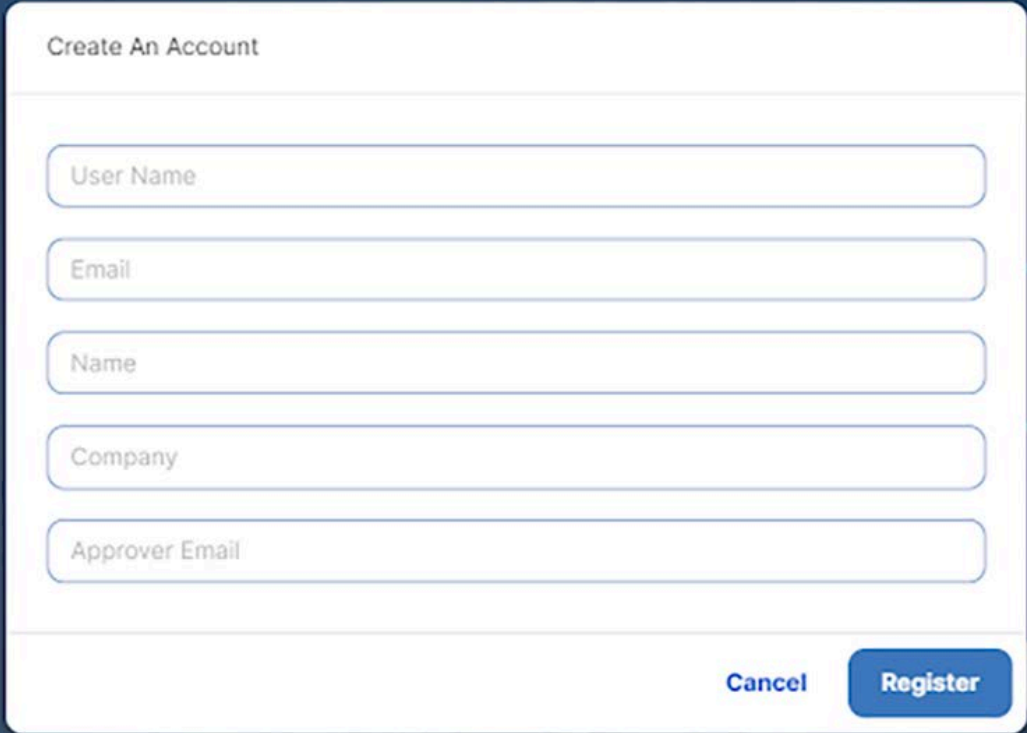
Connect

[Don't have an account?](#)

By signing in you accept the [Terms Of Use.](#)

The users can generate their own credentials by using the **Don't have an account** option. A form is displayed when you click this option.

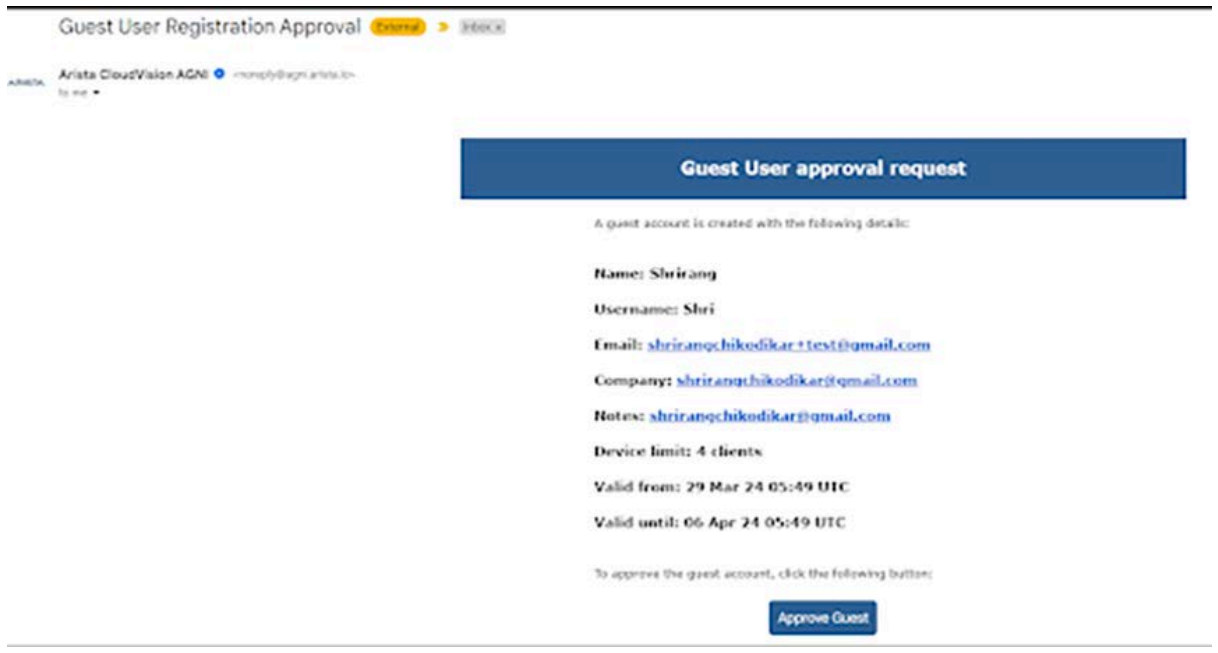
Following is a sample form:



The image shows a 'Create An Account' form with the following fields and buttons:

- User Name
- Email
- Name
- Company
- Approver Email
- Cancel
- Register

Fill in the form and click the **Register** button. An email is sent to the approver.
Following is a sample email:



Click the **Approve Guest** button to approve the guest. A portal user is created in AGNI, and the username and password are sent to the guest. Guests can use these credentials to log in to the portal.

In the Host Approval method, if the guest provides an incorrect approver email address in the form, an approval email is sent to the users who were added to the user groups in the portal configuration earlier.

If the admin has chosen an Email Domain option, the approver email from the form should match this email domain. If the approver email is incorrect or not found in that domain, then approval mail is sent to all users who are part of the “Default User Group” added in the portal configuration. In this case, the admin can hide or make the Approver Email field an optional field, and when not provided by the Guest, an approval email is sent to all members of the “Default User Group.”

UPSK Based Guest Onboarding

AGNI offers its Unique PSK advantages to guest users. Guest Users can be onboarded onto the guest network using UPSK for the guest option. In this method, guest operators create guest users, and the UPSK or QR codes are sent to the guest users via email. The guest users can use these to onboard their devices on the guest network. UPSK provides isolation between two different users' devices, but at the same time, all devices can access the shared devices. Guest onboarding using UPSK is becoming popular in enterprise and hospitality verticals. The admin needs to configure the network with UPSK for guests, and the User Private Network with shared clients enabled. All UPSK features and caveats apply to this guest onboarding method. Here, AGNI uses the UPSK Identity Look-up feature to onboard guest users. Hence, it is supported only by the WPA2 encryption method.

Configuring UPSK for Onboarding Guest (Wireless)

This document describes how to configure UPSK for guest onboarding in a network. Guests can use all the UPSK functionalities, such as User Private Network and Identity Lookup. Currently, this method is supported only with the WPA2 PSK method. To achieve this, you must have the required configurations on both AGNI and CV-CUE.

Configuring AGNI

1. Login to AGNI and navigate to **Access Control > Networks**
2. Click **+ Add Network** to add a new wireless network with the following configurations:
 - a. Network Name - UPSK for Guest
 - b. Connection Type — Wireless
 - c. SSID - upskGuest
 - d. Status - Enabled
 - e. Authentication
 - i. Authentication Type - UPSK
 - ii. Allowed Users - Guest Users Only
 - iii. User Private Network - Enabled
 - iv. Shared Clients - Disabled
3. Click the **Add Network** button.

Add Network
Provide the following details to add a new Network

Name: UPSK for Guest

Connection Type: Wireless Wired

SSID: upskGuest

Status: Enabled

Authentication

Authentication Type: Unique PSK (UPSK)

Allowed Users: Organizational users only Guest users only

The wireless SSID type must be configured as WPA2 only for guest access. Applicable for Arista Wi-Fi only.

User Private Networks Enabled

Shared Clients: Disabled

Enable to make a set of clients accessible to all users.

Cancel Add Network

4. Login to the self-service portal with a guest operator user group access.
Note: You must be part of the **Guest Operator** access group to make these configuration changes.
5. Navigate to **Guest > Users** from the left side panel.
6. Click the **Add or Import Guest** option to add a UPSK guest.
7. Select the **Add UPSK** user option.

CloudVision agni | Self-Service Portal

- Manage Clients
- Register Client
- Wi-Fi Passphrase
- GUESTS
 - Users

Add or Import Guests

Provide the following details to add a new guest user or upload a file to import guest users.

[← Back](#)

Choose Action: Add portal user Add UPSK user Import

Email

Validity Hours

Device Limit

Additional guest user information

[Cancel](#) [Add](#) [Add and Email](#)

- Add the user's email address and click the **Add and Email** option.
- The guest gets an email address including SSID name: UPSK, Device limit, user validity details, and QR code. The user details are also displayed on the registration portal.

Update Guest User

View guest user details and update the selected guest user

[← Back](#)

Email

Apname

This is a UPSK based guest user.

Passphrase [Copy](#)


Created at: Hours Valid until:

Device Limit

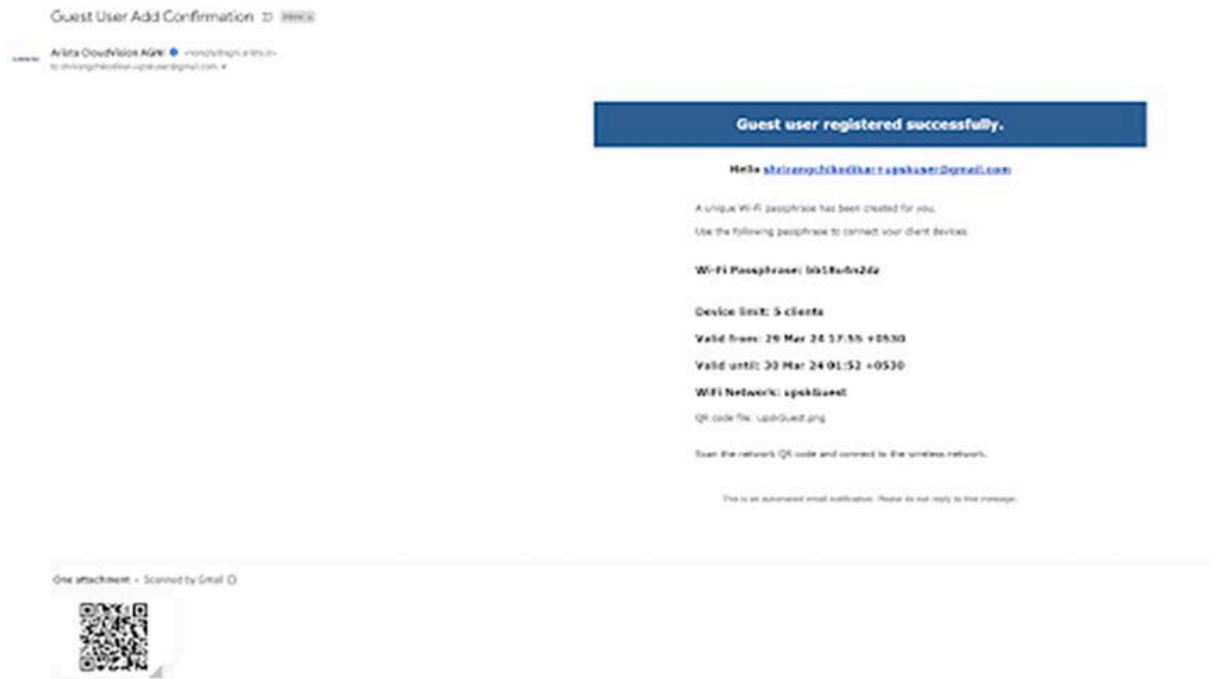
Status: Enabled

Network QR code for this user

Wireless Network:



Below is an example of the email received:



Configuring CV-CUE

1. Login to CV-CUE and navigate to **Configure > WiFi**. Add a **WLAN** profile with the following settings:
 - a. SSID name - upskGuest
 - b. Security - WPA2 + UPSK
 - c. Access Control
 - i. Radius Settings - Radsec enabled
 - ii. Authentication server
 - iii. Accounting server
 - iv. CoA - Enable

WiFi ▾ **SSID**

Changes will restart the SSID if it is on. The changes will affect all groups and folders using this SSID.

← upskGuest

WLAN ▾ Basic Security Network Access Control ⋮

Name

SSID Name *

upskGuest

Profile Name *

upskGuest

Select SSID Type

Services

WiFi ▾ **SSID**

upskGuest Changes will restart the SSID if it is on. The changes will affect all groups and folders using this SSID.

← upskGuest

WLAN ▾ Basic Security Network Access Control ⋮

Select Security Level for Associations
At the 6 GHz band, WiFi 6E does not support security methods older than WPA3 (WPA2, WPA1, etc.). Hence, this SSID will not be activated on 6 GHz radios.

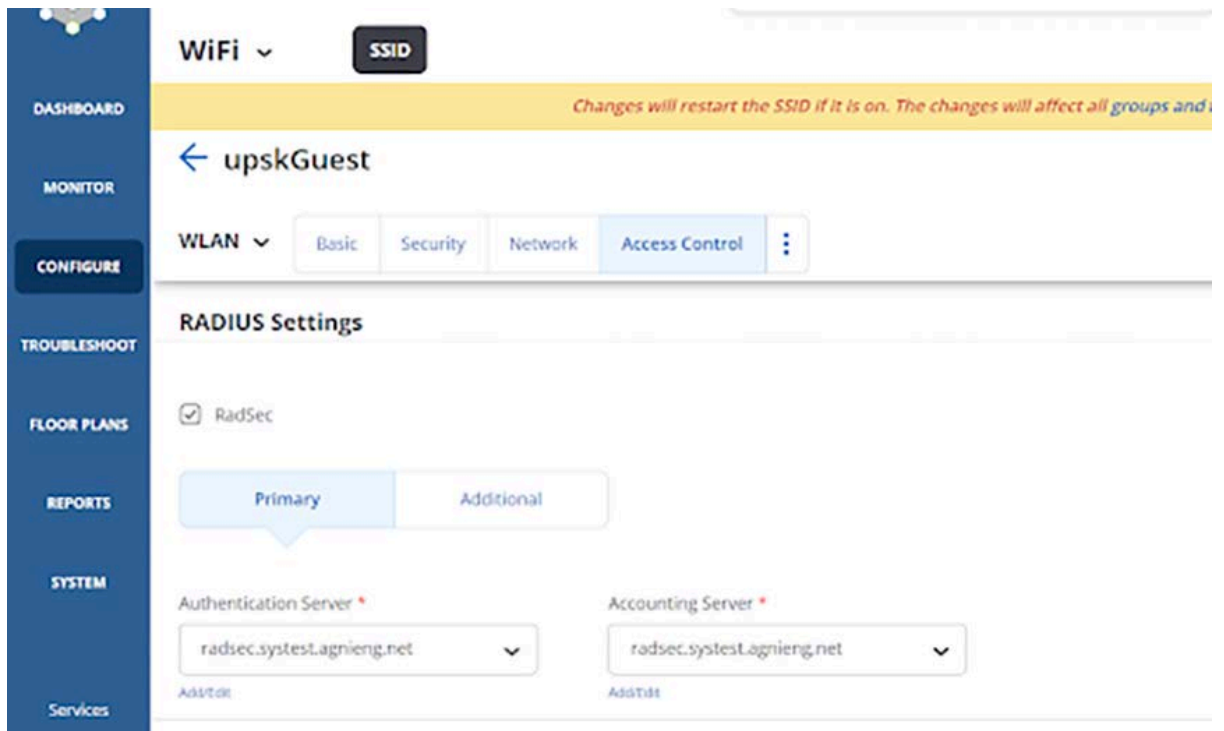
WPA2 ▾ PSK LIPSK 802.1X

LIPSK User Private Networks For a radio with multiple SSIDs on the same VLAN, if LIPSK User Private Networks is enabled for any SSID, the first configured SSID takes preference.

LIPSK Identity Lookup This setting is not editable because of LIPSK User Private Networks is enabled.

Mitigate WPA/WPA2 Key Reinstallation Vulnerabilities in Clients

Services



2. Save and **Turn ON** the SSID Profile.

Onboarding the User

To onboard yourself to the AGNI network, the guest user can perform one of the following methods:

1. The guest user scans the UPSK QR code and onboard to the AGNI network.
OR
2. The guest user can use the UPSK received in the email.

Note: Users can access their own devices but cannot access other guest devices. However, if the shared clients flag is **enabled**, then all guest users can access all clients marked as shared.

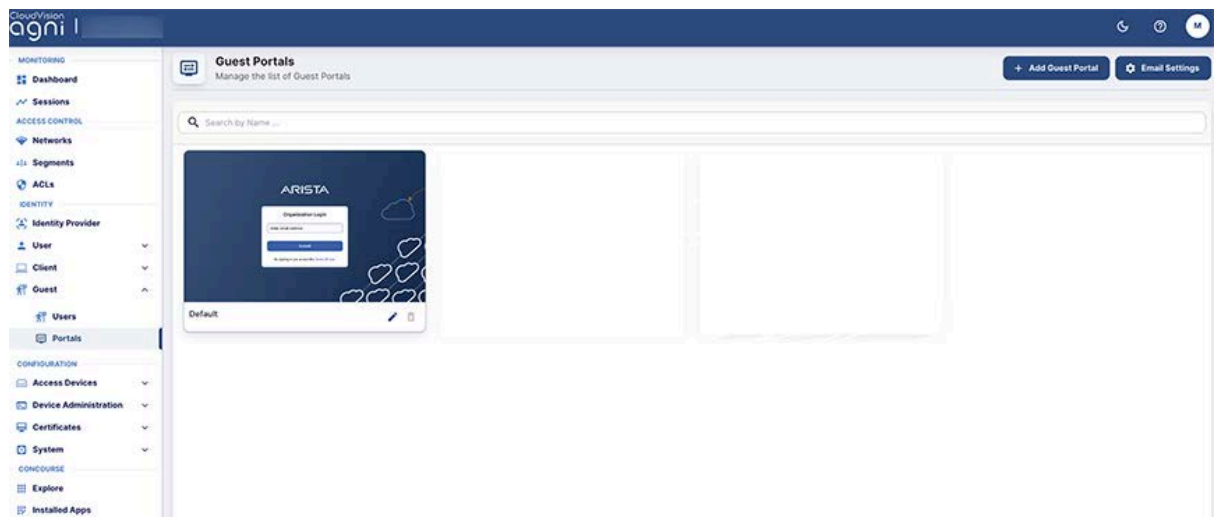
Configuring Guest Portal Using Guestbook (Wireless)

This article describes the steps to configure the guest portal with the Guest Book authentication method for wireless clients. You must configure both AGNI and CV-CUE to configure the guest portal.

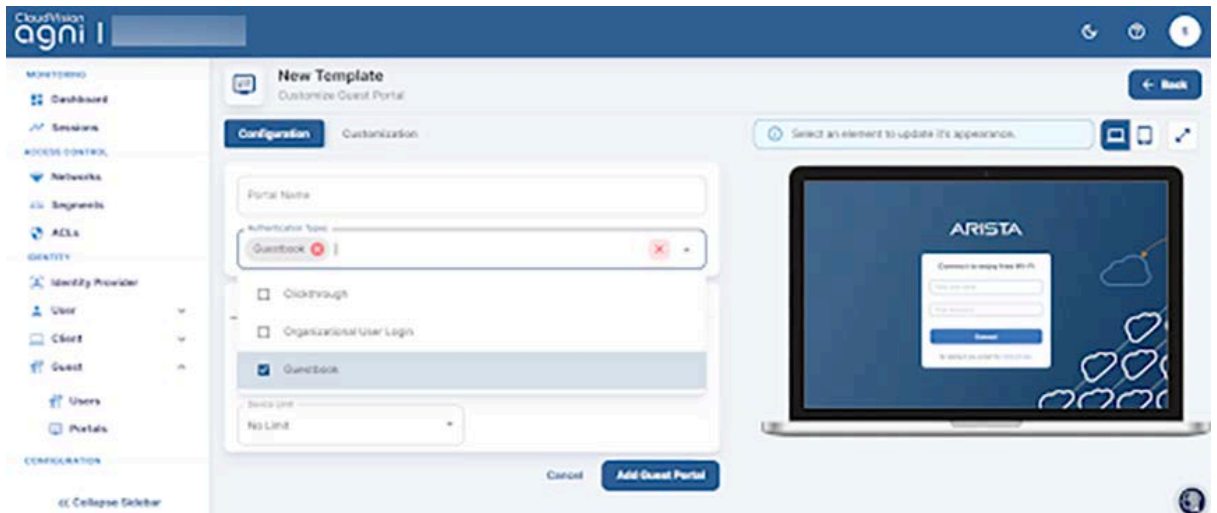
Configuring the Portal on AGNI

1. Log in to AGNI and navigate to **Identity > Guest > Portals**

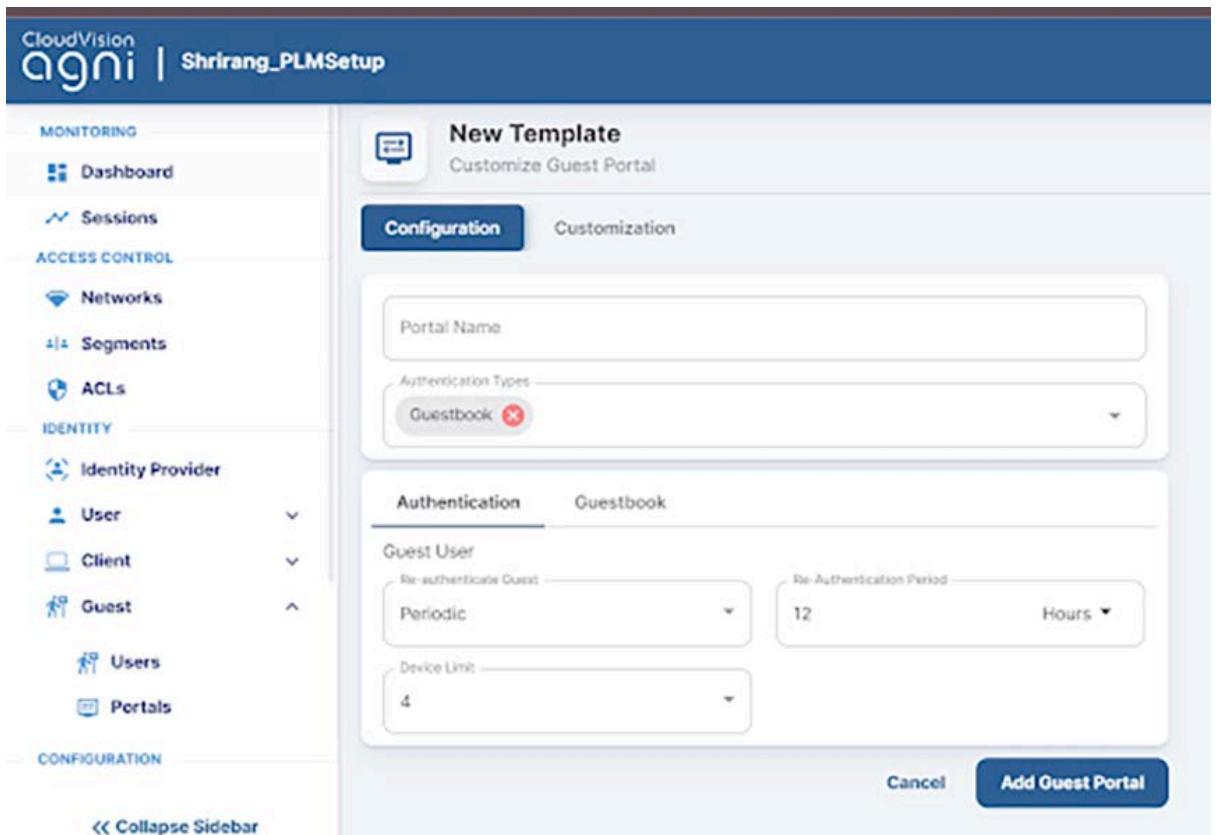
Note: The **Default** portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.



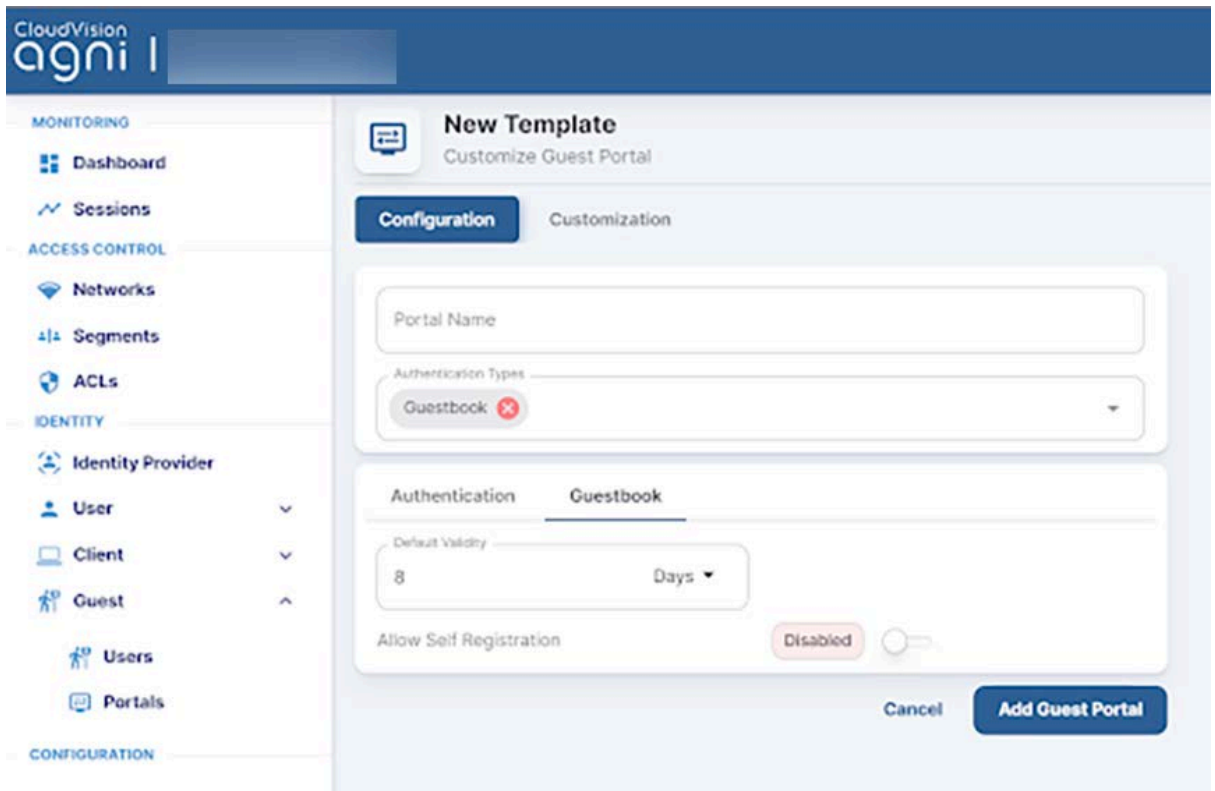
2. Click the **+Add Guest Portal** button.
3. In the **Configuration** tab, provide the portal name and select the Authentication Types. The available Authentication types are **Default**, **Organizational User Login**, and **Guestbook**. Select **Guestbook** as the Authentication Type.



4. From the Authentication section, select the following settings for the guest user:
- Re-authenticate Guest - **Periodic**
 - Re-authentication
 - Device Limit - 4



5. Navigate to Guestbook settings and configure the Device Validity to 8 Days. Keep **Allow Self Registration** Disabled.



Note: Device validity should always be greater than the re-authentication period. The default value for Device Validity is 8 Hours.

6. Click the **Customization** tab to customize the portal settings:
 - Theme template
 - Default
 - Split Screen
 - Select element
 - Global
 1. Page
 2. Login Toggle
 3. Terms of Use and Privacy Policy
 4. Logo
 - Guest
 1. Guest Login Submit Button
 2. User Name Textbox
 3. Password Textbox
 4. Guest Login Header
 5. Guest Login Form
 6. Self Registration
 7. Clickthrough

CloudVision
agni |

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals

CONFIGURATION

<< Collapse Sidebar

AGNI Guestbook

Customize Guest Portal

Configuration **Customization**

Theme template
Default

Select element
Page

- Global
- Login Toggle
- Logo
- Page
- Terms of Use and Privacy Policy
- Guest
- Guest Login Form
- Guest Login Header

CloudVision
agni |

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals

CONFIGURATION

- Access Devices
- Device Administration
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

<< Collapse Sidebar

AGNI Guestbook

Customize Guest Portal

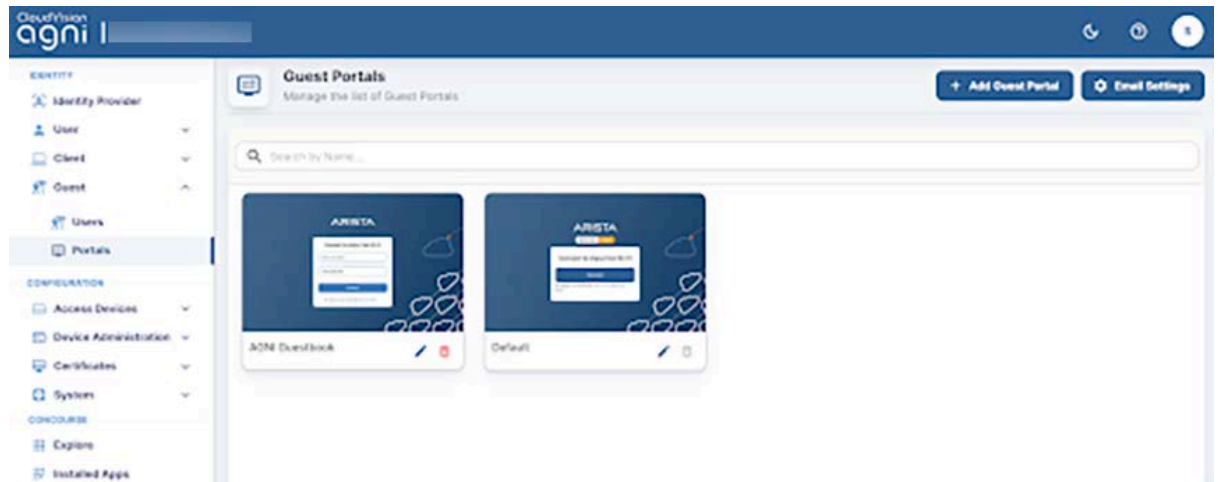
Configuration **Customization**

Theme template
Default

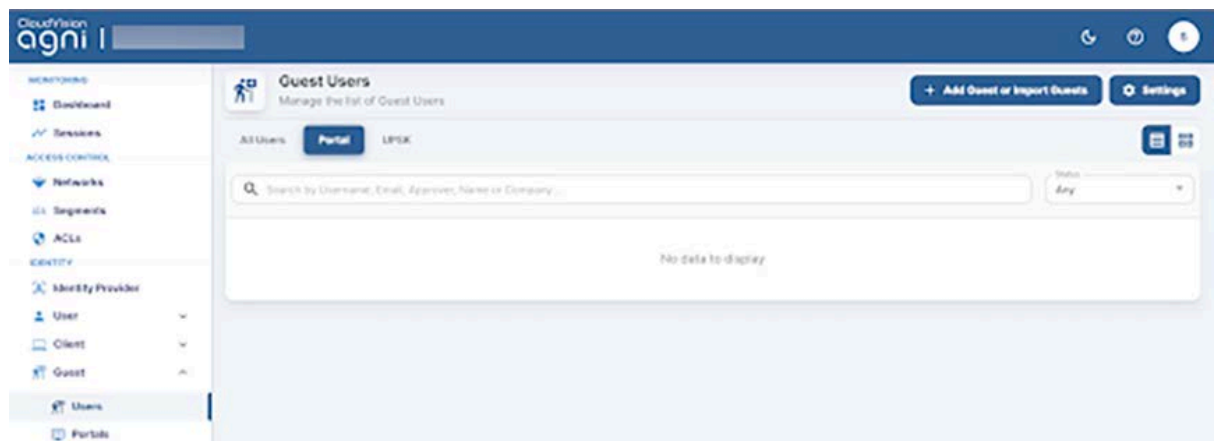
Select element
Page

- Guest
- Guest Login Form
- Guest Login Header
- Guest Login Submit Button
- Password Textbox
- User Name Textbox
- Self Registration
- Clickthrough

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



- Navigate to **Identity > Guest > Users**
- Click on the **Add Guest or Import Guests** option to add portal users.



- Add a Guest user with the following settings:
 - Username - guestuser1
 - Email - guest@example.com
 - Portal - AGNI Guestbook
 - Validity - 8 Days
 - Device Limit - 4**Note:** The Validity & Device Limit changes automatically as per the portal selected

CloudVision agni I

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals

CONFIGURATION

<< Collapse Sidebar

Provide the following details to add a new guest user or upload a file to import guest users.

[← Back](#)

Username: guestuser1

Email: guest@example.com

Portal: AGNI Guestbook

Valid From: 28/03/2024 11:28 AM

Valid To: 05/04/2024 11:28 AM

Validity: 8 Days

Device Limit: 4

Additional guest user information

[Cancel](#) [Add](#) [Add and Email](#)

- Click the **Add** button to add the guest user. If the admin clicks on **Add and Email**, you receive an email with the username, password, and other details.
- The guest user is listed in the Portal User listing.

CloudVision agni I

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals

Guest Users
Manage the list of Guest Users

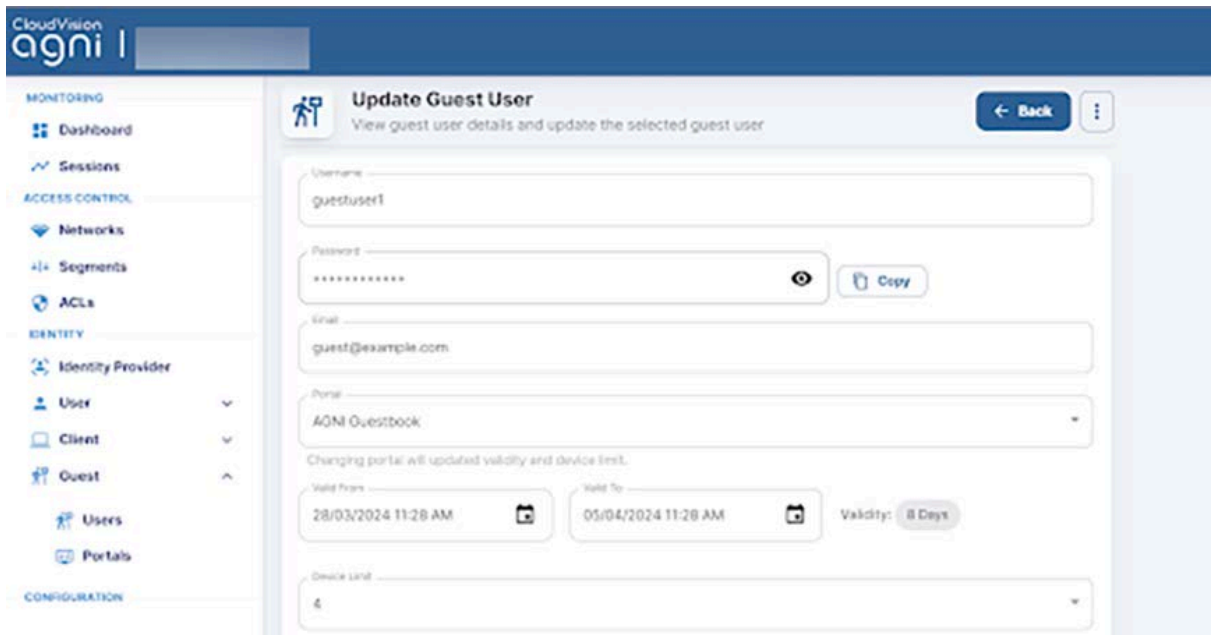
[+ Add Guest or Import Guests](#) [Settings](#)

All Users **Portal** UPSC

Search by Username, Email, Approver, Name or Company...

#	USERNAME	EMAIL	GUEST APPROVER	TYPE	STATUS	ACTIVATION DATE	EXPIRATION DATE
1	guestuser1	guest@example.com		Portal	Enabled	28/03/2024 11:28:00	05/04/2024 11:28:00

- Edit the guest user to get the system-generated password.

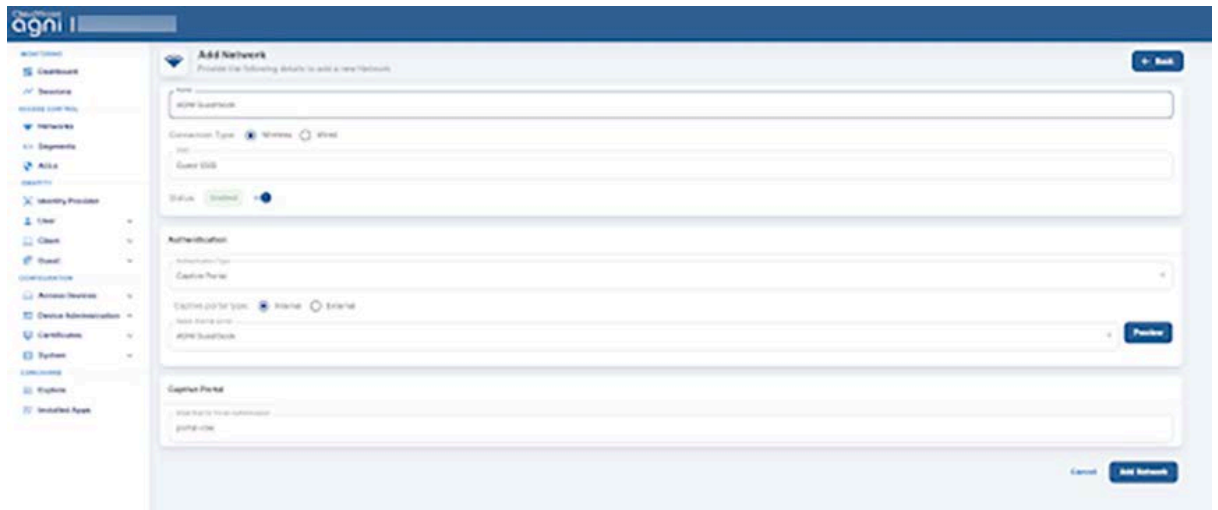


14. Select the guest user from the portal user listing and use the **Export** option to export user details (including password) into a CSV file.



Configuring Network

1. Navigate to the **Access Control > Network**.
2. Add a new network with the following settings:
 - Network Name - AGNI Guestbook
 - Connection Type — Wireless
 - SSID - Guest SSID
 - Status - Enabled
 - Authentication
 - Authentication Type - Captive Portal
 - Captive Portal Type - Internal
 - Select internal portal - AGNI Guestbook
 - Captive Portal
 - Internal Role for Portal Authentication - portal-role



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-role**
4. Click the **Redirection** check box and select **Dynamic Redirection**.
5. Keep other settings to default values.

[←](#) portal-role

Profile Name *

portal-role

 Use default settings in AutoKerberos Role Specific Settings

Role Specific Settings

 VLAN * VLAN ID VLAN Name [0 - 4094]

Firewall

User Bandwidth Control

 Limit the maximum upload bandwidth per user to Mbps [1 - 1024] Redirection Static Redirection Dynamic Redirection HTTPS Redirection

Certificate Information

Common Name

www.arista.com

Organization

Arista Networks

Organization Unit

Arista Networks

Websites That Can Be Accessed Before Authorization *

login.microsoftonline.com:80,443



aadcdn.msftauth.net:80,443



aadcdn.msauth.net:80,443



login.live.com:80,443



system.aging.net:80,443



Configuring SSID

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

WiFi ▾

SSID

← Guest SSID

WLAN ▾

Basic

Security

Network



Name

SSID Name *

Guest SSID

Profile Name *

Guest SSID

Select SSID Type

Private Guest

Hide SSID

Include AP Name in Beacon

4. Click the **Access Control** tab.
5. Click the **Client Authentication** checkbox and select **RADIUS MAC Authentication**.
6. Select **RadSec**.

7. Select the **Authentication** and **Accounting** servers.

WiFi ▼ **SSID**

[← Guest SSID](#)

WLAN ▼ Basic Security Network **Access Control** ⋮

[▶ Firewall](#)

Client Authentication

Google Integration RADIUS MAC Authentication

RADIUS Settings

RadSec

Primary **Additional**

Authentication Server ^{*}
radsec.systemsengineering.net ▼
Account

Accounting Server
radsec.systemsengineering.net ▼
Account

Send DHCP Options and HTTP User Agent

Retry Parameters

Attempts ^{*}
4 ⬆ ⬇ ⬆ [1 - 10]

Timeout ^{*}
2 ⬆ ⬇ ⬆ seconds [1 - 100]

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** role profile while configuring the Role Profile in the previous section.

WIFI SSID

← Guest SSID

WLAN Basic Security Network Access Control

Accounting Stop Delay

If Client Authorization Fails

Disconnect Stay connected

Role Based Control

RADIUS VSA Google DU This setting is not editable because Client Authentication via Google integration is disabled. [Change Settings?](#)

Rule Type *

Operand *

Assign Role *

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 portal authentication after entering their username and password.

Configuring Guest Portal Using Guestbook-Host Approval (Wireless)

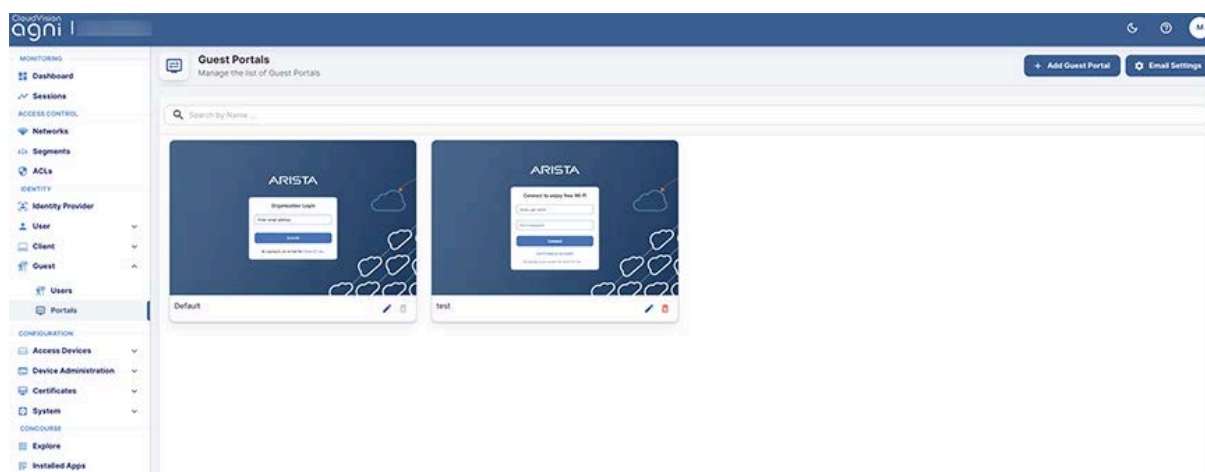
This document describes the steps to configure the guest portal using the Guest Book authentication method for wireless clients. You must configure both AGNI and CV-CUE to configure the guest portal.

Configurations on AGNI

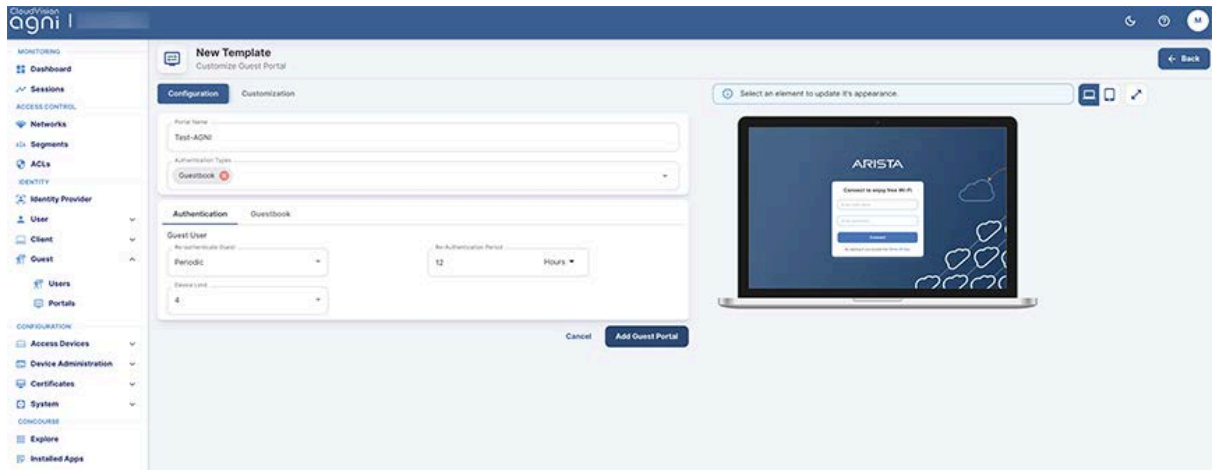
To configure AGNI for Guestbook authentication:

1. Log in to AGNI and navigate to **Identity > Guest > Portals**.

Note: The **Default** portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.



2. Click the **+Add Guest Portal** button.
3. In the **Configuration** tab, provide the portal name and select the Authentication Types. The available Authentication types are **Default**, **Organizational User Login**, and **Guestbook**. Select **Guestbook** as the Authentication Type.
4. From the Authentication section, select the following settings for the guest user:
 - Re-authenticate Guest - **Periodic**
 - Re-authentication Period - **12 Hours**
 - Device Limit - **4**



5. Click the **Guestbook** tab and configure the Device Validity for 8 Days. Enable **Allow Self Registration** and **Approval required for guest access** flags. Select the **User Groups** option in the **Add approvers by** section and add the following user fields for the **Customize Guest User Fields** tab.
 - User Name
 - Email
 - Name
 - Company
 - Address
 - Notes
6. Click the **Update** button.

The screenshot displays the 'Test-AGNI' configuration page for a Guest Portal. The interface is organized into a sidebar and a main configuration area.

- Sidebar:** Contains navigation menus for MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client, Guest, Users, Portals), CONFIGURATION (Access Devices, Device Administration, Certificates, System), and CONCOURSE (Explore, Installed Apps).
- Main Configuration Area:**
 - Portal Name:** Test-AGNI
 - Authentication Types:** Guestbook
 - Default Validity:** 8 Days
 - Allow Self Registration:** Enabled
 - Approval required for guest access:** Enabled
 - Add approvers by:** User Groups (selected), Email Domains
 - Authorized User Groups:** (Dropdown menu)
 - Customize Guest User Fields:**

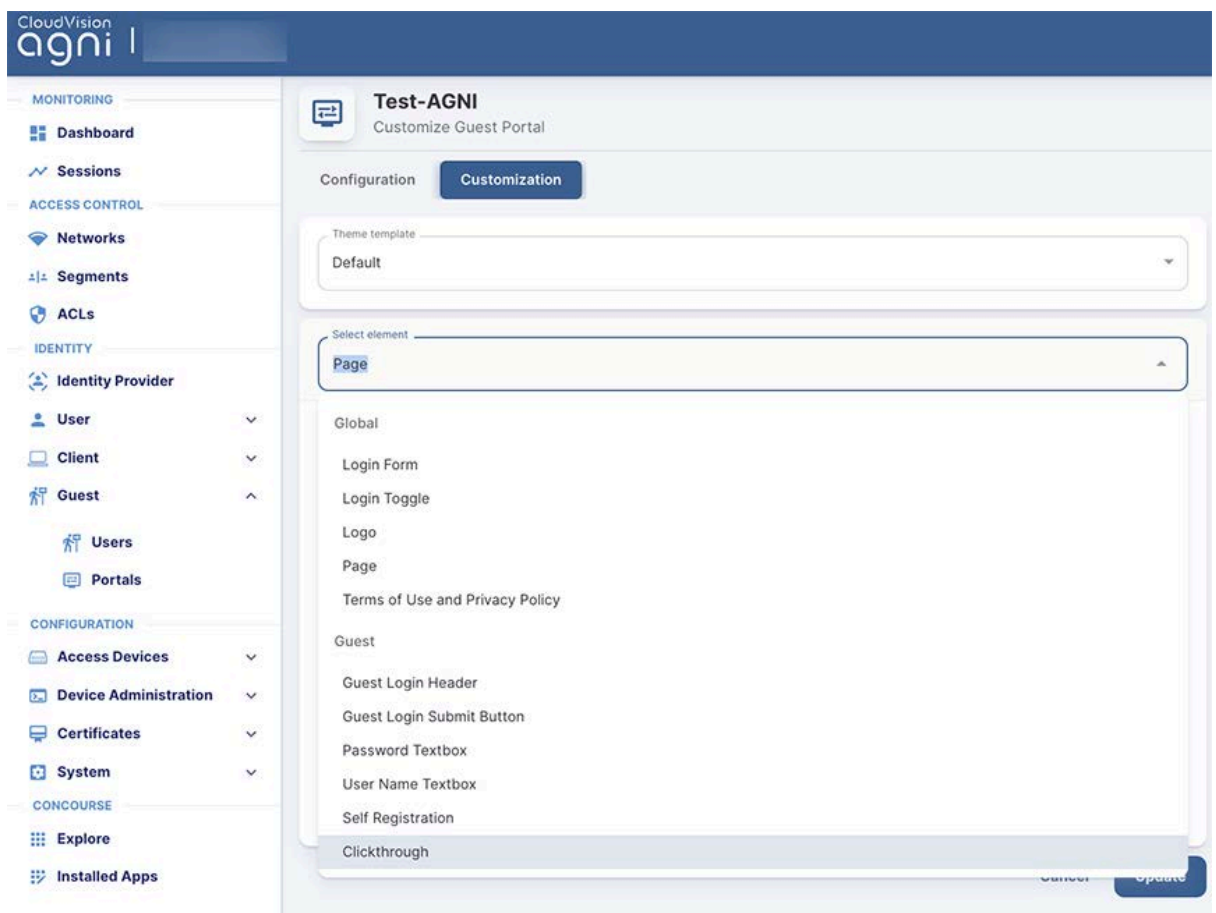
Display	Field Label	Mandatory
<input checked="" type="checkbox"/>	User Name	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Name	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Company	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Phone	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Address	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Notes	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Approver Email	<input type="checkbox"/>

Two options are available to approve guest accounts that are created using self-registration:

1. **User Groups:** Approvers must belong to one of the selected Groups. Guests must specify a valid approver's email that belongs to the user group. Guests cannot complete the self-registration without a valid approver email address.
2. **Email Domains:** This is more flexible where validation is only for approver email to match one of the email domains specified. If there is no valid user for the approver email provided by the guest during self-registration, the approve request email is sent to all members of the "Default User Group".

Note: Device validity should always be greater than the re-authentication period. The default value for Device Validity is 8 Hours.

7. Click the **Customization** tab to customize the portal settings, including:
 - Theme template
 - Default
 - Split Screen
 - Select element
 - Global
 1. Page
 2. Login Toggle
 3. Terms of Use and Privacy Policy
 4. Logo
 - Guest
 1. Guest Login Submit Button
 2. User Name Textbox
 3. Password Textbox
 4. Guest Login Header
 5. Guest Login Form
 6. Self Registration
 7. Clickthrough



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

CloudVision
agn1 | 🔍 ⌚ 👤

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals**

CONFIGURATION

- Access Devices
- Device Administration
- Certificates
- System


CONFORMANCE

- Explore
- Installed Apps

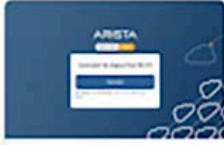
Guest Portals
Manage the list of Guest Portals

[+ Add Guest Portal](#) [Email Settings](#)

🔍 Search by Name...



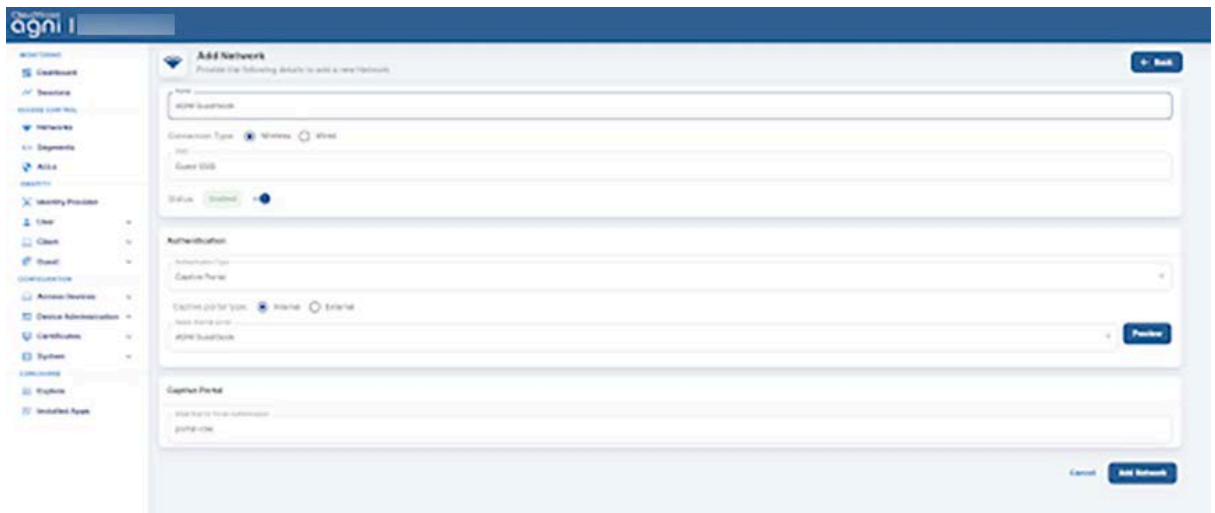
AON Guestbook



Default

Configuring the Network

1. Navigate to **Access Control > Network**.
2. Add a new network with the following settings:
 - Network Name - AGNI Guestbook
 - Connection Type — Wireless
 - SSID - Guest SSID
 - Status - Enabled
 - Authentication
 - Authentication Type - Captive Portal
 - Captive Portal Type - Internal
 - Select internal portal - AGNI Guestbook
 - Captive Portal: Internal Role for Portal Authentication - portal-role



Configuring CV-CUE

In CV-CUE, configure a role profile and the SSID settings. Ensure 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-role**.
4. Enable the **Redirection** check box and select **Dynamic Redirection**.
5. Keep other settings to default.

[←](#) portal-role

Profile Name *

portal-role

 Use default settings in AutoKerberos Role Specific Settings

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 HTTPS Redirection

Certificate Information

Common Name

www.arista.com

Organization

Arista Networks

Organization Unit

Arista Networks

Websites That Can Be Accessed Before Authorization *

login.microsoftonline.com:80,443



aadcdn.msftauth.net:80,443



aadcdn.msauth.net:80,443



login.live.com:80,443



system.aging.net:80,443



Configuring SSID

To configure SSID:

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

WiFi ▾

SSID

← Guest SSID

WLAN ▾

Basic

Security

Network



Name

SSID Name *

Guest SSID

Profile Name *

Guest SSID

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.

WiFi ▼ **SSID**

[← Guest SSID](#)

WLAN ▼ Basic Security Network **Access Control** ⋮

▸ Firewall

Client Authentication

Google Integration RADIUS MAC Authentication

RADIUS Settings

RADIUS

Primary

Additional

Authentication Server *

radius.system.agrieng.net ▼

AAA:01

Accounting Server

radius.system.agrieng.net ▼

AAA:01

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 (the **portal-role** role profile created while configuring the Role Profile in the previous section).

WIFI SSID

← Guest SSID

WLAN Basic Security Network Access Control

Accounting Stop Delay

If Client Authorization Fails

Disconnect Stay connected

Role Based Control

RADIUS VSA Google DU This setting is not editable because Client Authentication via Google integration is disabled. [Change Settings?](#)

Rule Type *

Operand *

Assign Role *

DHCP Fingerprinting based Access Control

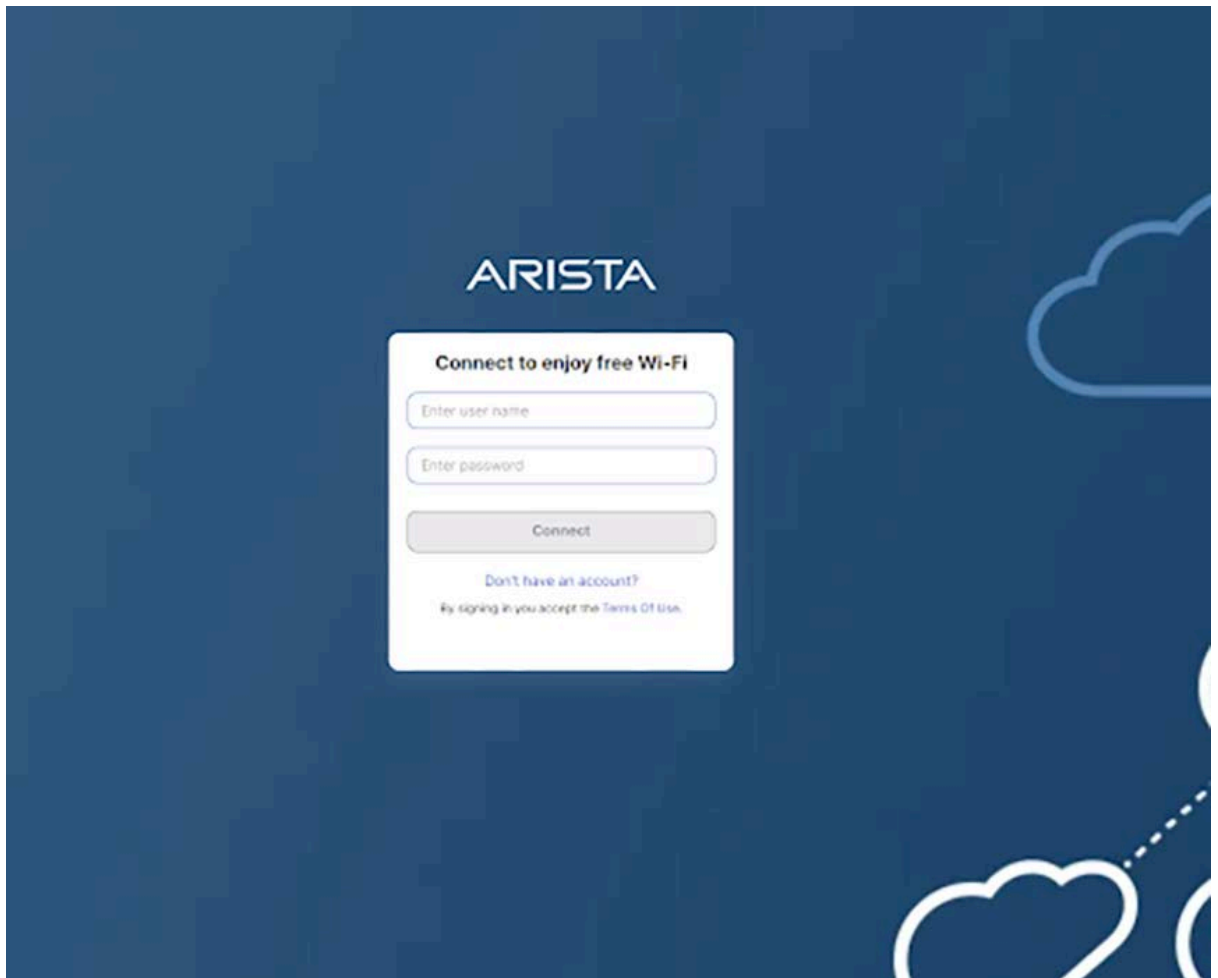
Bonjour Gateway

Redirection

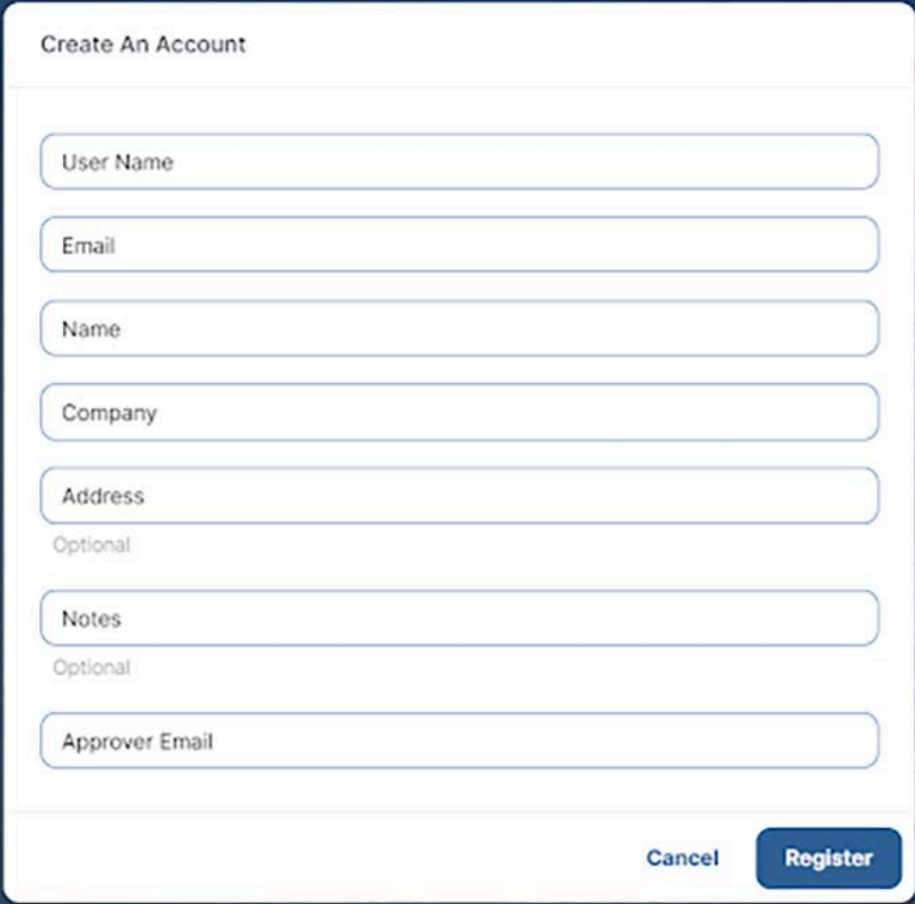
WiFi Clients in Allow List or Deny List

Client Isolation

9. Save the settings and **turn ON** the SSID.
The clients get connected and authenticated via portal authentication after entering their username and password.



1. Enter the required details in the Create an Account page and click the **Register** option.

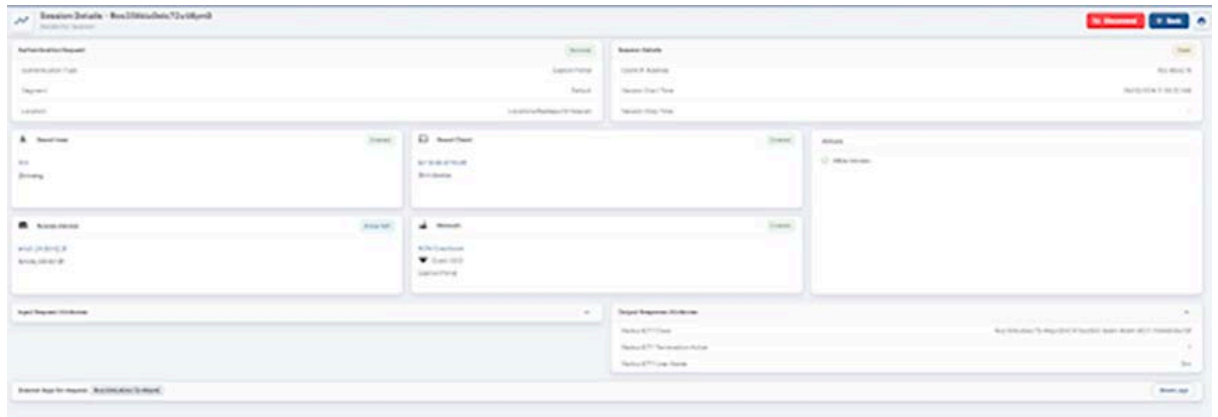


The image shows a 'Create An Account' form with the following fields and buttons:

- User Name
- Email
- Name
- Company
- Address
- Optional
- Notes
- Optional
- Approver Email
- Cancel
- Register

2. On clicking the **Register** button, the guest users receive an email with the following details:
 - a. Username
 - b. Password
 - c. Device limit
 - d. Valid From time in UTC
 - e. Valid until time in UTC

3. Provide the received credentials and the user gets onboarded to the network with a new session including all user details.



Configuring Guest Portal Using Self-Registration (Wireless)

Guest management in AGNI is enabled using the Guestbook authentication type in Guest Portals. In earlier releases, AGNI supported only the **Clickthrough** authentication type, which allowed anonymous guest access.

This article describes configuring the guest portal with the Guestbook authentication type for wireless clients. To configure the guest portal, you must configure both AGNI and CV-CUE.

Configuring the Portal on AGNI

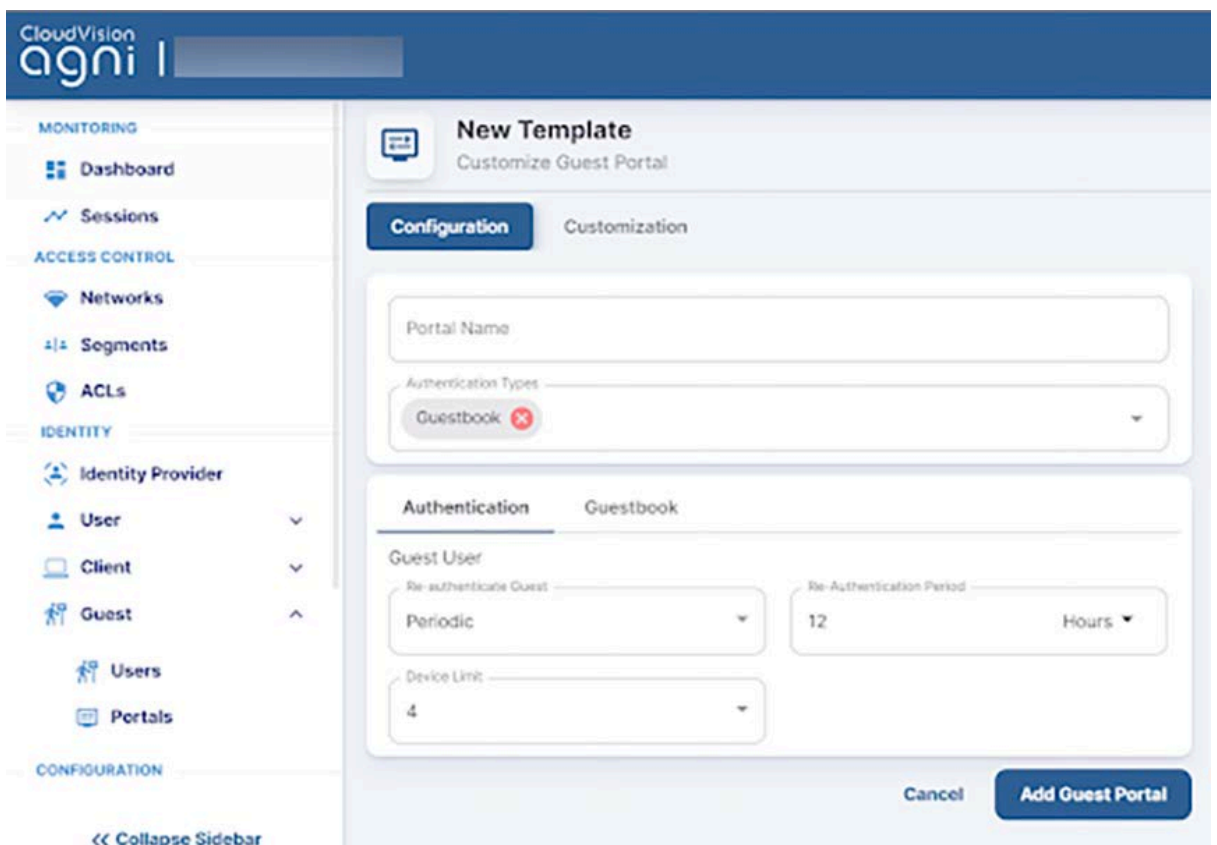
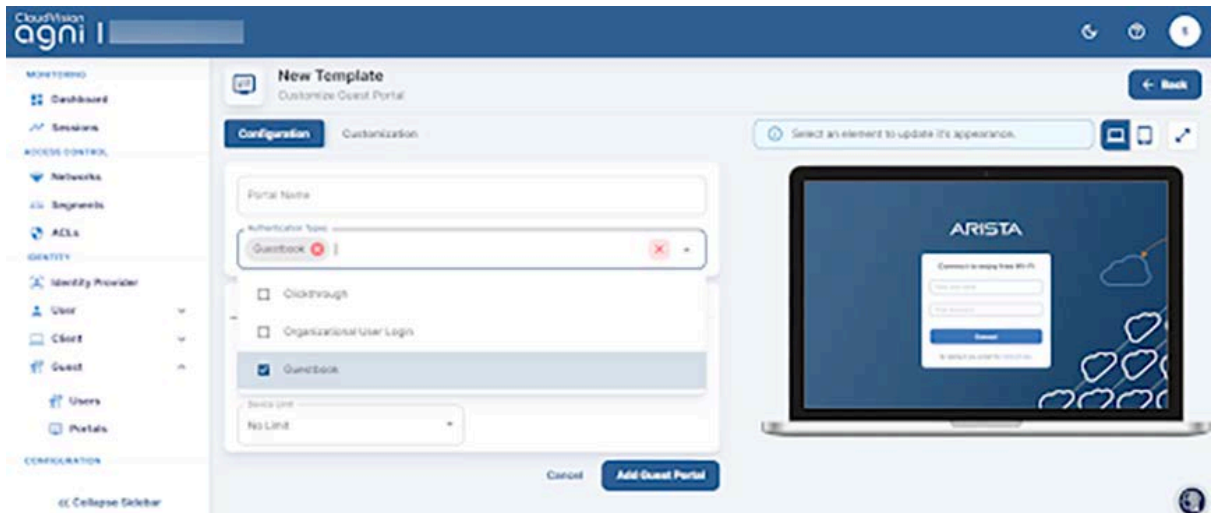
To configure the portal:

1. Log in to AGNI and navigate to **Identity > Guest > Portals**
Note: The **Default** portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.



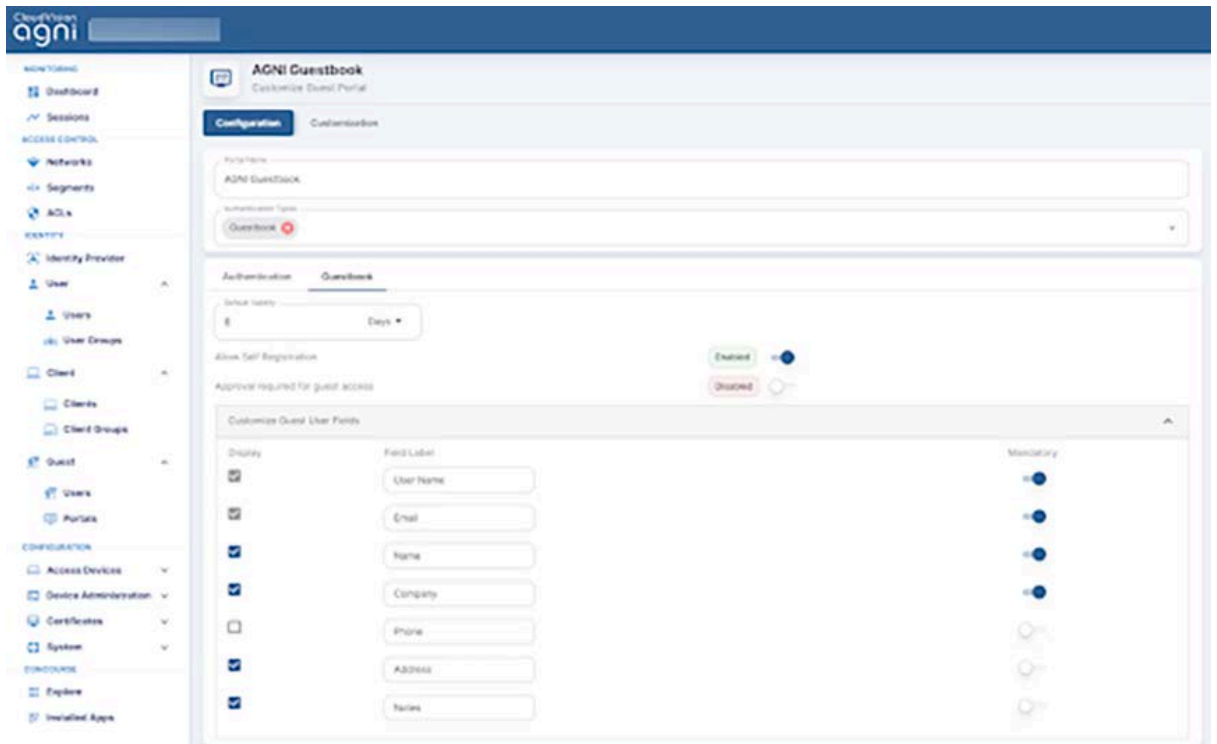
2. Click the **+Add Guest Portal** button.
3. In the **Configuration** tab, provide the portal name and select the Authentication Types. The available Authentication types are **Default**, **Organizational User Login**, and **Guestbook**. Select Guestbook as the Authentication Type.
4. From the Authentication section, select the following settings for the guest user:
 - Re-authenticate Guest - **Periodic**

- Re-authentication Period - **12 Hours**
- Device Limit - **4**



5. Navigate to Guestbook settings and configure the **Device Validity** for 8 Days. Keep **Allow Self Registration** Enabled add the following user fields:
 - User Name
 - Email
 - Name
 - Company

- Address
- Notes



Note: Device validity should always be greater than the re-authentication period. The default value for Device Validity is 8 Hours.

6. Click the **Customization** tab to customize the portal settings:
 - Theme template
 - Default
 - Split Screen
 - Select element
 - Global
 1. Page
 2. Login Toggle
 3. Terms of Use and Privacy Policy
 4. Logo
 - Guest
 1. Guest Login Submit Button
 2. User Name Textbox
 3. Password Textbox
 4. Guest Login Header
 5. Guest Login Form
 6. Self Registration
 7. Clickthrough

CloudVision
agni | [REDACTED]

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals

CONFIGURATION

<< Collapse Sidebar

AGNI Guestbook

Customize Guest Portal

Configuration **Customization**

Theme template
Default

Select element
Page

- Global
- Login Toggle
- Logo
- Page
- Terms of Use and Privacy Policy
- Guest
- Guest Login Form
- Guest Login Header

CloudVision
agni | [REDACTED]

IDENTITY

- Identity Provider
- User
- Client
- Guest
- Users
- Portals

CONFIGURATION

- Access Devices
- Device Administration
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

<< Collapse Sidebar

AGNI Guestbook

Customize Guest Portal

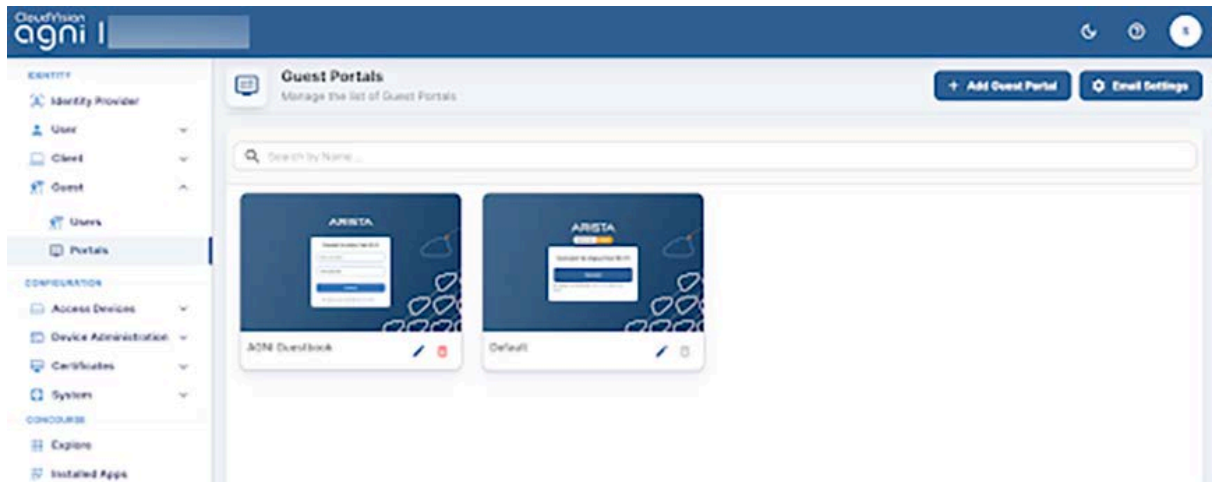
Configuration **Customization**

Theme template
Default

Select element
Page

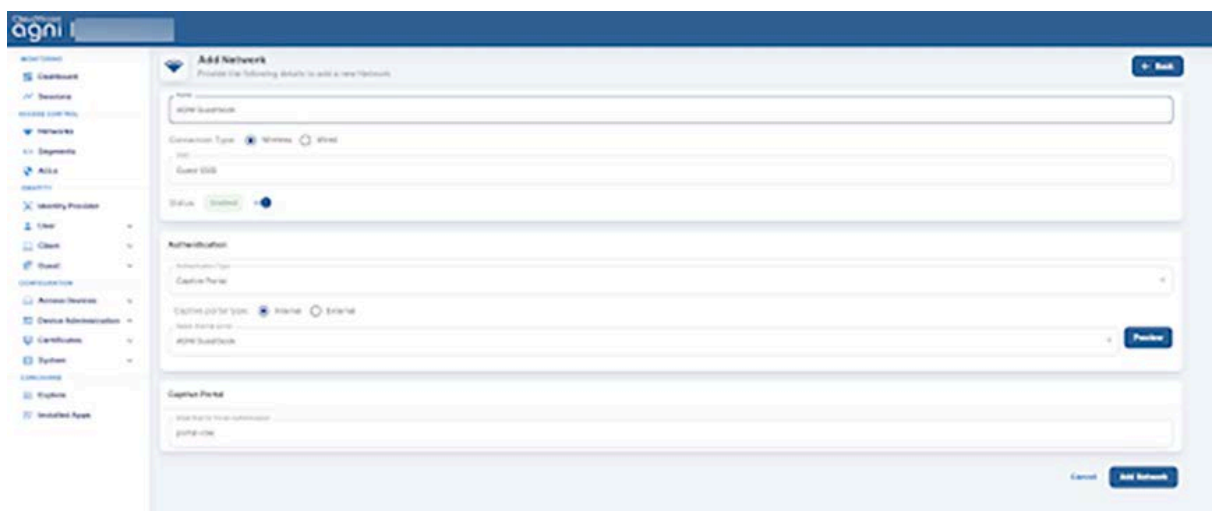
- Guest
- Guest Login Form
- Guest Login Header
- Guest Login Submit Button
- Password Textbox
- User Name Textbox
- Self Registration
- Clickthrough

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



Configuring Network

1. Navigate to the **Access Control > Network**.
2. Add a new network with the following settings:
 - o Network Name - AGNI Guestbook
 - o Connection Type — Wireless
 - o SSID - Guest SSID
 - o Status - Enabled
 - o Authentication
 - Authentication Type - Captive Portal
 - Captive Portal Type - Internal
 - Select internal portal - AGNI Guestbook
 - o Captive Portal: Internal Role for Portal Authentication - portal-role



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-role**
4. Click the **Redirection** check box and select **Dynamic Redirection**.
5. Keep other settings to default.

← portal-role

Profile Name *

portal-role

 Use default settings in Auto Role Profile
Specific Settings

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 HTTPS Redirection

Certificate Information

Common Name

www.arista.com

Organization

Arista Networks

Organization Unit

Arista Networks

Websites That Can Be Accessed Before Authorization *

login.microsoftonline.com:80,443 × aadcdn.msftauth.net:80,443 ×
aadcdn.msftauth.net:80,443 × login.live.com:80,443 ×
tyrant.sgsieng.net:80,443 ×

Configuring SSID

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

WiFi ▾

SSID

← Guest SSID

WLAN ▾

Basic

Security

Network



Name

SSID Name *

Guest SSID

Profile Name *

Guest SSID

Select SSID Type

Private Guest

Hide SSID

Include AP Name in Beacon

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

7. Select the **Authentication** and **Accounting** servers.

WiFi ▼ **SSID**

[← Guest SSID](#)

WLAN ▼ Basic Security Network **Access Control** ⋮

[▶ Firewall](#)

Client Authentication

Google Integration **RADIUS MAC Authentication**

RADIUS Settings

Radius

Primary **Additional**

Authentication Server *
radius.system.agnsrg.net ▼
Account

Accounting Server
radius.system.agnsrg.net ▼
Account

Send DHCP Options and HTTP User Agent

Retry Parameters

Attempts *
4 ⬆ ⬇ ⬆ [1 - 10]

Timeout *
2 ⬆ ⬇ ⬆ seconds [1 - 100]

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** role profile while configuring the Role Profile in the previous section.

WiFi ▾ **SSID**

← Guest SSID

WLAN ▾ Basic Security Network Access Control ⋮

Accounting Stop Delay

If Client Authorization Fails

Disconnect Stay connected

Role Based Control

RADIUS VSA Google OÜ This setting is not editable because Client Authentication via Google Integration is disabled. [Change Settings?](#)

Rule Type *

▾

Operand *

▾

Assign Role *

▾

DHCP Fingerprinting based Access Control

Bonjour Gateway

Redirection

WiFi Clients in Allow List or Deny List

Client Isolation

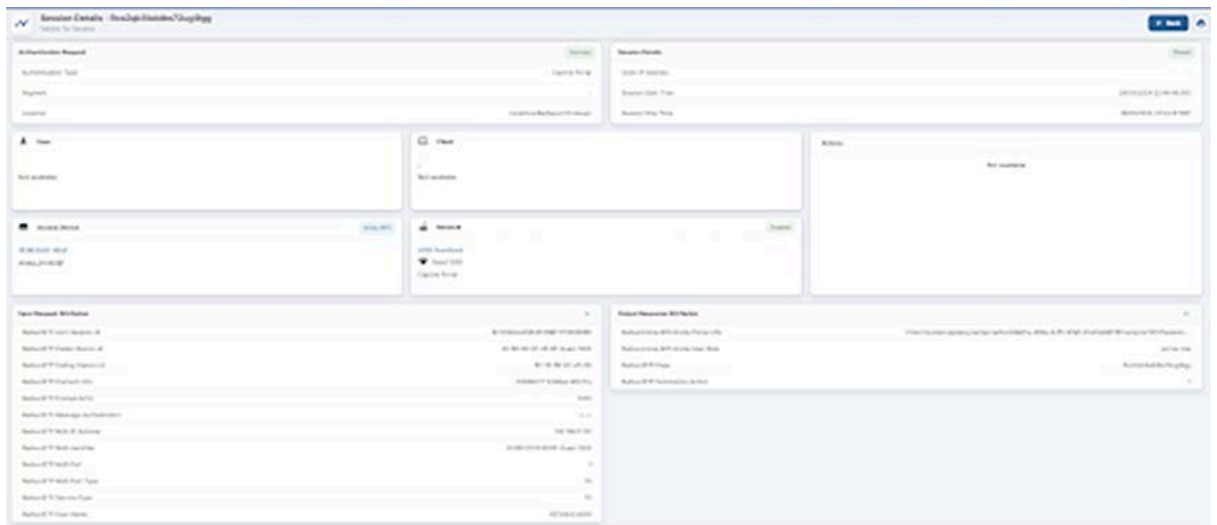
9. **Save** the settings and turn **ON** the SSID.
The clients get connected and authenticated through portal authentication after entering their username and password.
For a new client, the user should fill out the required information. An email is sent to the registered email with a username and password. Use these credentials to log in to the portal for onboarding to the network.

For existing clients, the user can use their credentials until the user validity expires.

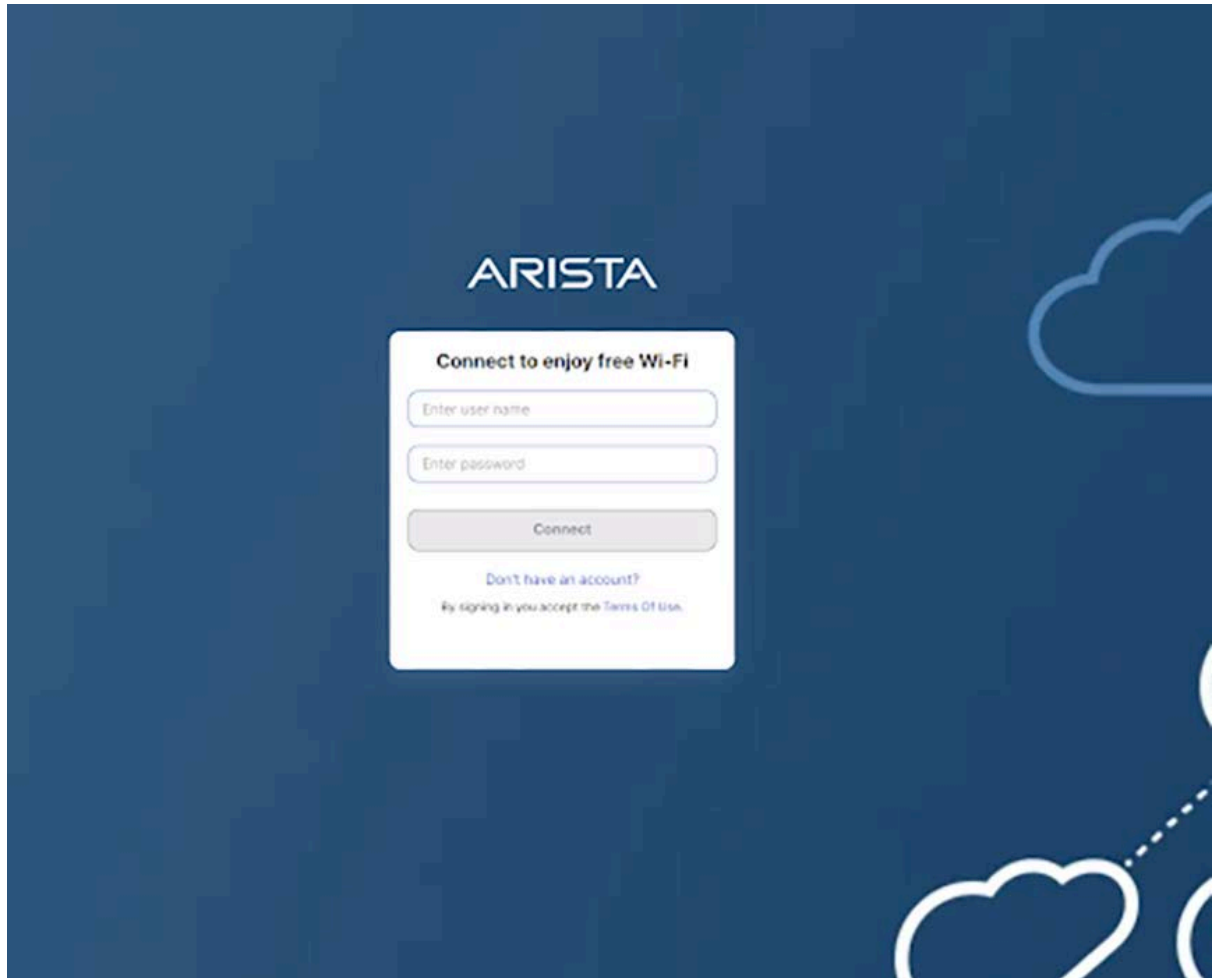
User Onboarding

To onboard the user:

When the user connects to the Guest SSID, a session is opened in AGNI. AGNI sends the role profile and portal URL in the radius access accept message.



On the portal page, the user is asked for login credentials. If the guest user does not have the login credentials, select the **Don't have an account?** Link to generate the credentials.



1. Enter the required details in the Create an Account page and click the **Register** option.

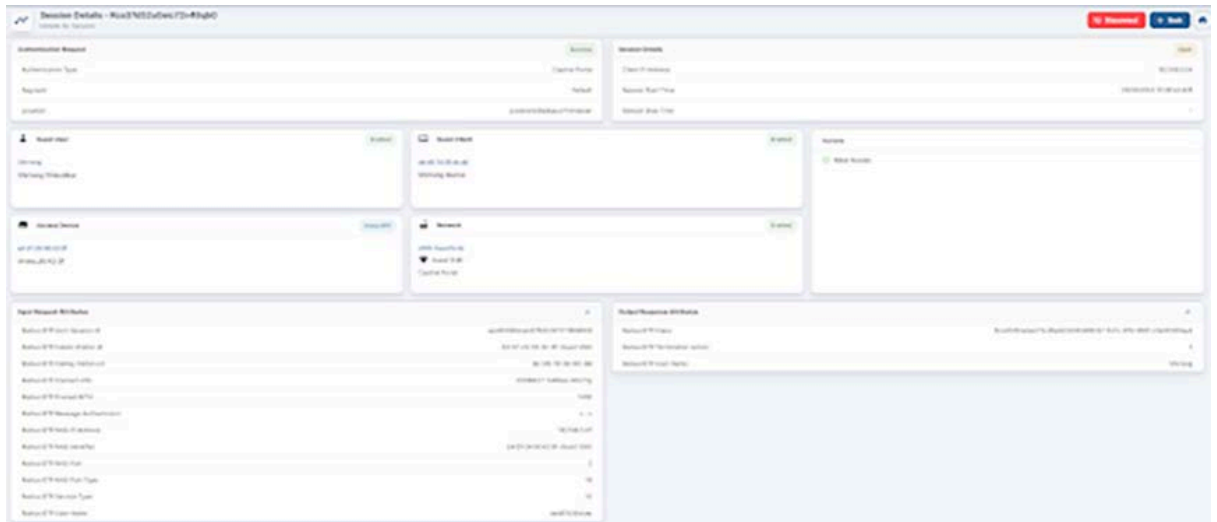
The image shows a 'Create An Account' form with the following fields and values:

- User Name: Testuser
- Email: testuser@example.com
- Name: Test
- Company: Example LLC
- Address: (empty)
- Notes: (empty)

At the bottom right, there are two buttons: 'Cancel' and 'Register'.

2. On clicking the **Register** option, guest users receive an email with the following details:
 - a. Username
 - b. Password
 - c. Device limit
 - d. Valid From time in UTC
 - e. Valid until time in UTC

3. Provide the received credentials and the user gets onboarded to the network with a new session including all user details.



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**.

The screenshot displays the CloudVision AGNI interface for configuring a network. The left sidebar shows the navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Certificates, System), and CONCOURSE (Explore, Installed Apps). The main content area is titled 'ACME-CORP' and includes a 'Back' button. The configuration form is divided into several sections: 1. Network Name: 'ACME-CORP'. 2. Connection Type: 'Wireless' (selected) and 'Wired'. 3. SSID: 'ACME-Corp'. 4. Status: 'Enabled' (toggle switch). 5. Authentication: 'Authentication Type' is set to 'Client Certificate (EAP-TLS)'. 6. Domain Machine Authentication: 'Enabled' (toggle switch). 7. Trust External Certificates: 'Enabled' (toggle switch). 8. CRL Verification: 'Enabled' (toggle switch). 9. OCSP Verification: 'Enabled' (toggle switch). 10. User Identity Binding: 'Required' (selected) and 'Optional'. Informational messages are provided for CRL and OCSP verification, and for user identity binding.

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. **Enable Allow Email Code Login for IDP User**: This configuration is applicable for UPSK and EAP-TLS network authorization types. Users onboarding the device to AGNI through Self-Service portal have the option to login through Email Code (OTP). AGNI Self-Service Portal onboards the user after OTP verification (sent to your registered email account). Optionally, if IDP synchronization is enabled, then the user attributes and group information gets updated. For details, see the [Authenticating Users with Email Codes \(as against IDP\)](#) section.
 - c. **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** or **Update 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

Initial Passphrase for Onboarding

Initial Role for Onboarding

Show Domains

Allow Email Code Login for IDP User: Enabled

Allow Local User Self Registration: Enabled

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

Copy

Users can scan a Wi-Fi QR code to connect to this SSID for onboarding. Print QR Code

Onboarding
Enabled

Allow Local User Self Registration: Enabled

i Users can onboard their clients using the below URL.

Copy

Cancel
Update Network

Figure: Wireless EAP-TLS Network User Onboarding

Authenticating Users with Email Codes (as against IDP)

The Identity Provider (IDP) users can now onboard their devices using an email OTP authentication method, removing the necessity of entering their Single Sign-On (SSO) credentials.

To enable this feature:

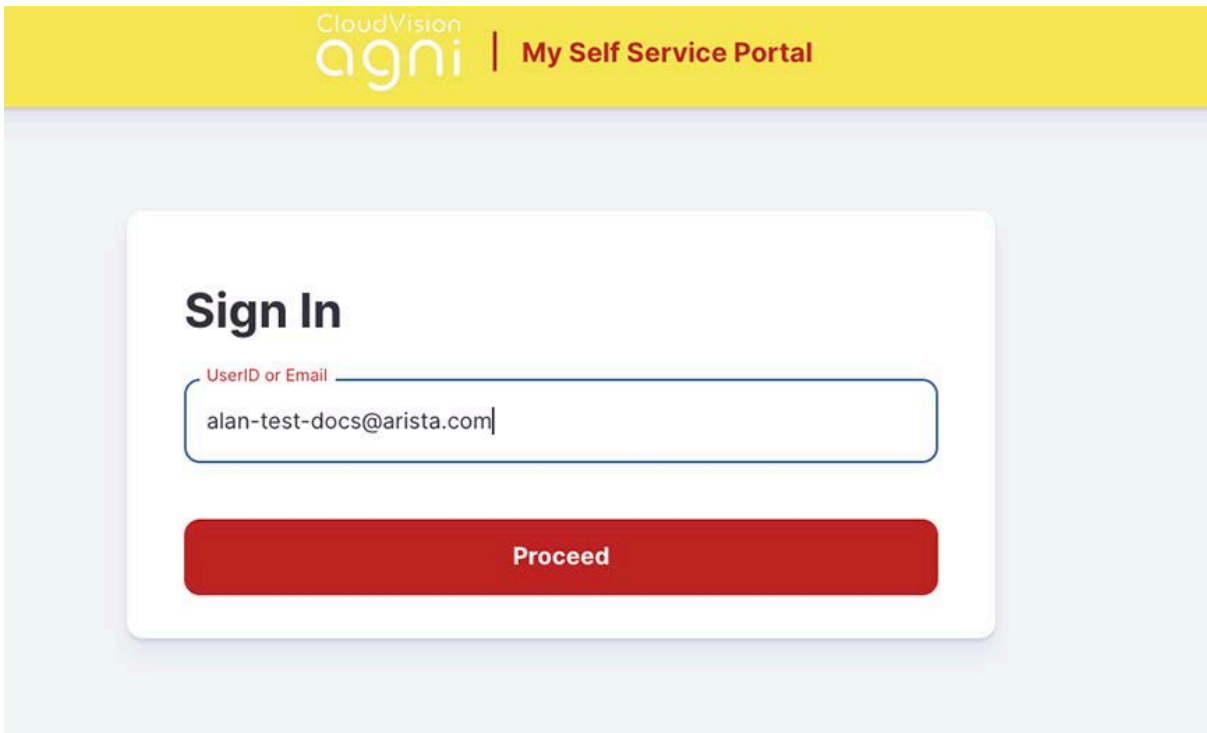
1. Navigate to **Access Control >> Networks** and select your network.
2. Enable the **Allow Email Code Login for IDP Users** in the Onboarding section.
3. Click the **Update Network** to enable the feature.

The screenshot shows the CloudVision agni interface for configuring a network named "Test-docs". The left sidebar lists various sections: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client, Guest), CONFIGURATION (Access Devices, Device Administration, Access Policy, TACACS+ Profiles), Certificates, System, CONCOURSE (Explore, Installed Apps). The main content area is titled "Test-docs" and includes a "Back" button. The configuration fields are as follows:

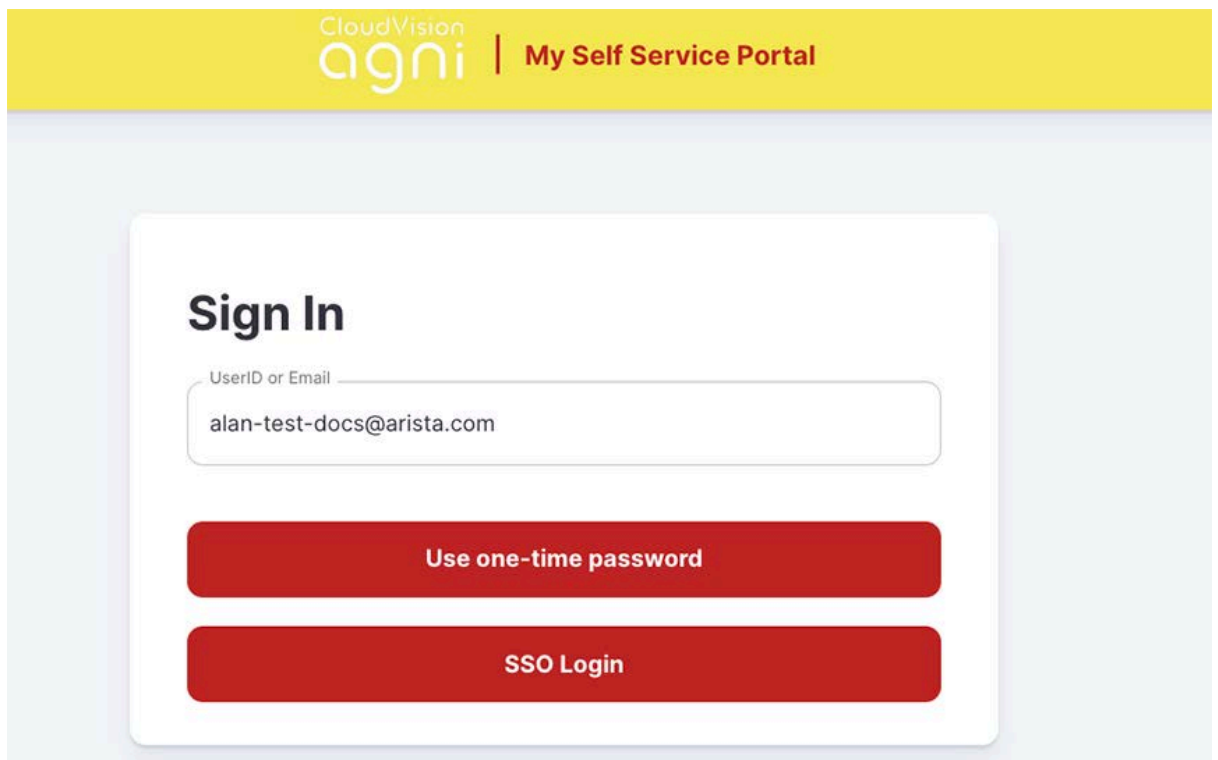
- Name: Test-docs
- Connection Type: Wireless Wired
- SSO: Test-docs
- Status: Enabled
- Authentication Type: Client Certificate (EAP-TLS)
- Domain Machine Authentication: Enabled
- Trust External Certificates: Disabled
- Onboarding: Enabled
- Allow Email Code Login for IDP User: Enabled
- Authorized User Group: Select Authorized User Groups...
- Users can onboard their clients using the following URL: <https://dev.agnienet.net/onboard/Eb9107b0d-c35f-42e8-ad1f-48f2c39f6686/network/378> (Copy)

Buttons at the bottom: Cancel, Update Network

4. Once enabled, copy the onboarding URL and open it from the computer you want to onboard and log in to.



5. Click the **Proceed** button and click the **Use one-time password** option.



6. Check your registered email for OTP details:

Arista Guardian for Network Identity (AGNI)

Hello [redacted] [@arista.com](mailto:[redacted]@arista.com)

You have requested for one-time password (OTP) to log in to AGNI Self-Service Portal.

Login using the following details:

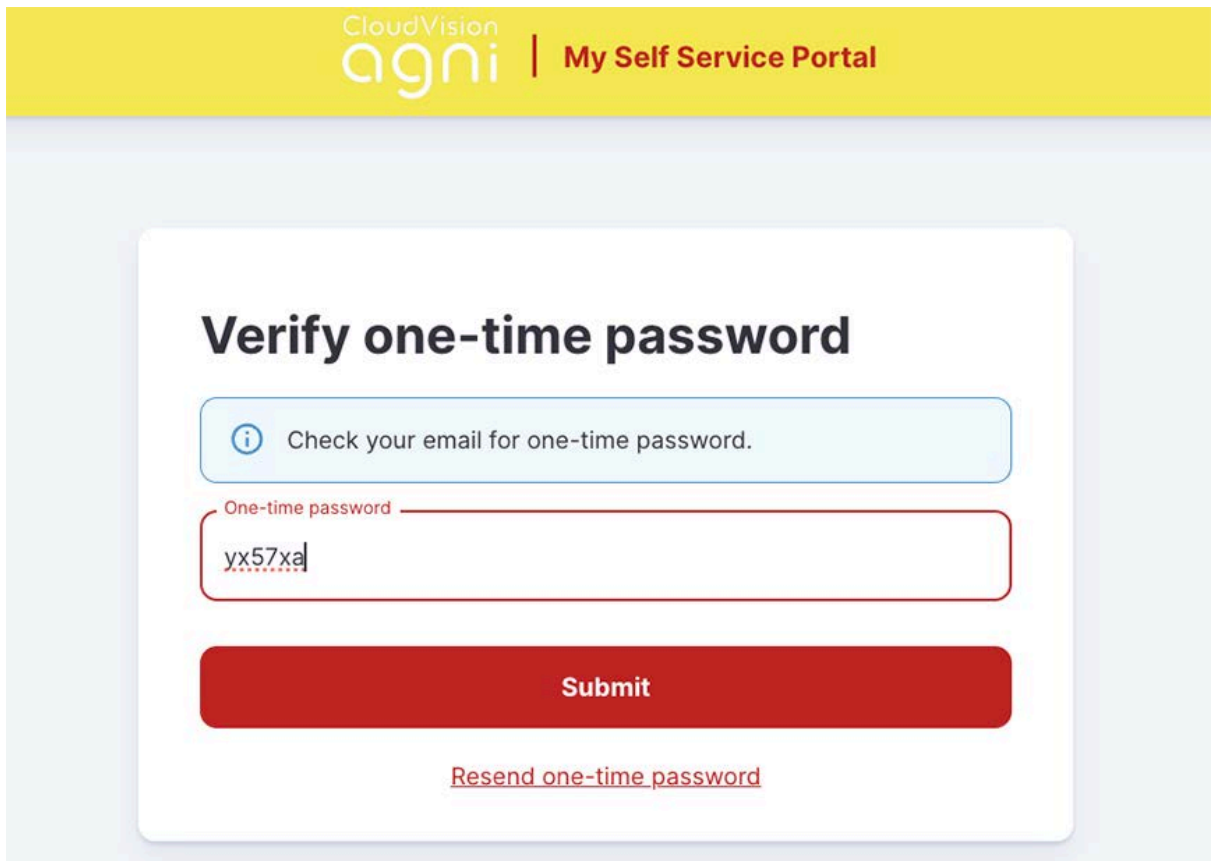
Email: [redacted] [@arista.com](mailto:[redacted]@arista.com)

OTP: yx57xa

The one-time password (OTP) will expire at 01 Apr 24 08:46 UTC.

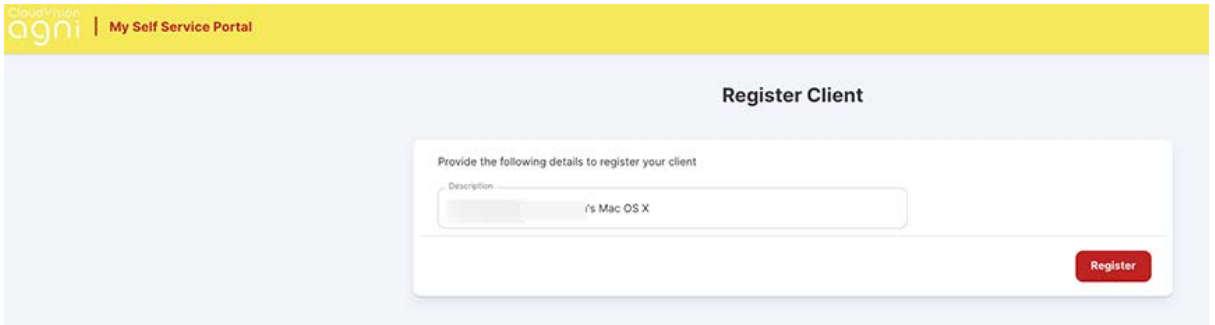
This is an automated email notification. Please do not reply to this message.

7. Copy the OTP, paste that for the authentication against IDP, and click the **Submit** button.

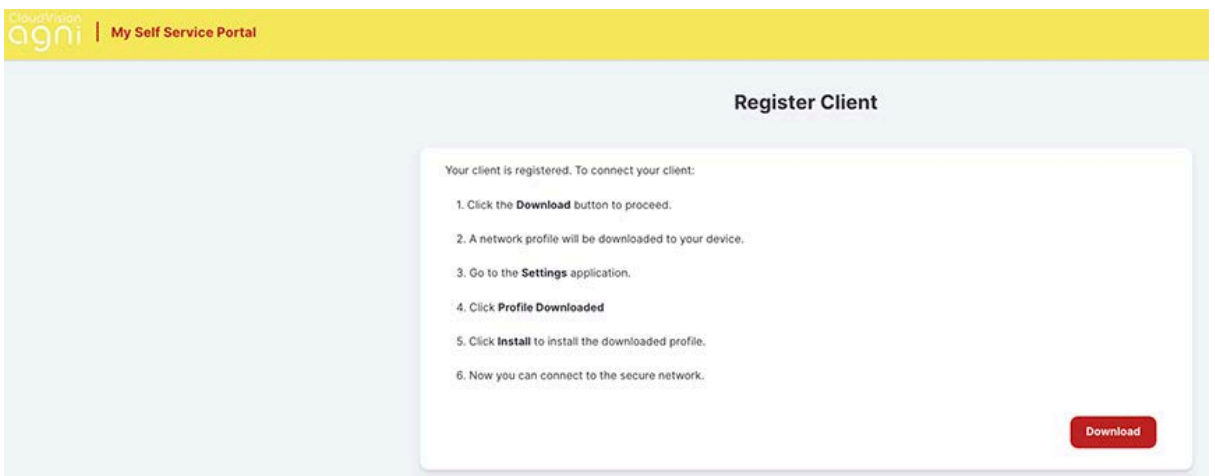


The screenshot shows the 'Verify one-time password' page in the AGNI Self-Service Portal. The page has a yellow header with the 'CloudVision agni' logo and 'My Self Service Portal' text. The main content area is white with a light blue border. It features a title 'Verify one-time password', an information box with an 'i' icon and the text 'Check your email for one-time password.', a text input field labeled 'One-time password' containing 'yx57xa', a red 'Submit' button, and a red link for 'Resend one-time password'.

8. After successfully logging into the Self-Service portal, click on the **Register** button to complete the onboarding process.



The device client gets registered, and the following page is displayed. Click the download button and proceed with the steps to connect to AGNI network.



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.

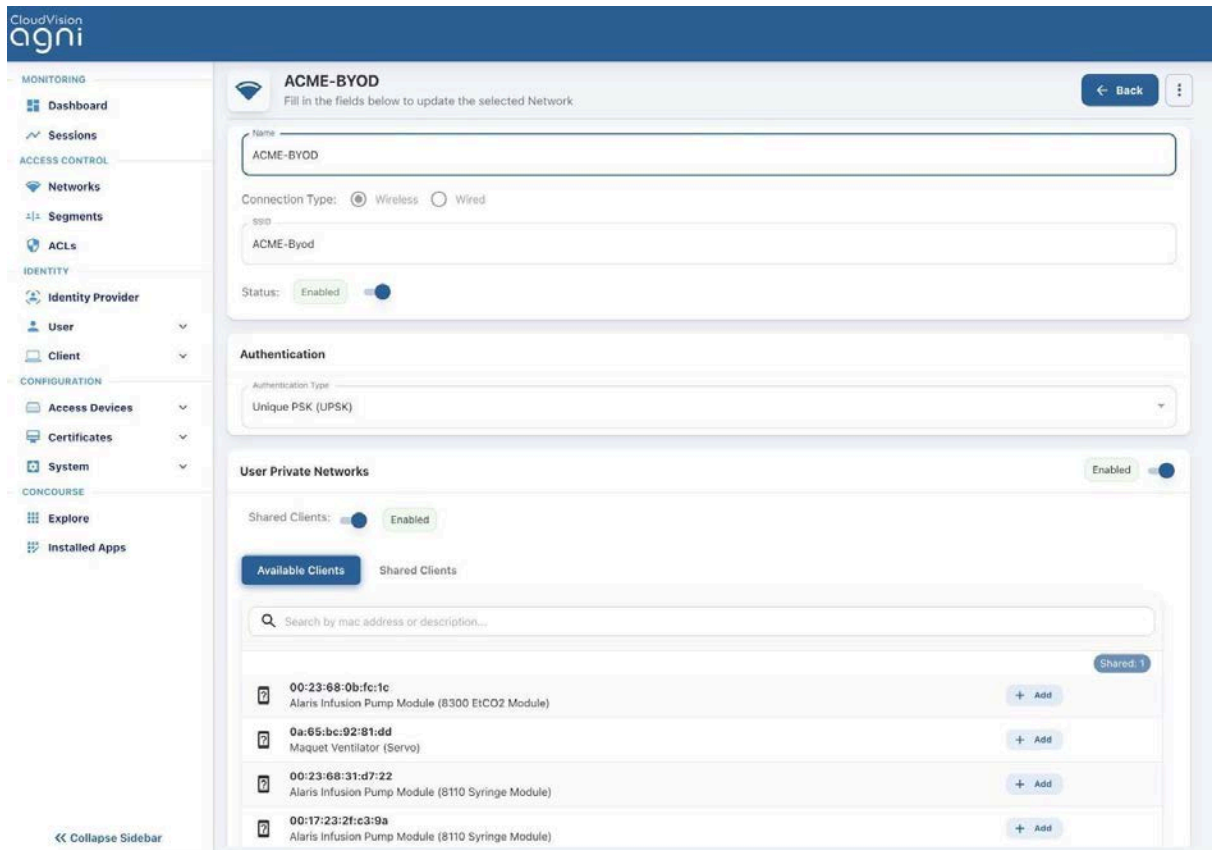


Figure: Wireless UPSK Network

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 Email Code Login for IDP User:** Click the toggle button to enable email code login.
- e. **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.

The screenshot shows a configuration page for network onboarding. At the top right, there is a toggle switch labeled 'Enabled'. Below this, there are two input fields: 'Initial Passphrase for Onboarding' with the value 'changeme123' and 'Initial Role for Onboarding' with the value 'onboarding-psk'. To the right of the second field is a 'Show Domains' button. Below these fields is another toggle switch for 'Allow Local User Self Registration', also labeled 'Enabled'. A light blue box contains the instruction: 'Configure the below URL as captive portal for this SSID to allow users to onboard their clients.' Below this is a text input field containing the URL 'https://qa.antaraops.net/onboard/Ee8eb46d1-d266-460d-9b41-a904b655234b/network/4', with 'Copy' and 'Print QR Code' buttons to its right. At the bottom right, there are 'Cancel' and 'Update Network' buttons.

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)

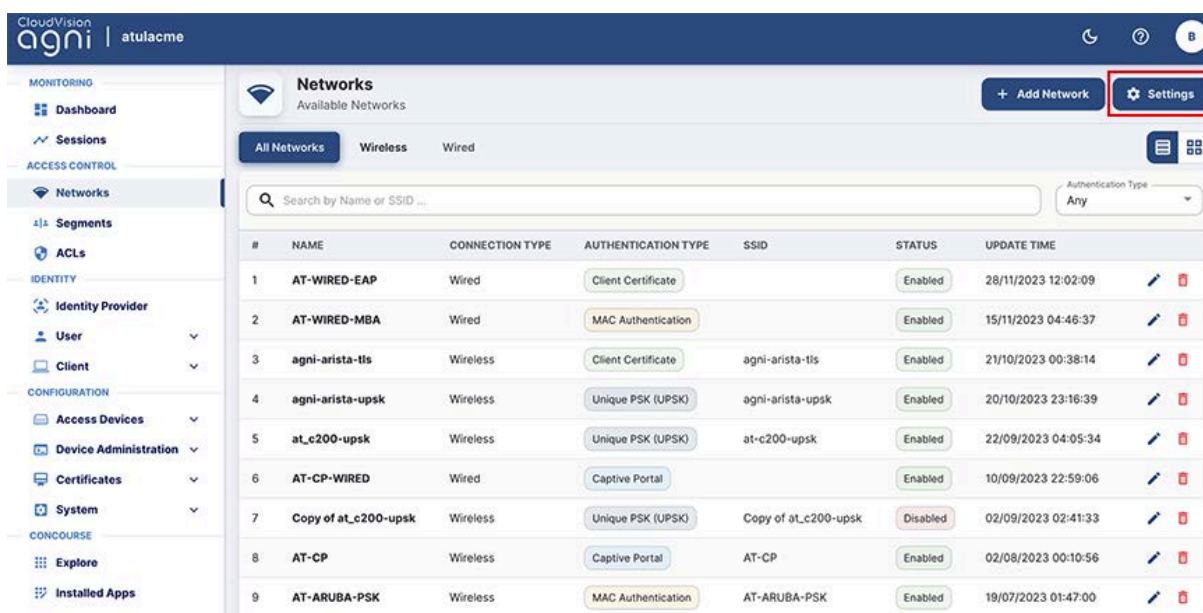


Figure:Networks Page

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

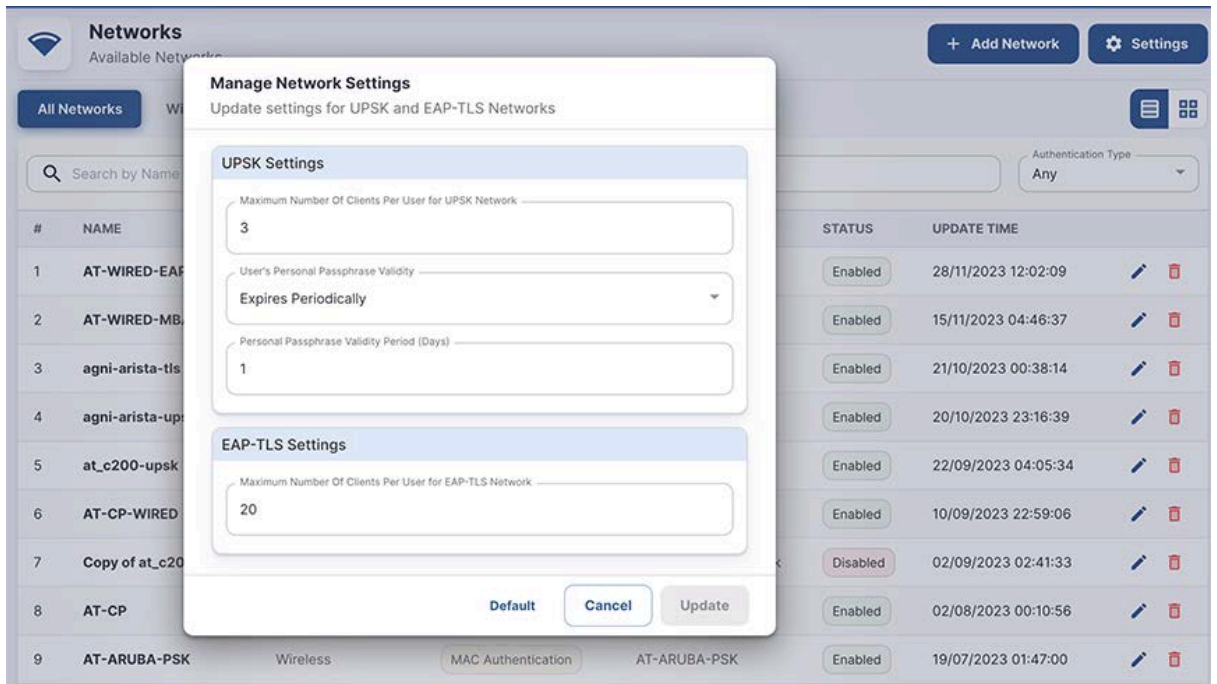


Figure: Manage Network Settings

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:

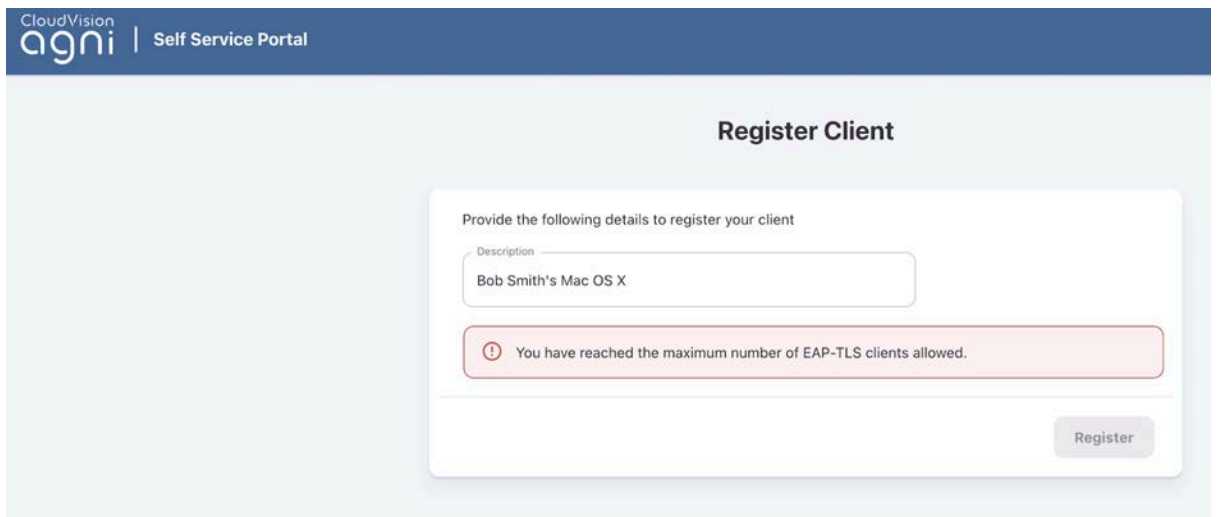


Figure: Registering a Client

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.

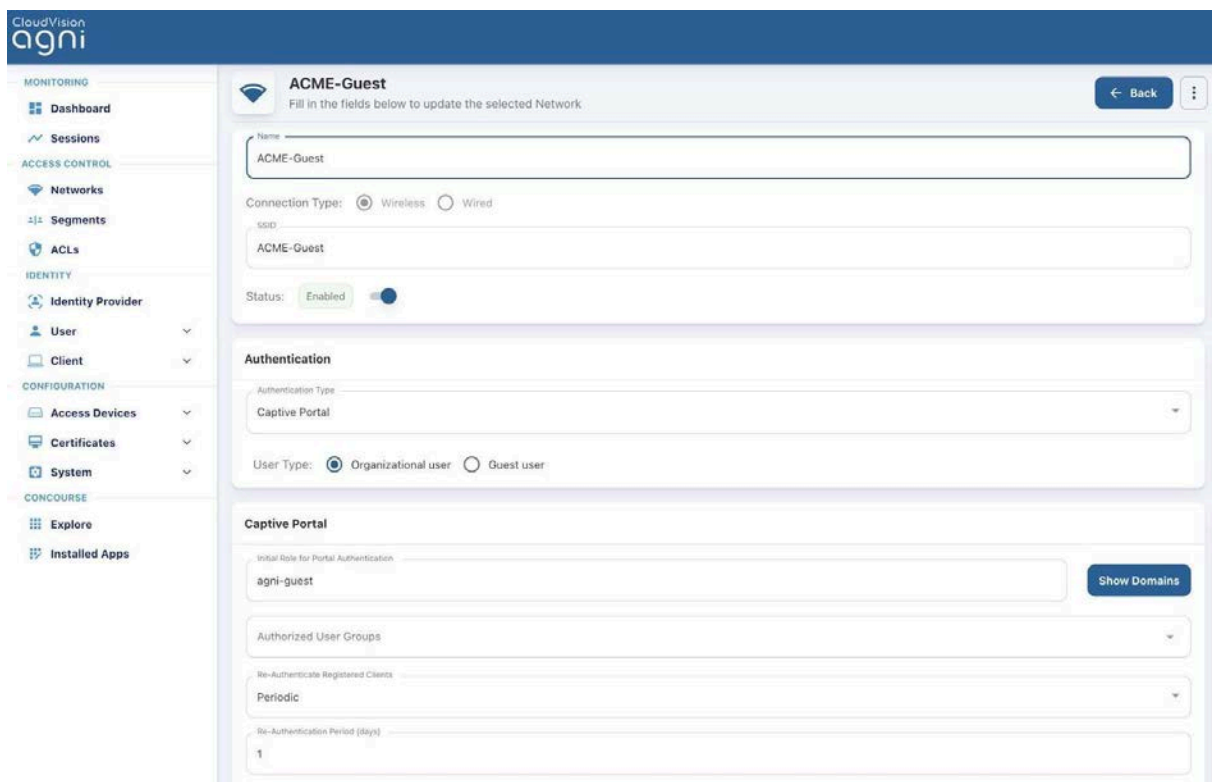


Figure: Wireless Captive Portal Network-page-1

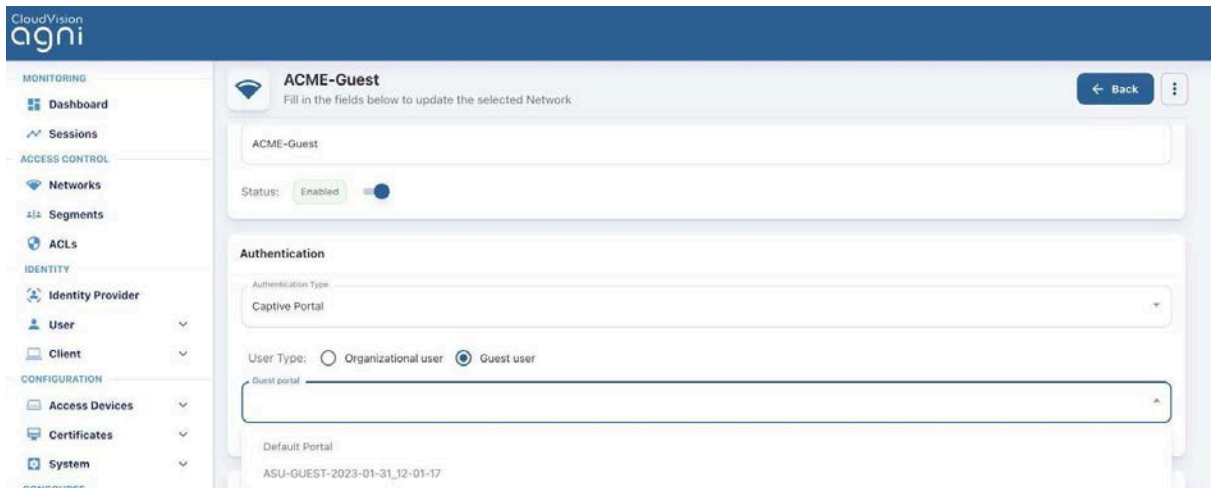


Figure: Wireless Captive Portal Network-page2

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.



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**.

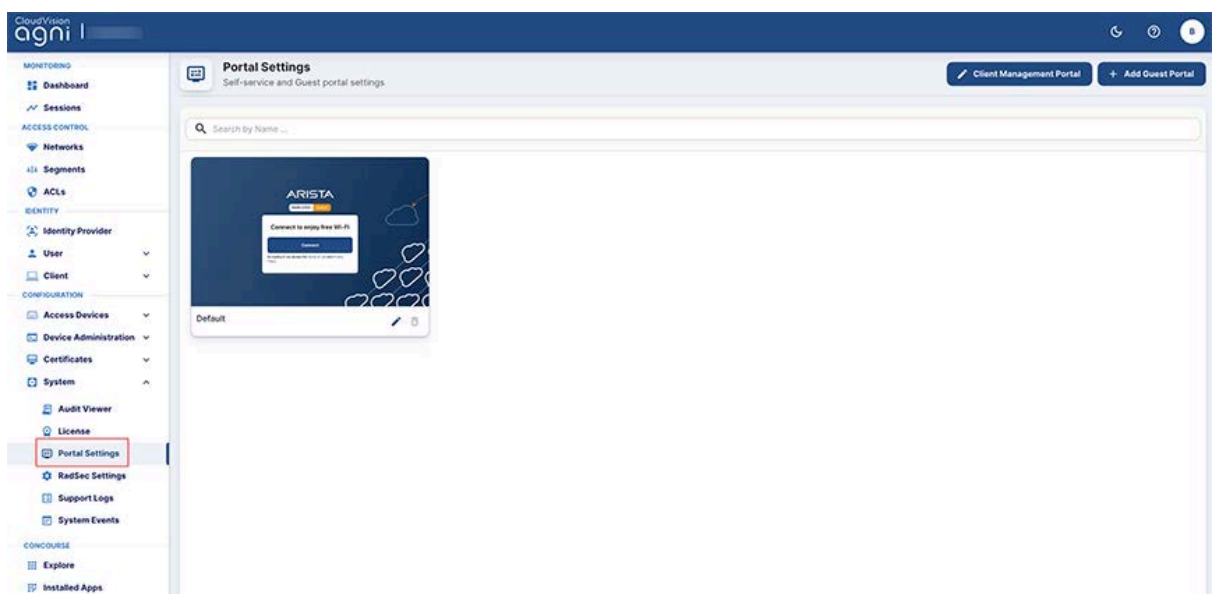


Figure: Portal Settings

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.

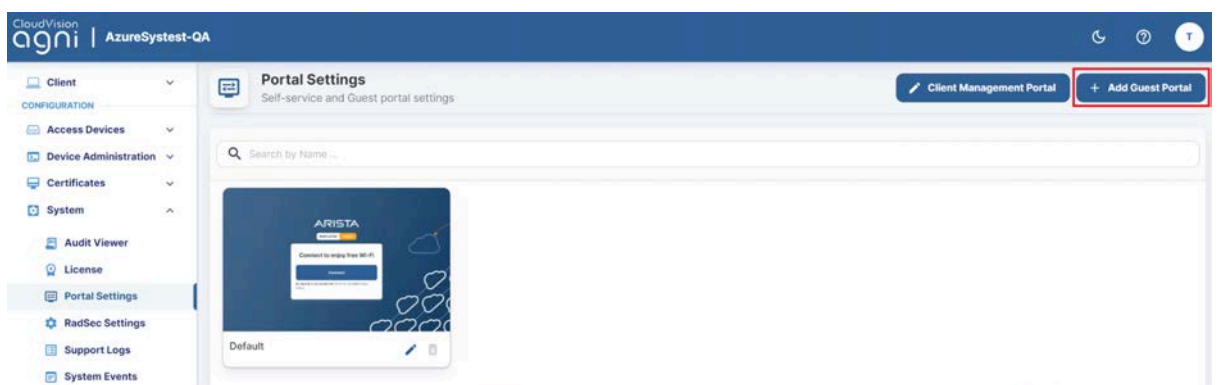


Figure: Portal Settings -1

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**.

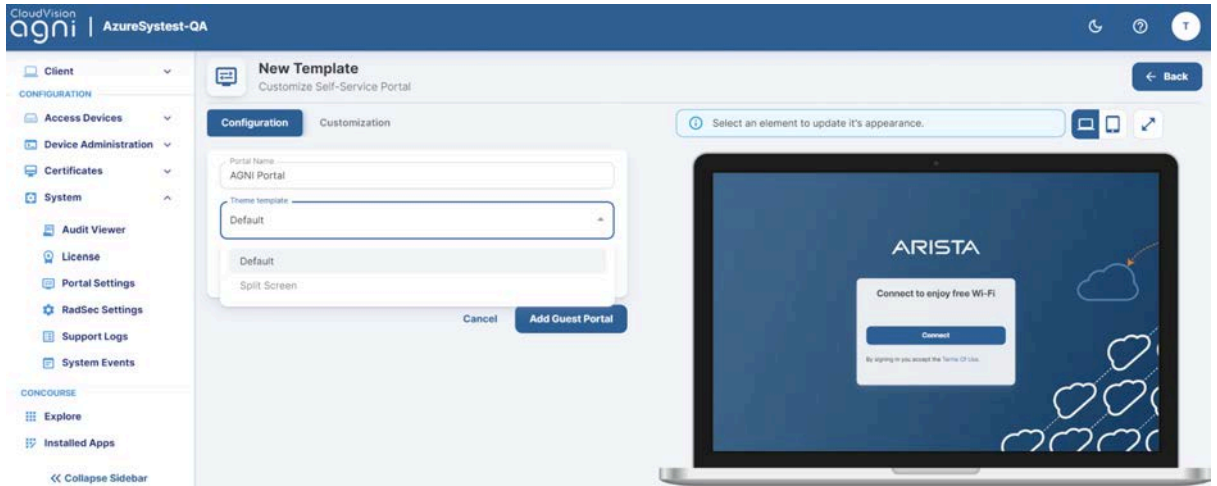


Figure:Portal Settings - Template

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

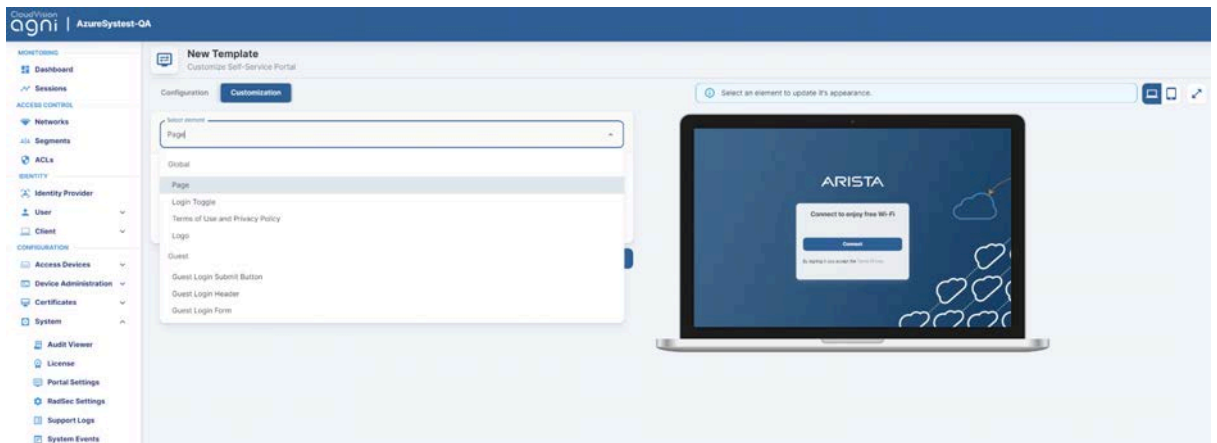


Figure:Portal Settings- Template-1

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

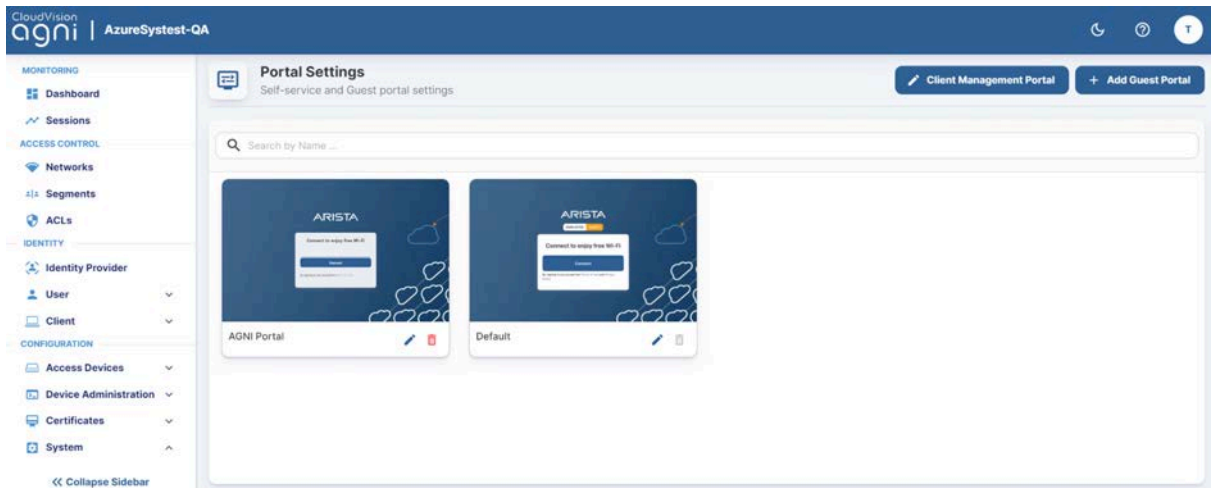


Figure: Portal Settings page

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

← Back

Provide the following details to add a new Network

Captive portal type: Internal External

Select internal portal Preview

AGNI Portal

Captive Portal

Initial Role for Portal Authentication

Portal

Authorized User Groups ▼

Applicable for organizational users only

Re-Authenticate Clients ▼

Always

Cancel
Add Network

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

The screenshot shows the 'Captive Portal' configuration page. At the top, there's a header with a Wi-Fi icon, the title 'Captive Portal', and a subtitle 'Provide the following details to update the selected Network'. A 'Back' button and a menu icon are in the top right. Below the header, there are two main sections. The first section is for 'Captive portal type', with 'Internal' selected and 'External' unselected. A dropdown menu shows 'AGNI Portal' selected, and a 'Preview' button is to its right. The second section is titled 'Captive Portal' and contains several fields: 'Initial Role for Portal Authentication' set to 'Portal' with a 'Show Domains' button; 'Authorized User Groups' dropdown; 'Applicable for organizational users only' checkbox; 'Re-Authenticate Clients' dropdown set to 'Always'; and a text field for the portal URL: 'https://qa.agnienet.net/portal/Eba61d189-e361-4837-a116-182575420cfb/network/376' with a 'Copy' button. At the bottom right, there are 'Cancel' and 'Update Network' buttons.

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**

← **Portal**

Profile Name*
Portal

Use SSID Settings in Absence of Role-Specific Settings

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.agnienet.net/portal/Eba61d189-e361-4f

HTTPS Redirection

Certificate Information

Common Name: www.arista.com
Organization: Arista Networks
Organization Unit: Arista Networks

Websites That Can Be Accessed Before Authorization *

qa.agnienet.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.

WiFi ▾

SSID

← Captive Portal Test

WLAN ▾

Basic

Security

Network

Access Control



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 OUI

This setting is not editable because Client Authentication via Google Integration is disabled.

[Change Settings?](#)

Rule Type *		
<input type="text" value="802.1X Default VSA"/>	<input type="text"/>	
Operand *	Assign Role *	
<input type="text" value="Match"/>	<input type="text" value="All"/>	<input type="text"/>



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.

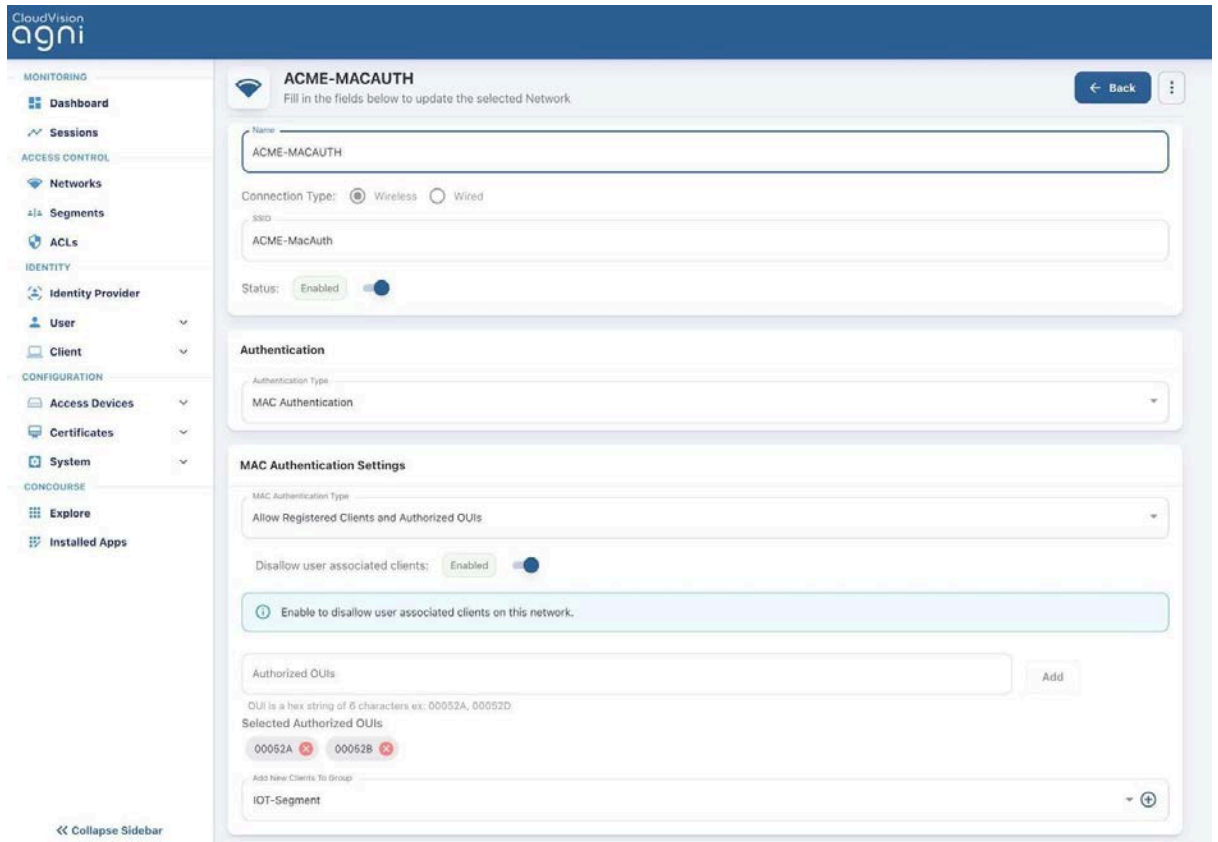


Figure: Wireless MAC Authentication Network

Wired 802.1X

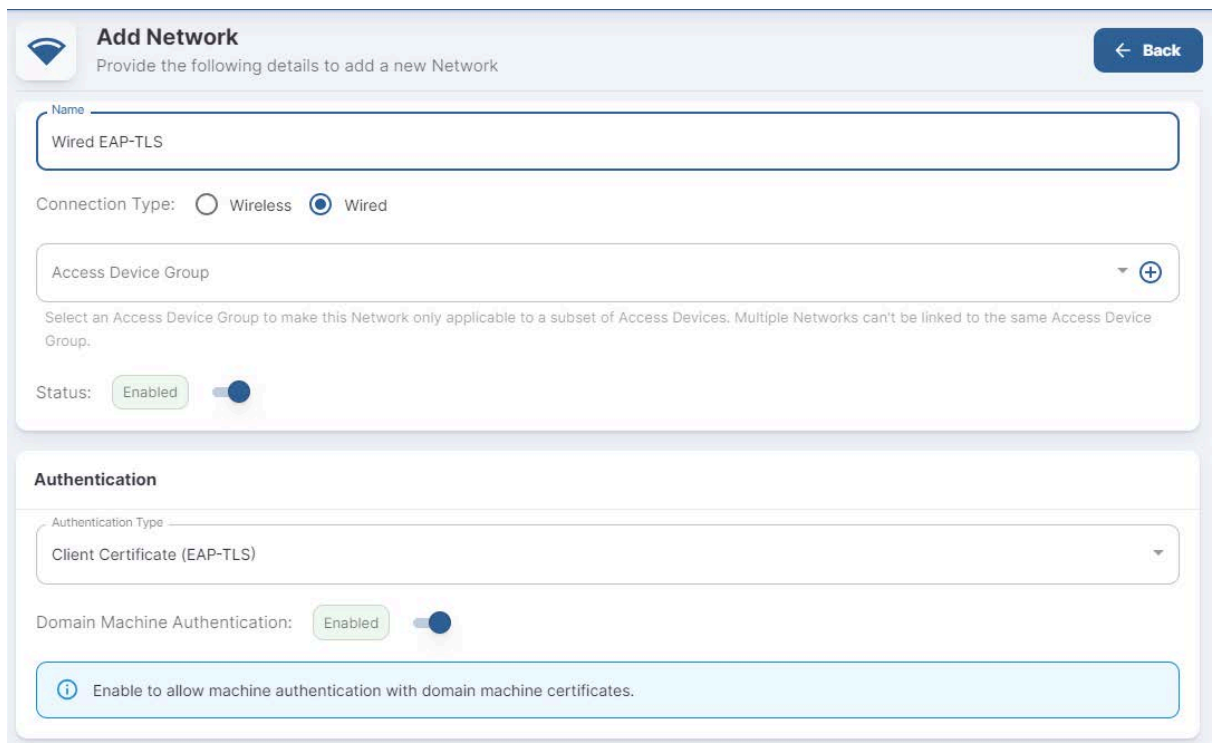
Wired network configuration enables you to authenticate end clients connected to the wired switch port. The system supports 802.1X authentications from the endpoints.

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.



The screenshot shows the 'Add Network' configuration page. At the top, there is a title 'Add Network' and a subtitle 'Provide the following details to add a new Network'. A 'Back' button is in the top right corner. The main form contains the following fields and controls:

- Name:** A text input field containing 'Wired EAP-TLS'.
- Connection Type:** Radio buttons for 'Wireless' and 'Wired', with 'Wired' selected.
- Access Device Group:** A dropdown menu with a plus icon, currently empty.
- Status:** A toggle switch labeled 'Enabled' that is turned on.
- Authentication:**
 - Authentication Type:** A dropdown menu with 'Client Certificate (EAP-TLS)' selected.
 - Domain Machine Authentication:** A toggle switch labeled 'Enabled' that is turned on.
 - Info:** A light blue box with an information icon and the text: '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.



The screenshot shows a single toggle switch for 'Trust External Certificates'. The label 'Trust External Certificates' is on the left, and the toggle is on the right, currently in the 'Disabled' position.

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.

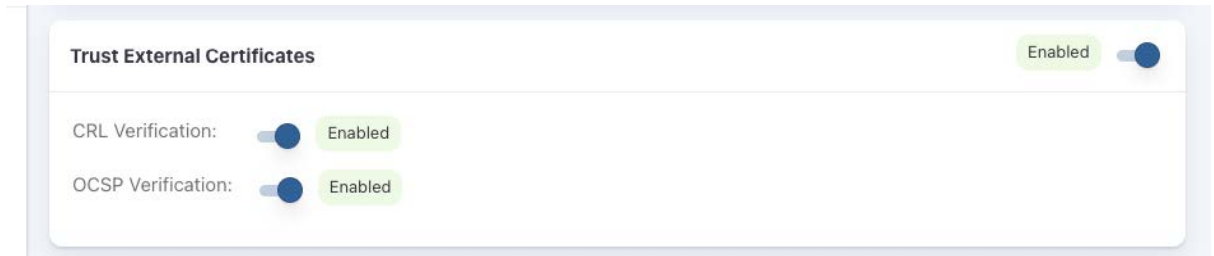


Figure: Add Network (Trusted External Certificates)

7. Fallback to MAC Authentication

- a. **Disabled** - When 802.1X authentication fails, the system rejects the client authentication attempt.

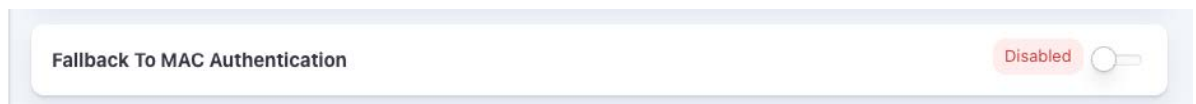


Figure 45: Add Network (Fallback To MAC Authentication)

- 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.



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.

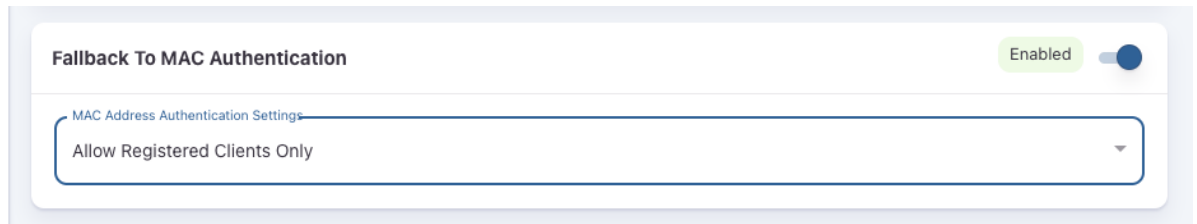


Figure: Add Network (Fallback to MAC Authentication)

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.



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.

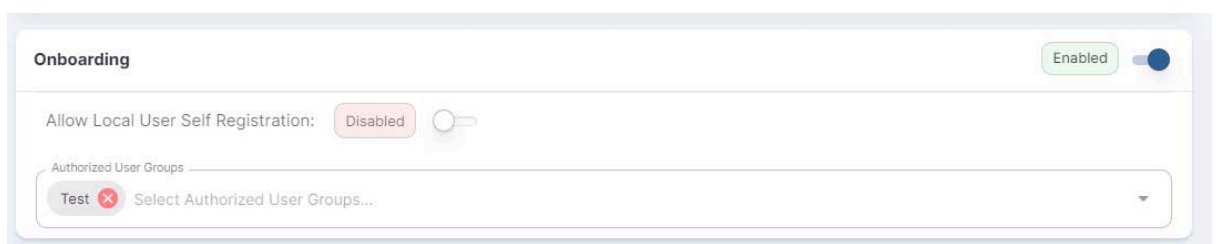


Figure: Onboarding

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

The screenshot shows the 'Add Network' configuration page in the CloudVision interface. The page is titled 'Add Network' and includes a 'Back' button in the top right corner. The main content area is divided into several sections:

- Status:** A toggle switch labeled 'Enabled' is turned on.
- Authentication:** A dropdown menu for 'Authentication Type' is set to 'Client Certificate (EAP-TLS)'. Below it, a 'Domain Machine Authentication' toggle is also turned on. A blue button with a plus icon and the text 'Enable to allow machine authentication with domain machine certificates.' is visible.
- Trust External Certificates:** A toggle switch labeled 'Disabled' is turned off. A blue button with a plus icon and the text 'Enable this setting to accept client certificates issued by external CAs.' is visible.
- Fallback To MAC Authentication:** A toggle switch labeled 'Enabled' is turned on. A dropdown menu for 'MAC Authentication Type' is set to 'Allow Registered Clients Only'. A blue button with a plus icon and the text 'Enable to disallow user associated clients on this network.' is visible.
- Onboarding:** A toggle switch labeled 'Disabled' is turned off.

At the bottom right, there are 'Cancel' and 'Add Network' buttons.

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.



The screenshot shows the 'MAC Authentication Settings' configuration panel. At the top, the title 'MAC Authentication Settings' is displayed. Below it, there is a dropdown menu labeled 'MAC Authentication Type' with 'Allow All Clients' selected. Underneath, there is a text input field labeled 'Add New Clients To Group' with a plus sign icon to its right.

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.



The screenshot shows the 'MAC Authentication Settings' configuration panel. The 'MAC Authentication Type' dropdown is set to 'Allow Registered Clients Only'. Below this, there is a toggle switch for 'Disallow user associated clients:' which is currently turned on (labeled 'Enabled'). At the bottom, there is a light blue information box with an 'i' icon and the text: '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.

The screenshot shows the 'MAC Address Authentication Settings' configuration page. At the top, there is a dropdown menu for 'MAC Address Authentication Settings' currently set to 'Allow Authorized OUIs Only'. Below this is a text input field for 'Authorized OUIs' with an 'Add' button to its right. A note below the field states: 'OUI is a hex string of 6 characters ex: 00052A, 00052D'. Underneath, a section titled 'Selected Authorized OUIs' displays two entries: '00052A' and '00052D', each with a red 'X' icon to its right. At the bottom, there is another dropdown menu labeled '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.

The screenshot shows the ARISTA Next-Gen Identity 'Update Network' configuration page for a 'Corporate MAC ByPass Authentication Wired' network. The page has a left-hand navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Certificates, Administration), and CONCOURSE (Explore, Installed Apps). The main content area is titled 'Update Network - Corporate MAC ByPass Authentication Wired' and includes a sub-header 'Fill in the fields below to update the selected Network'. The configuration fields are: 'Name' (Corporate MAC ByPass Authentication Wired), 'Connection Type' (Wireless, Wired - with Wired selected), 'Access Device Group' (No Access Device Groups are configured), 'Authentication Type' (MAC Address Authentication), and 'MAC Address Authentication Settings' (Allow Registered Clients Only). At the bottom right, there are 'Cancel' and 'Update Network' buttons.

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
 [Show Domains](#)

Re-Authenticate Clients

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

[Copy](#)

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

Authorized User Groups

Re-Authenticate Registered Clients

Re-Authentication Period (days)

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.

[Copy](#)

Network has been saved. [Back to Networks](#)

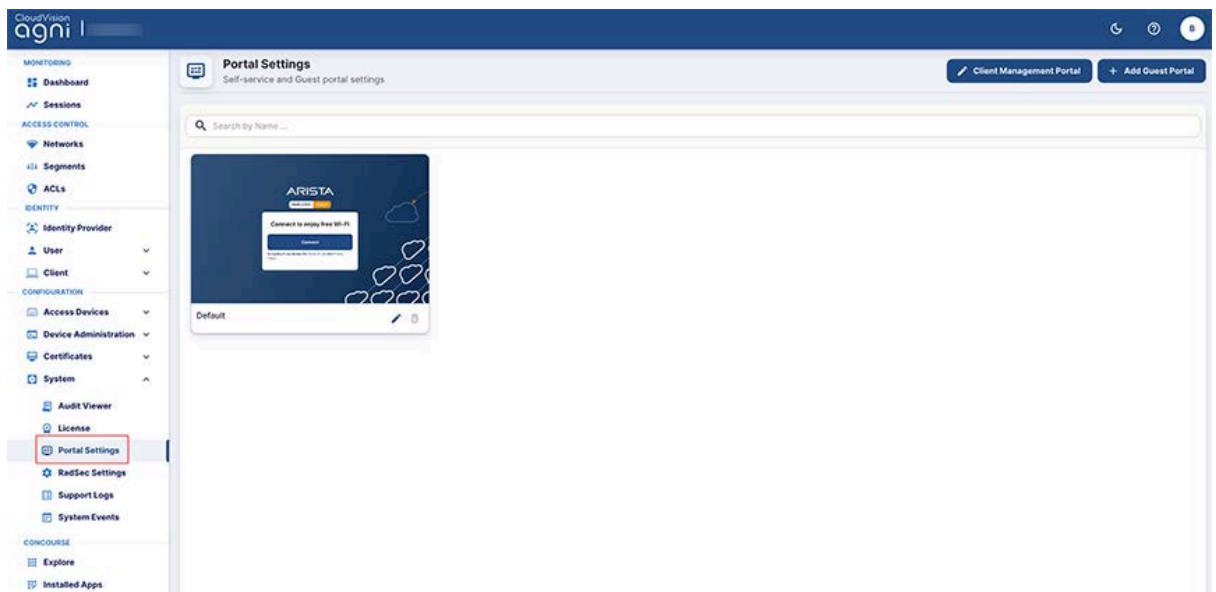
Figure: Captive Portal URL

Configuring Guest Portal in AGNI for Wired Clients

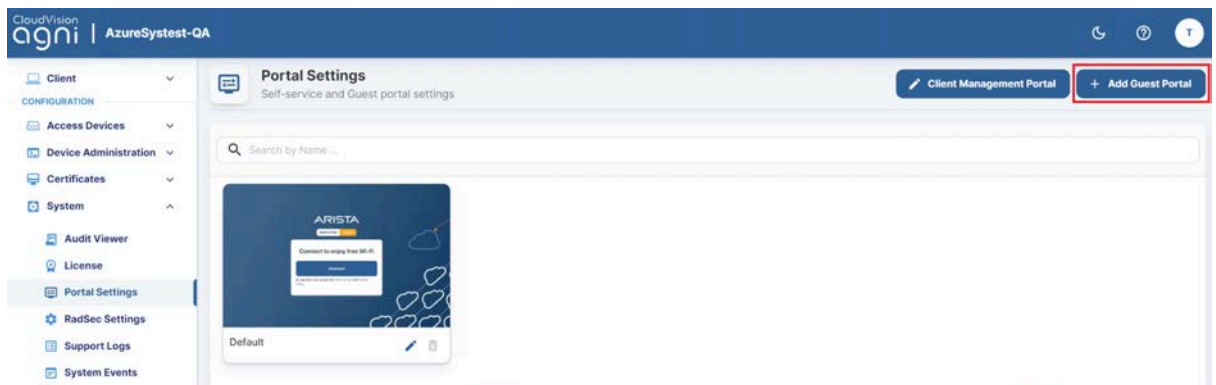
This section describes the steps to configure the guest portal using AGNI for wired clients. To configure the guest portal, you must configure AGNI and the switch.

Configuring AGNI

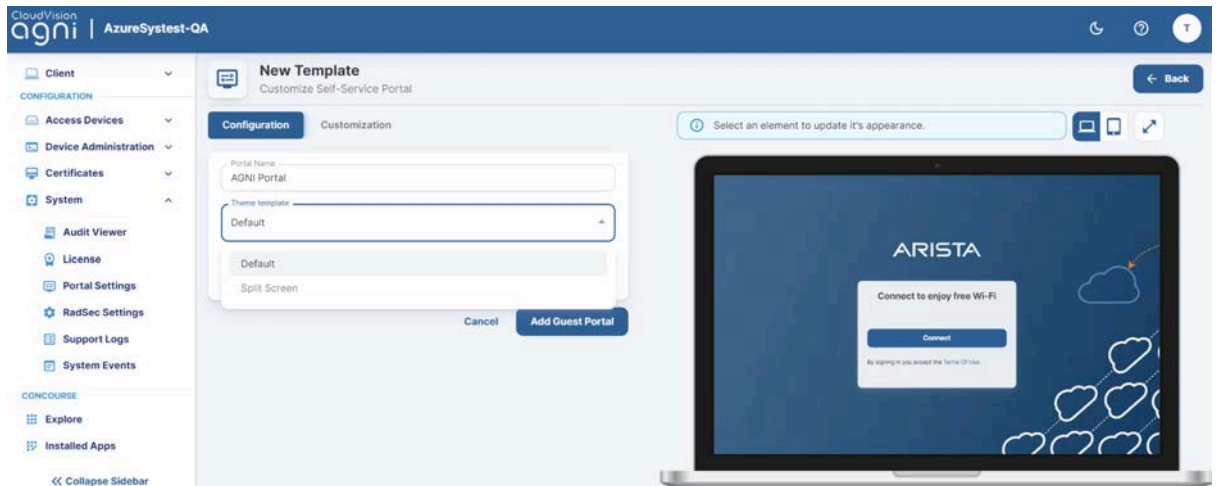
1. Log in to AGNI and navigate to **Configuration > System > Portal Settings**.



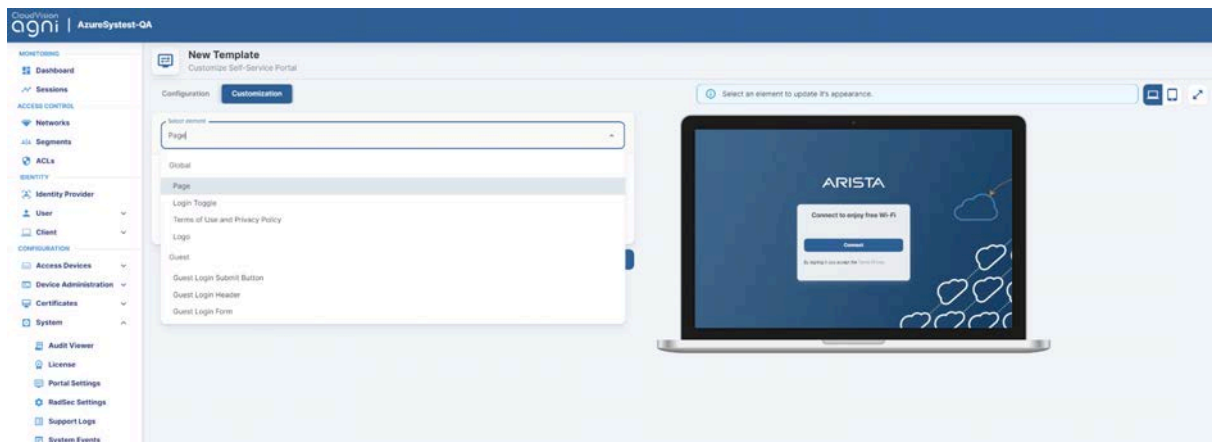
2. Click the **Add Guest Portal** button.



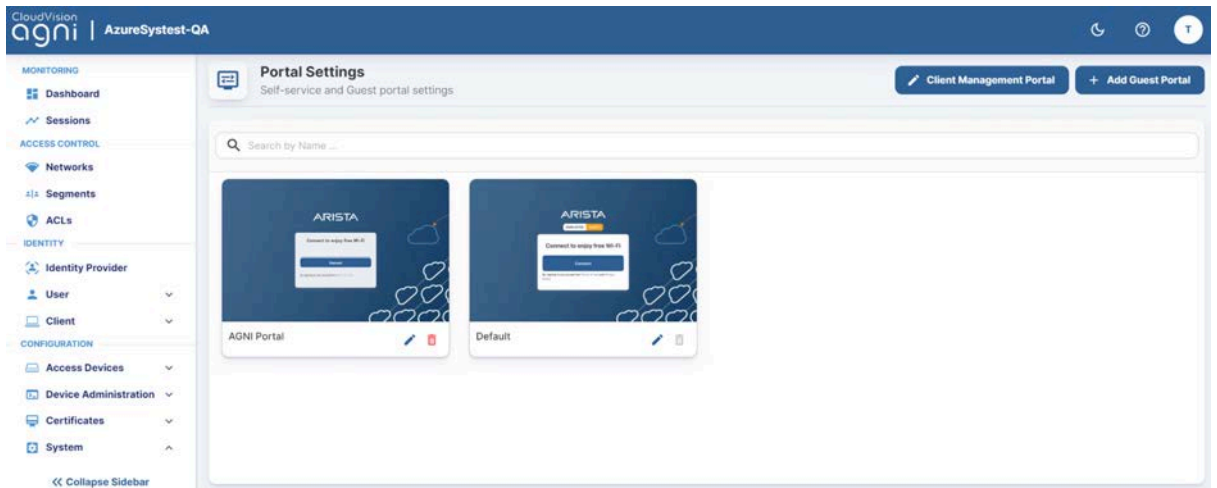
3. In the **Configuration** tab, provide the portal name and select the theme of the portal. The available theme options are **Default** or **Split Screen**.



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



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

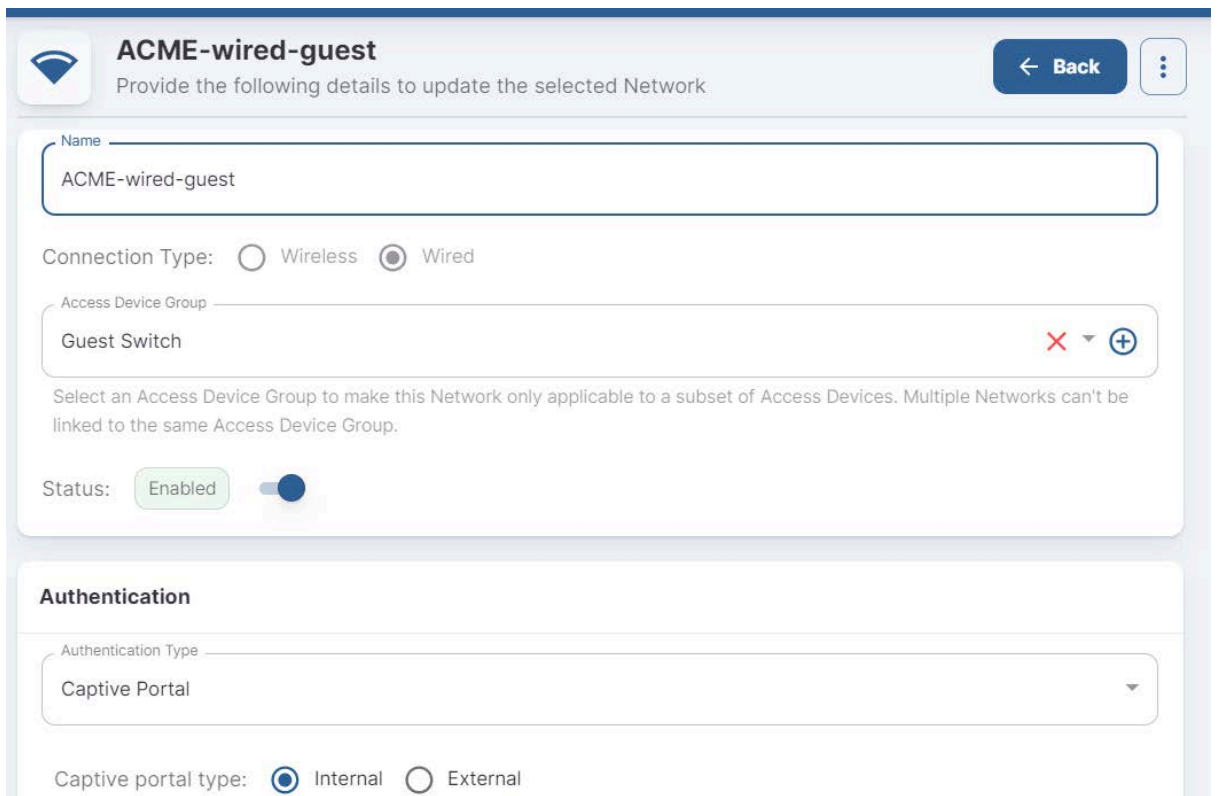


The portal gets listed in the portal listing.

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

Captive portal type: Internal External

Select internal portal: Preview

Captive Portal

Initial ACL For Portal Authentication: Show Domains

Authorized User Groups: ▼

Applicable for organizational users only

Re-Authenticate Clients: ▼

Re-Authentication Period (days):

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.

Copy

Cancel Update Network

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:

The screenshot displays the configuration for the 'ACME Corp Employee Access' segment policy. It includes a name field, a description field, a status indicator (Enabled), and two main sections: 'Conditions' and 'Actions'. The 'Conditions' section contains two rules: 'Network: Name is ACME-CORP' and 'User: Group is Employees'. The 'Actions' section contains one rule: 'Assign VLAN Assign VLAN through RADIUS response' with a dropdown menu set to 'VLAN' and a value of 'ACME-CORP-Access'.

Name
ACME Corp Employee Access

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

Status: Enabled Disable | Monitor

Conditions MATCHES ALL

Network: Name is ACME-CORP

User: Group is Employees

[Add Condition](#)

Actions

Assign VLAN Assign VLAN through RADIUS response

VLAN ACME-CORP-Access

[Add Action](#)

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 Disable | Monitor

Conditions MATCHES ALL

User: Group is Contractors

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

[Add Condition](#)

Actions

Assign VLAN Assign VLAN through RADIUS response

VLAN ACME-CONTR-Access

[Add Action](#)

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 Disable | Monitor

Conditions MATCHES ALL

- Access Device: Location contains Arista Cognitive WiFi/North America/San Jose
- Network: Name is ACME-BYOD
- User: Group in Employees Contractors

[Add Condition](#)

Actions

- Assign VLAN Assign VLAN through RADIUS response
 - VLAN ACME-Internet
- Radius: IETF Radius IETF attributes
 - Filter-Id 13

[Add Action](#)

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 Disable | Monitor

Conditions MATCHES ALL

Network: Name is ACME-IOT ×

Client: Group is IOT Devices ×

[≡+ Add Condition](#)

Actions

Assign VLAN Assign VLAN through RADIUS response ×

VLAN ACME-IOT-Access

[+](#)

[≡+ Add Action](#)

Figure: IOT Access Segment Policy

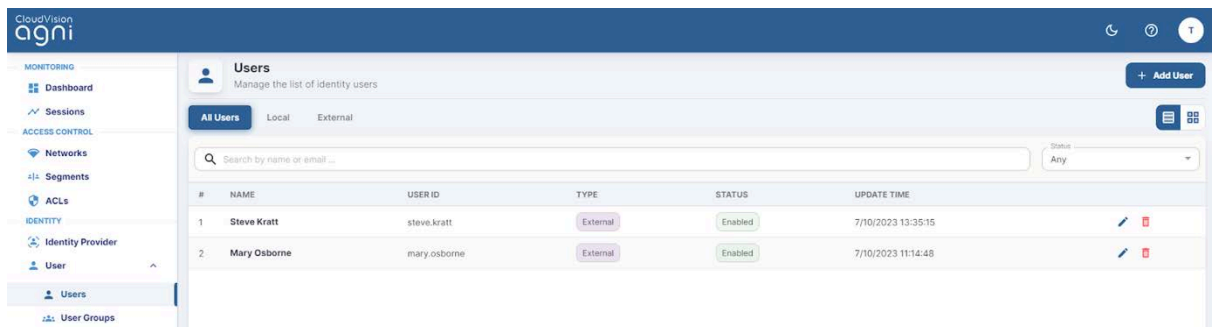
User Configurations

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.



The screenshot shows the AGNI Users management interface. The left sidebar contains navigation options: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), and IDENTITY (Identity Provider, User, User Groups). The main content area is titled 'Users' and includes a search bar, a status filter dropdown set to 'Any', and a table of users. The table has columns for #, NAME, USER ID, TYPE, STATUS, and UPDATE TIME. Two external users are listed: Steve Kratt and Mary Osborne, both with 'Enabled' status and update times from 7/10/2023.

#	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.

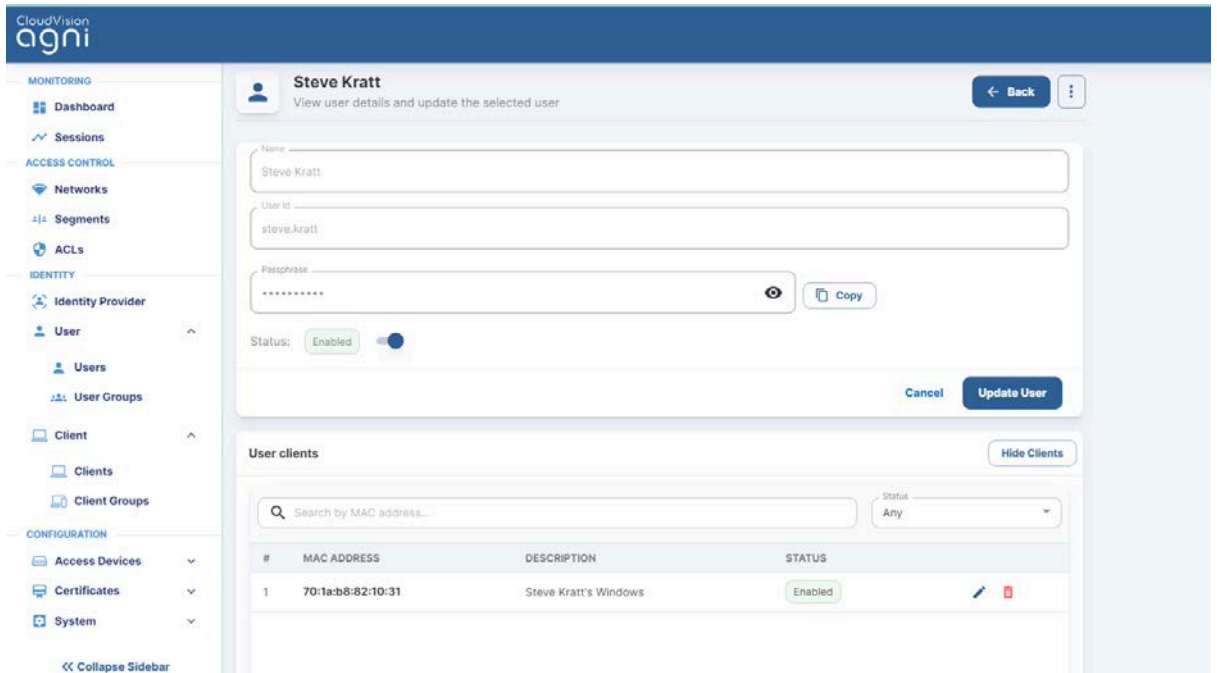


Figure: External User Update

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.

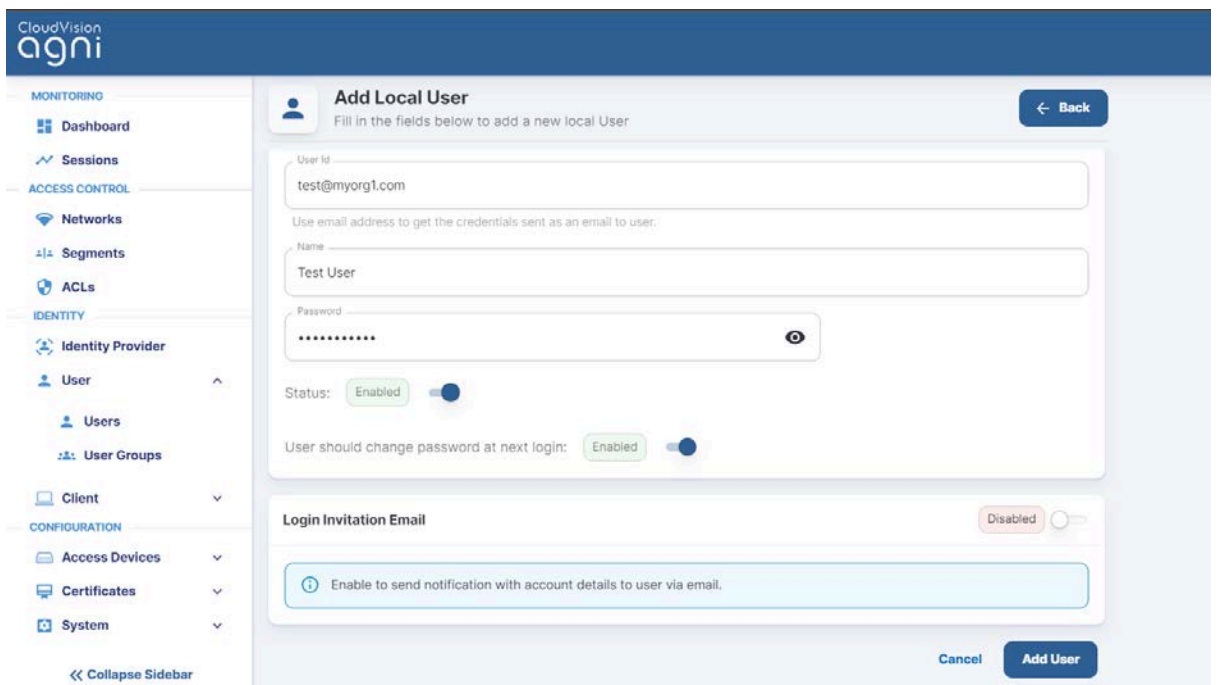


Figure: Local Users Addition

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.

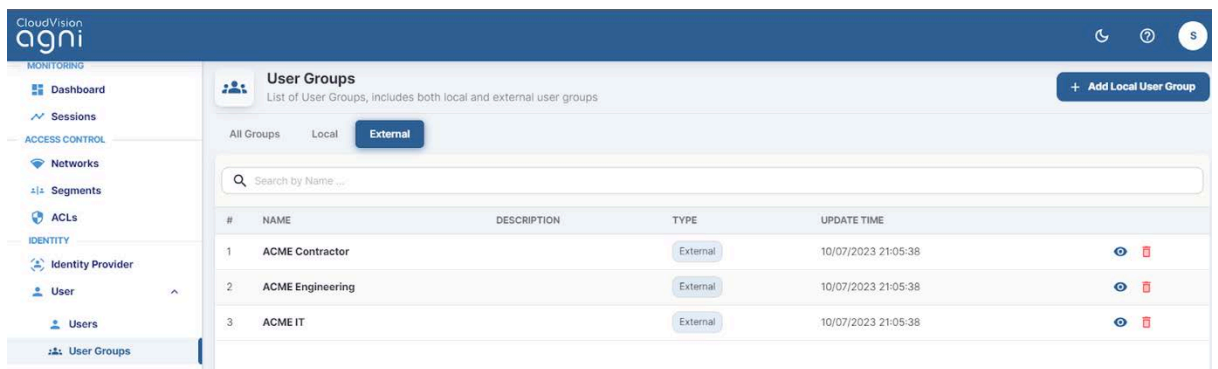


Figure: External User Groups

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.

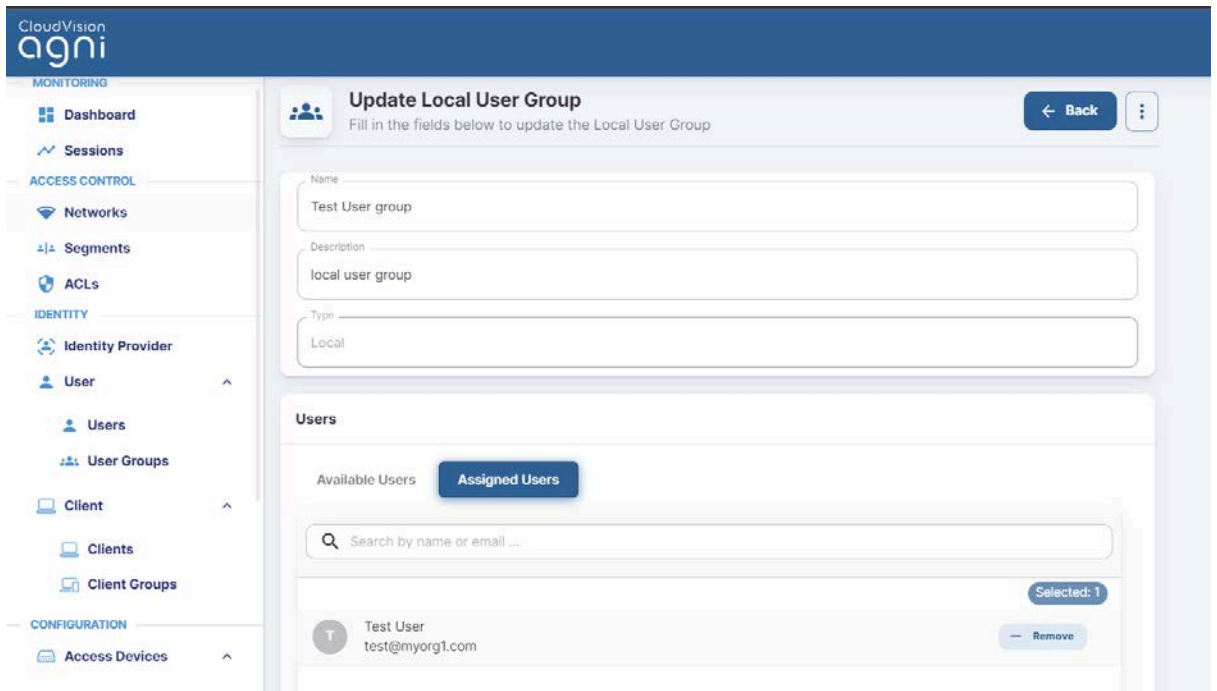


Figure: Local User Groups

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.

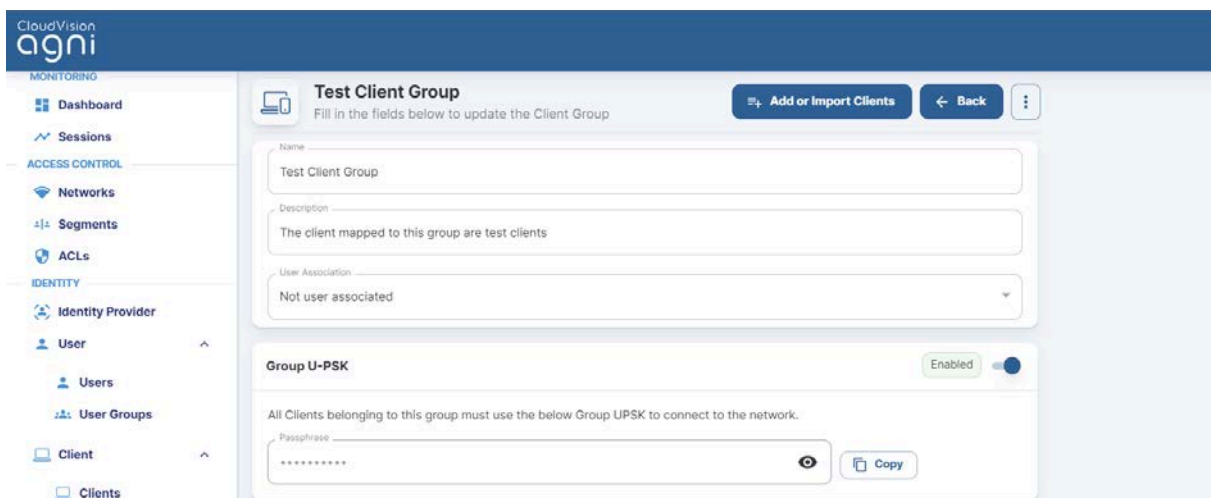


Figure: Client Group UPSK

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

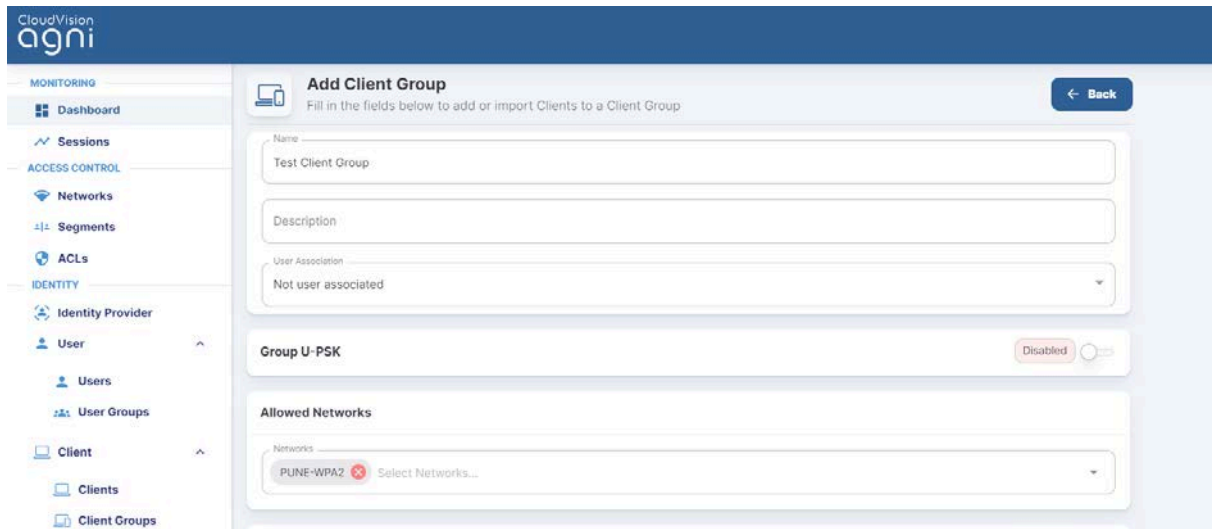


Figure: Client Group Allowed Network

- **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.

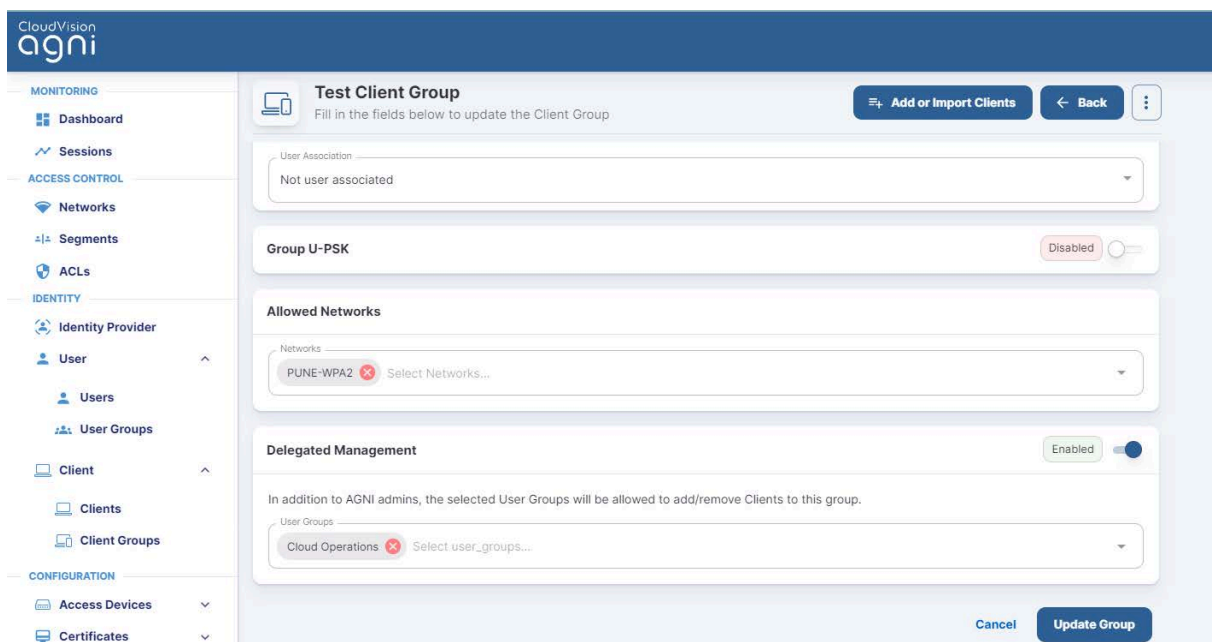


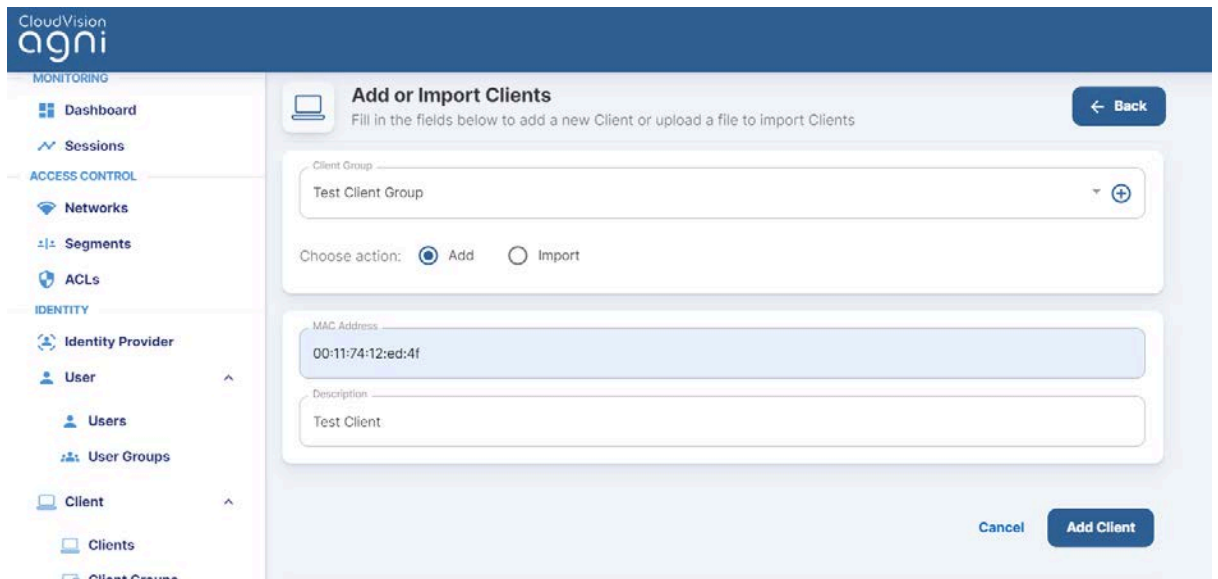
Figure: Client Group Delegated Management

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.



The screenshot displays the 'Add or Import Clients' interface in the CloudVision agni system. The left sidebar contains navigation menus for MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), and IDENTITY (Identity Provider, User, Users, User Groups, Client, Clients, Client Groups). The main content area is titled 'Add or Import Clients' and includes a 'Back' button. Below the title, there is a text prompt: 'Fill in the fields below to add a new Client or upload a file to import Clients'. The form contains the following fields: 'Client Group' (a dropdown menu with 'Test Client Group' selected and a plus icon), 'Choose action:' (radio buttons for 'Add' and 'Import', with 'Add' selected), 'MAC Address' (a text input field containing '00:11:74:12:ed:4f'), and 'Description' (a text input field containing 'Test Client'). At the bottom right, there are 'Cancel' and 'Add Client' buttons.

Figure: Client Addition

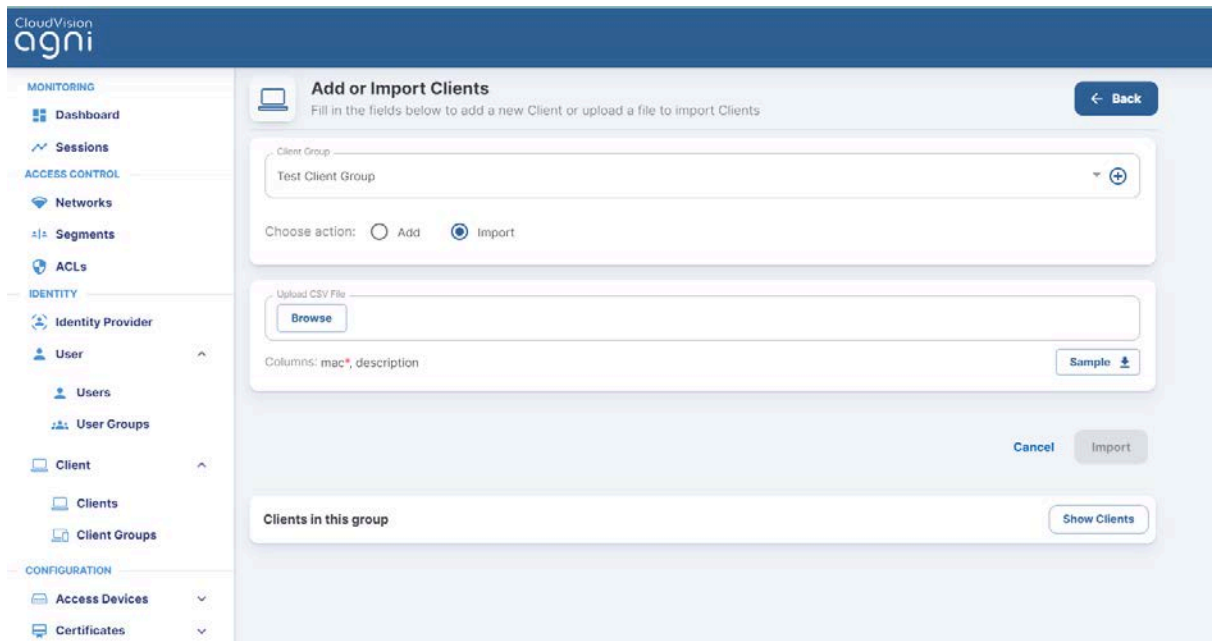


Figure: Client Import

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

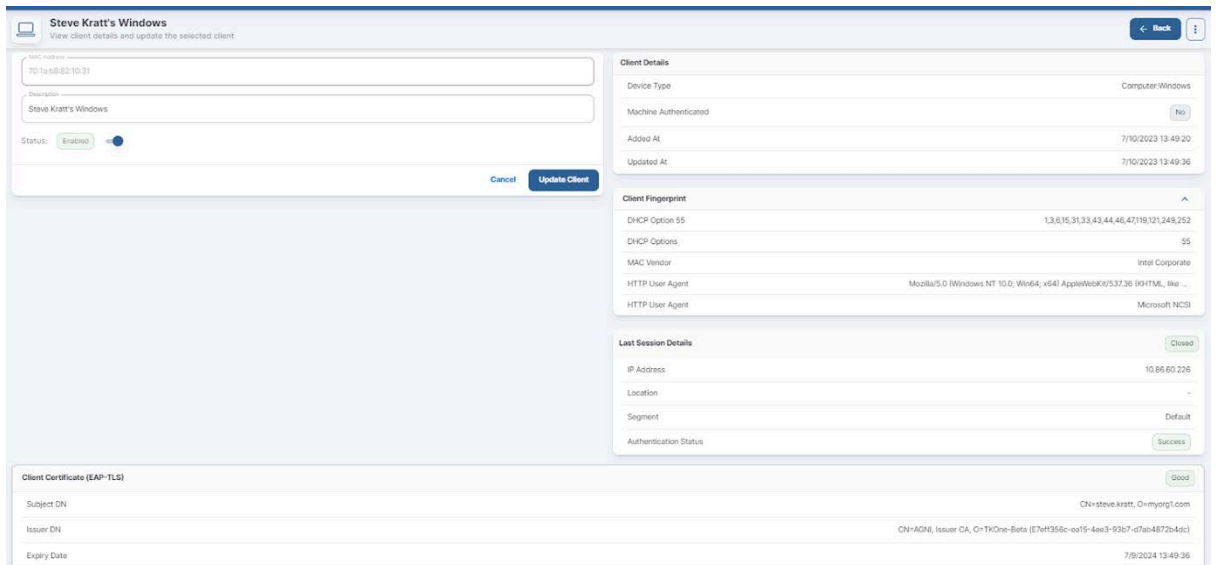


Figure: Client Details

#	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	192.168.114	Success	7/10/2023 11:19:11.704
23	mary.osborne@myorg1.com	Client Certificate	e4:a4:71:26:2a:b4	192.168.114	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

Creating Client Certificates Manually in AGNI

A client certificate refers to an X509 certificate used for EAP-TLS authentication by a client. This certificate can have user details, client device details, or both.

AGNI allows you to manually create individual client certificates to authenticate client devices that are not tied to a user or do not have an interface to help complete the onboard workflow. For example, Linux servers, some IoT devices, etc. that are not tied to any particular user or do not have the support for a web-based onboarding workflow.

Pre-requisite: You must log in as a network administrator to AGNI to create client certificates. You can generate the client certificate only for available clients in AGNI.

Before this release, the network admin could not generate individual client certificates. The only way to generate client certificates was by using AGNI's native onboarding workflow, where the end-user logs into AGNI's Onboard portal and onboards their MacOS/Android/iOS/Windows devices using the client application.

With the 2024.1.0 release, the network admins can

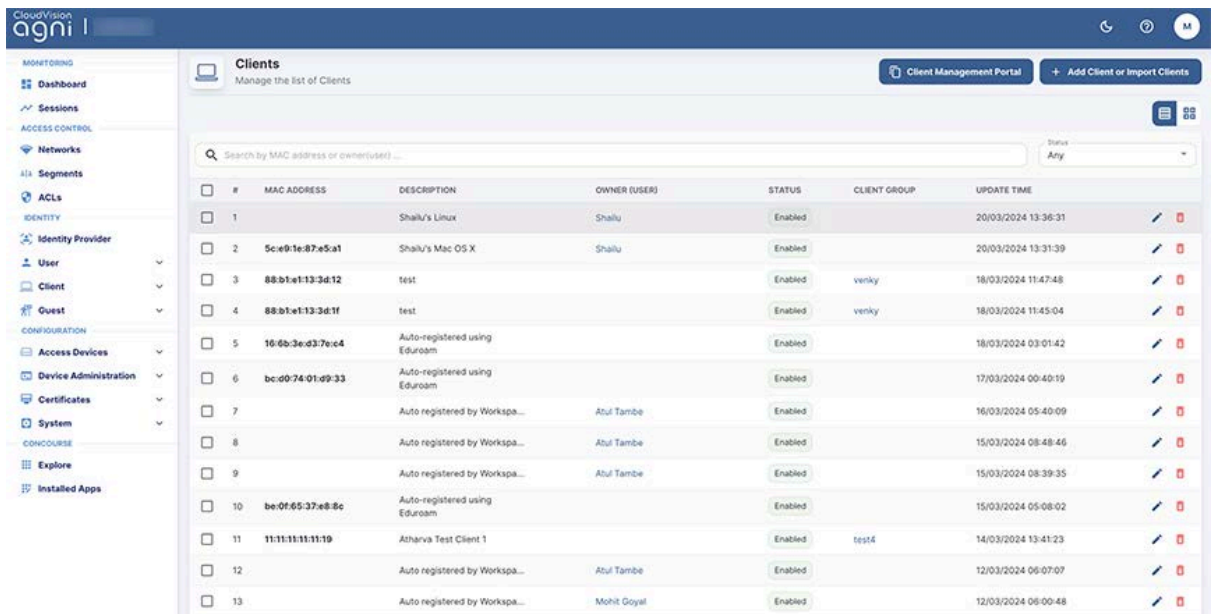
- Manually generate client certificates for each of the client/user devices in AGNI.
- Download the client certificate as a .pem file.
- Download the PFX (.p12) file containing the certificate and private key (if they have not used a CSR). This p12 file is encrypted by providing a password.

The new certificate is valid for one year from the time the certificate is generated.

Note: This client certificate is different from the RadSec client certificate, which is used in access devices such as switches, routers, servers, and so on.

To generate the Client certificate:

- Navigate to **Client > Clients** on AGNI portal (see image below).

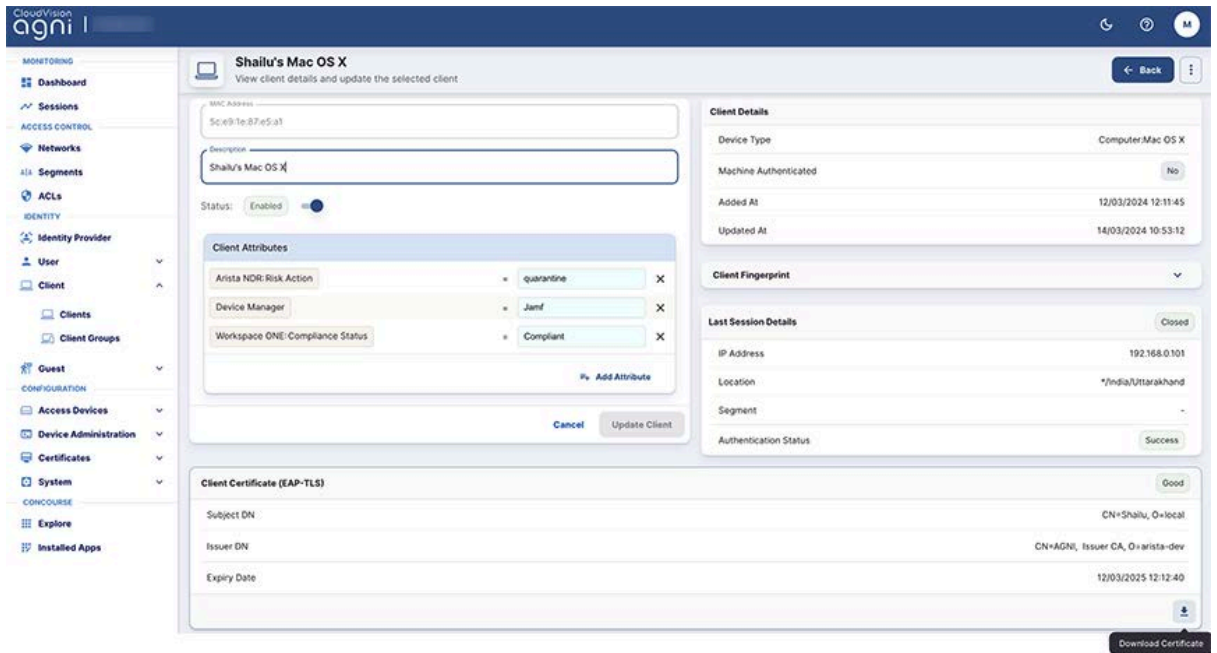


The screenshot shows the 'Clients' management page in the AGNI portal. The page has a sidebar with navigation options like 'Dashboard', 'Sessions', 'Networks', 'Segments', 'ACLs', 'Identity', 'Access Devices', 'Device Administration', 'Certificates', 'System', 'Explore', and 'Installed Apps'. The main content area displays a table of clients with columns for #, MAC ADDRESS, DESCRIPTION, OWNER (USER), STATUS, CLIENT GROUP, and UPDATE TIME. There are also buttons for 'Client Management Portal' and '+ Add Client or Import Clients'.

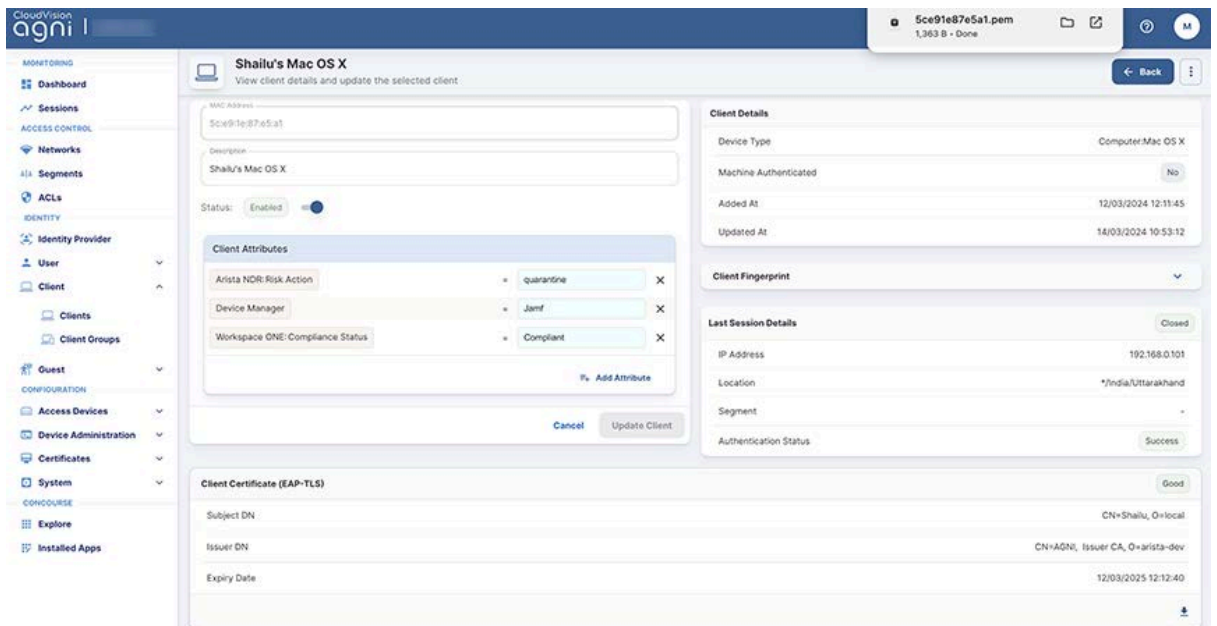
#	MAC ADDRESS	DESCRIPTION	OWNER (USER)	STATUS	CLIENT GROUP	UPDATE TIME
1		Shaili's Linux	Shaili	Enabled		20/03/2024 13:36:31
2	5c:e9:1e:87:e5:a1	Shaili's Mac OS X	Shaili	Enabled		20/03/2024 13:31:39
3	88:b1:e1:13:3d:12	test		Enabled	venky	18/03/2024 11:47:48
4	88:b1:e1:13:3d:1f	test		Enabled	venky	18/03/2024 11:45:04
5	16:6b:3e:d3:7e:c4	Auto-registered using Eduroam		Enabled		18/03/2024 03:01:42
6	bc:d9:74:01:d9:33	Auto-registered using Eduroam		Enabled		17/03/2024 00:40:19
7		Auto registered by Workspa...	Atul Tambe	Enabled		16/03/2024 05:40:09
8		Auto registered by Workspa...	Atul Tambe	Enabled		15/03/2024 08:48:46
9		Auto registered by Workspa...	Atul Tambe	Enabled		15/03/2024 08:39:35
10	be:0f:65:37:e8:8c	Auto-registered using Eduroam		Enabled		15/03/2024 05:08:02
11	11:11:11:11:11:19	Atharva Test Client 1		Enabled	test4	14/03/2024 13:41:23
12		Auto registered by Workspa...	Atul Tambe	Enabled		12/03/2024 06:07:07
13		Auto registered by Workspa...	Mohit Goyal	Enabled		12/03/2024 06:00:48

- Select a client to open the client details page (see image below). This page displays the client certificates of the selected client.

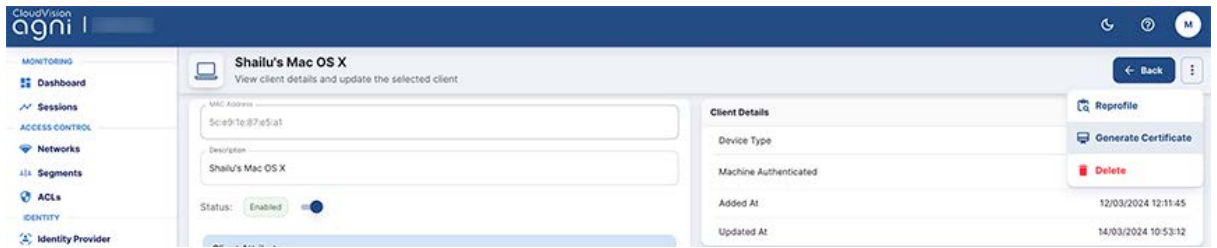
Note: If the client is not present in the client details table, the network admin should add the client before generating the client certificate.



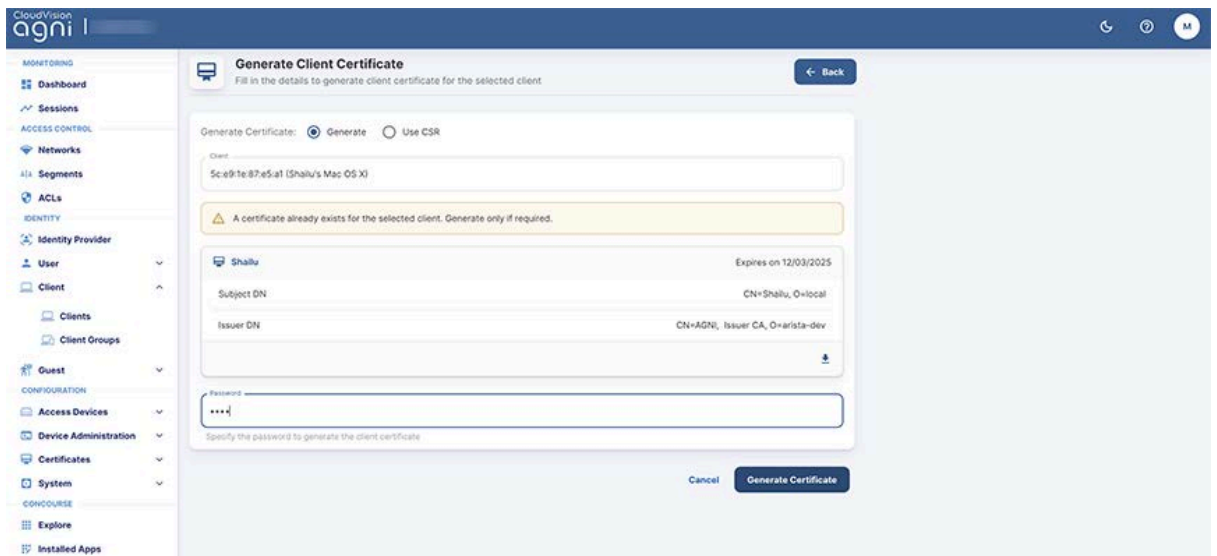
- Download the certificate by clicking the download button (arrow). The X509 certificate (.pem file) is saved to the download folder. You can open the file to verify the details.



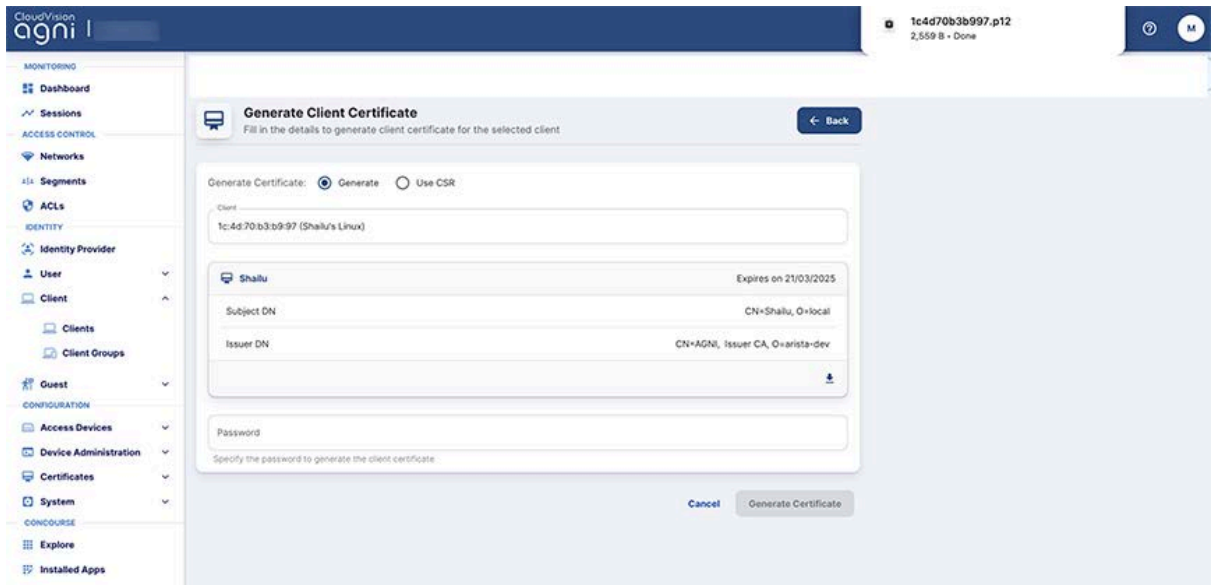
- You can also generate the certificate using the **Generate Certificate** menu (see image below).



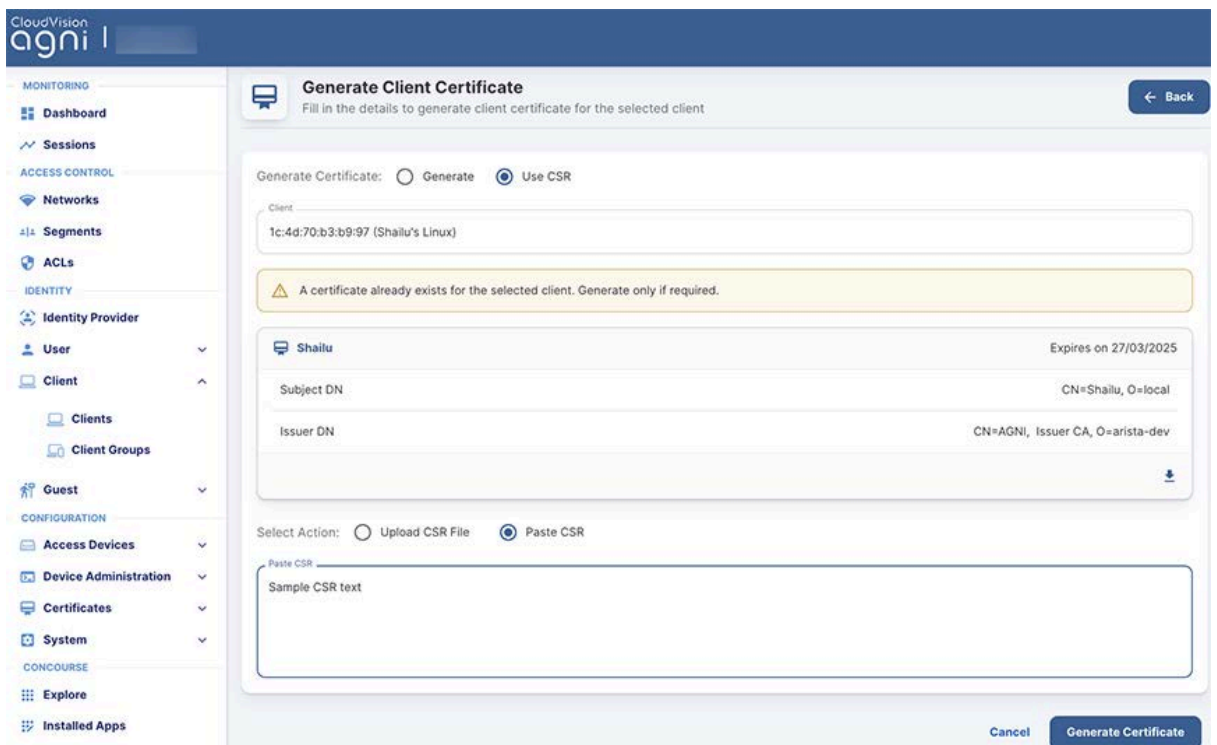
- Click the **Generate Certificate** menu, select the **Generate** radio button, enter a password (save the password for future reference), and click the **Generate Certificate** button (see image below).



The new certificate is downloaded to your system. The updated page displays the new certificate expiry date (one year from the date of generating the certificate). See the image below.



- If you select the **Use CSR** radio button, you can upload the CSR file or paste the contents of the CSR file into the text box, where the CSR file should be a PEM-encoded PKCS10 certificate file. Then click the **Generate Certificate** button.



As described above, AGNI allows you to either directly generate the client certificate or generate the certificate by adding the CSR file details.

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.

The screenshot displays the CloudVision interface for 'Test Org'. The left sidebar contains navigation menus for MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Certificates, Trusted, System), and CONCOURSE (License, Portal Settings, RadSec Settings, Support Logs, System Events). The main content area is titled 'Audit Viewer' and shows a list of audit records. A search bar is available with the placeholder 'Search by Name or User ...'. The records are as follows:

#	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
Details					
Name	Description	Group U-PSK	Allowed Networks		
Mac auth clients		Disabled → Enabled	All Networks		
2	ACME-CORP	Network	Update	bobby.flay@testorg1.com	7/24/2023 11:22:11
Details					
Name	Connection Type	SSID	Authentication Type		
ACME-CORP	Wireless	ACME-Corp	Client Certificate		
Trust External Certificates	Onboarding	Status			
Enabled	Enabled	Enabled			
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

Figure: Audit Viewer

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

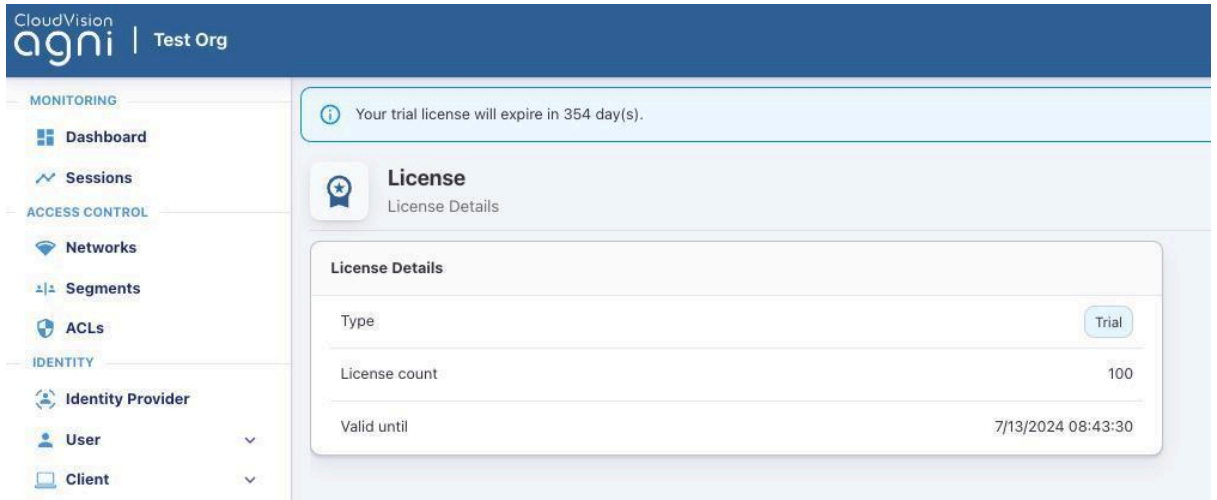


Figure: License

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.

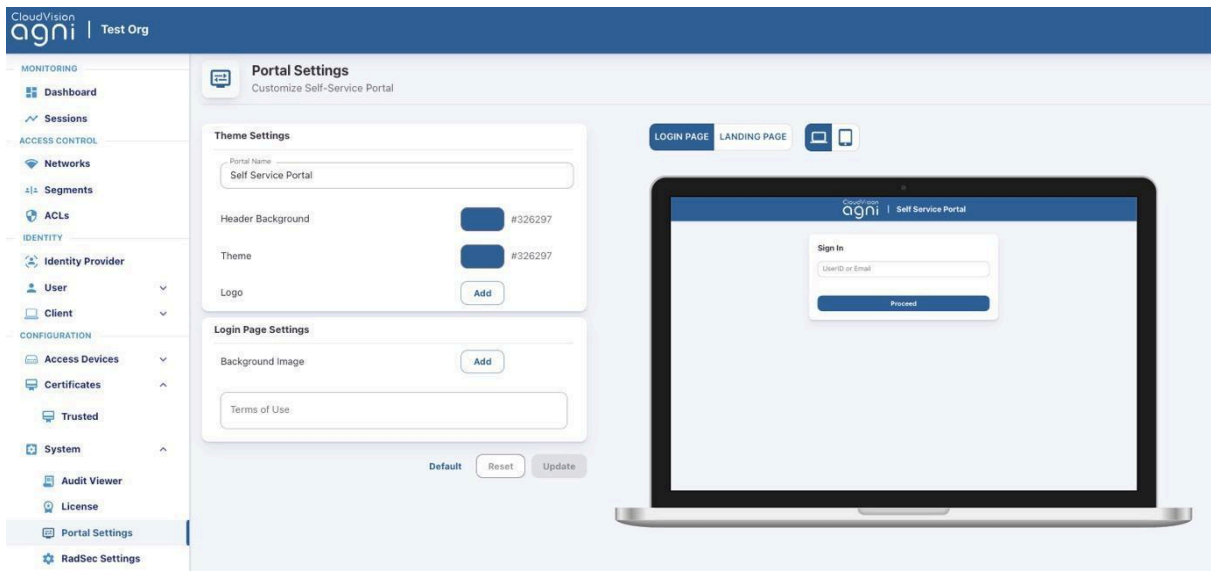


Figure: Portal Settings

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.

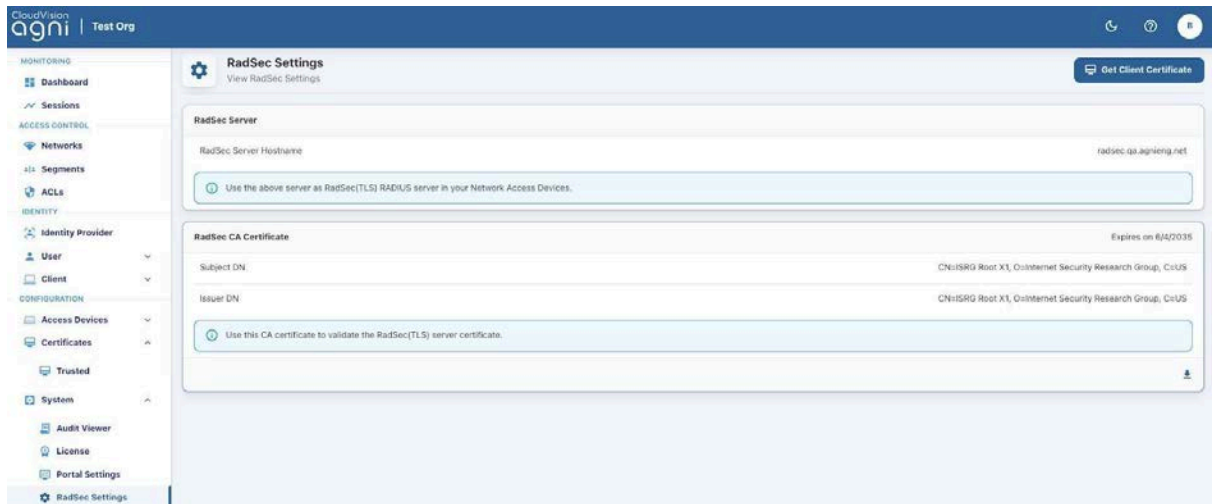


Figure: RadSec Settings

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.

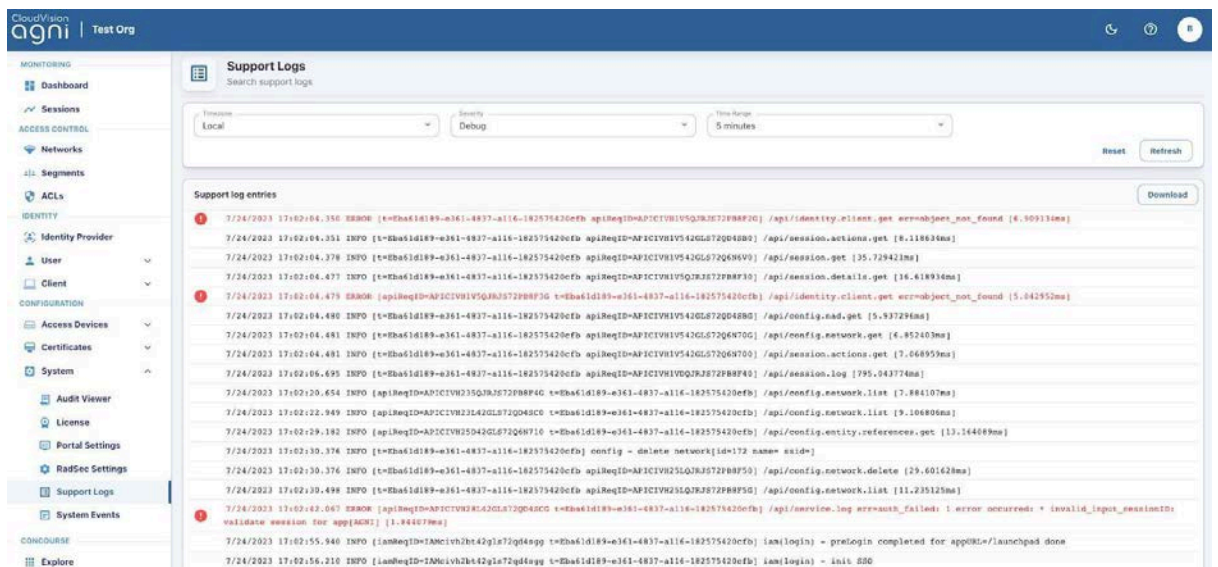
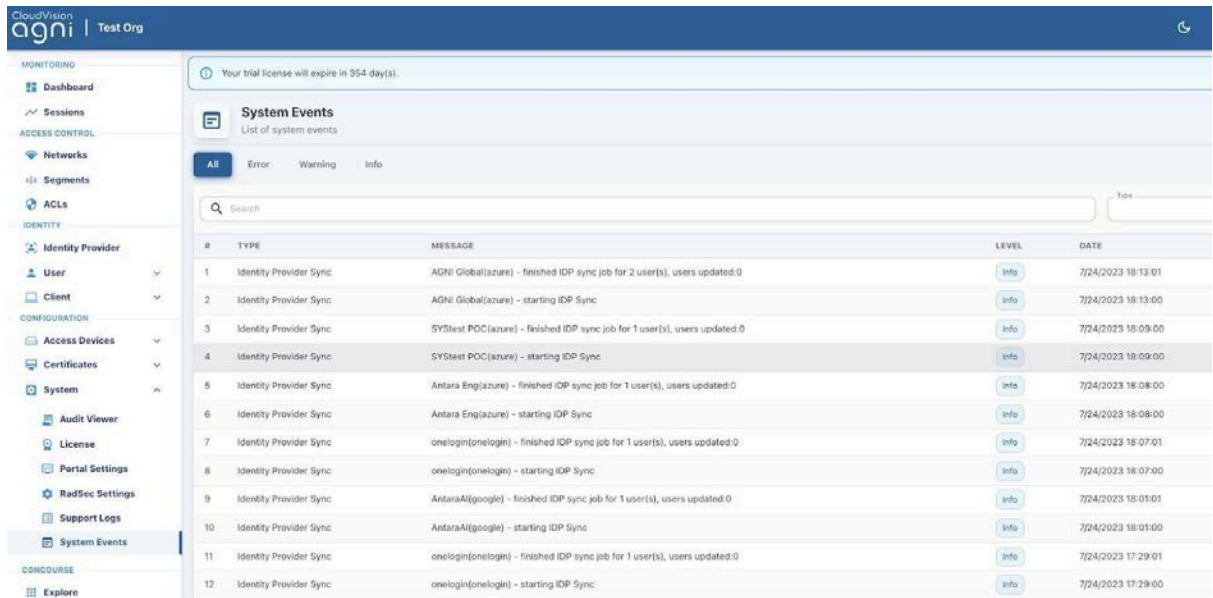


Figure: Support Logs

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.



CloudVision agni | Test Org

Your trial license will expire in 554 day(s).

System Events

List of system events

All Error Warning Info

Search: Type:

#	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	Antara AI(google) - finished IDP sync job for 1 user(s), users updated:0	Info	7/24/2023 18:01:01
10	Identity Provider Sync	Antara AI(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)

CloudVision agni I

MONITORING Dashboard Sessions

ACCESS-CONTROL Networks Segments ACLs

IDENTITY Identity Provider User Client

CONFIGURATION Access Devices Device Administration Certificates System

CONCOURSE Explore Installed Apps

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

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

#	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 14:07:37148
2	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success	08/12/2023 13:54:16193
3	Home-IOTs	MAC Authentication	00:11:09:5e:3d:44	10.201.110.50	Success	08/12/2023 13:48:42317
4	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success	08/12/2023 13:07:37065
5	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success	08/12/2023 12:54:16075
6	Home-IOTs	MAC Authentication	00:11:09:5e:3d:44	10.201.110.50	Success	08/12/2023 12:48:42236
7	CAMERA_GROUP	MAC Authentication	f8:e4:3b:c0:0c:1d	192.168.1.12	Success	08/12/2023 12:32:24121
8	CAMERA_GROUP	MAC Authentication	f8:e4:3b:c0:0c:1d		Success	08/12/2023 12:31:47824
9	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success	08/12/2023 12:07:36985
10	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success	08/12/2023 11:54:15993
11	Polycm Phones	MAC Authentication	f8:e4:3b:c0:0c:1d	192.168.1.12	Success	08/12/2023 11:50:47419
12	Home-IOTs	MAC Authentication	00:11:09:5e:3d:44	10.201.110.50	Success	08/12/2023 11:48:42102

CloudVision agni I

MONITORING Dashboard Sessions

ACCESS-CONTROL Networks Segments ACLs

IDENTITY Identity Provider User Client

CONFIGURATION Access Devices Device Administration Certificates System

CONCOURSE Explore Installed Apps

Session Details - Rclpdk84n37c72vis7v0
Details for Session

Disconnect Back

Authentication Request: Success

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

Session Details: Open
Client IP Address: 10.10.30.2
Session Start Time: 08/12/2023 14:07:37148
Session Stop Time: -

User: Not available

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

Access Device: Arista Switch
ac:35:94:c8:27:9c
agni-722xpm-48
AT-WIRED-EAP

Network: Enabled
AT-WIRED-EAP
Wired
MAC Authentication

Actions: Allow Access

Input Request Attributes Output Response Attributes

Session logs for request: Rclpdk84n37c72vis7v0 Show Logs

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

Network Access Device Administration

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

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	lsha@yystestpoc.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	lsha@yystestpoc.onmicrosoft.com	Client Certificate	30:bb:7d:4b:0f:4d	192.168.1.11	Success	11/23/2023 22:29:39.358
6	lsha@yystestpoc.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 - Rcl3g0g4n37c72strtv0
Details for Session

Disconnect 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 12:02:34.321

Session Stop Time: -

User Enabled

lsha@yystestpoc.onmicrosoft.com
lsha

Client Enabled

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

Access Device Arista WiFi

v4-df:24:10:0b:c7
Tarun_Arista_w318_30:0B:CF

Network Enabled

Carbera
Carbera
Client Certificate (EAP-TLS)

Actions

Allow Access

Input Request Attributes Output Response Attributes

Session logs for request: Rcl3g0g4n37c72strtv0 Show Logs

3. Click the **Disconnect** button.

Session Details - Rcl3g0g4n37c72strtv0
Details for Session

Disconnect 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 12:02:34.321

Session Stop Time: -

User Enabled

lsha@yystestpoc.onmicrosoft.com
lsha

Client Enabled

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

Access Device Arista WiFi

v4-df:24:10:0b:c7
Tarun_Arista_w318_30:0B:CF

Network Enabled

Carbera
Carbera
Client Certificate (EAP-TLS)

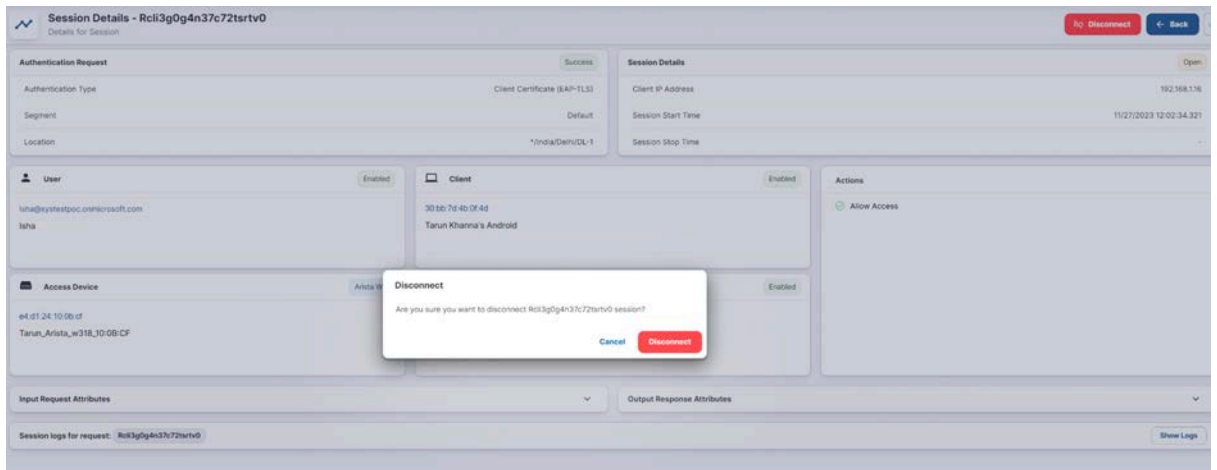
Actions

Allow Access

Input Request Attributes Output Response Attributes

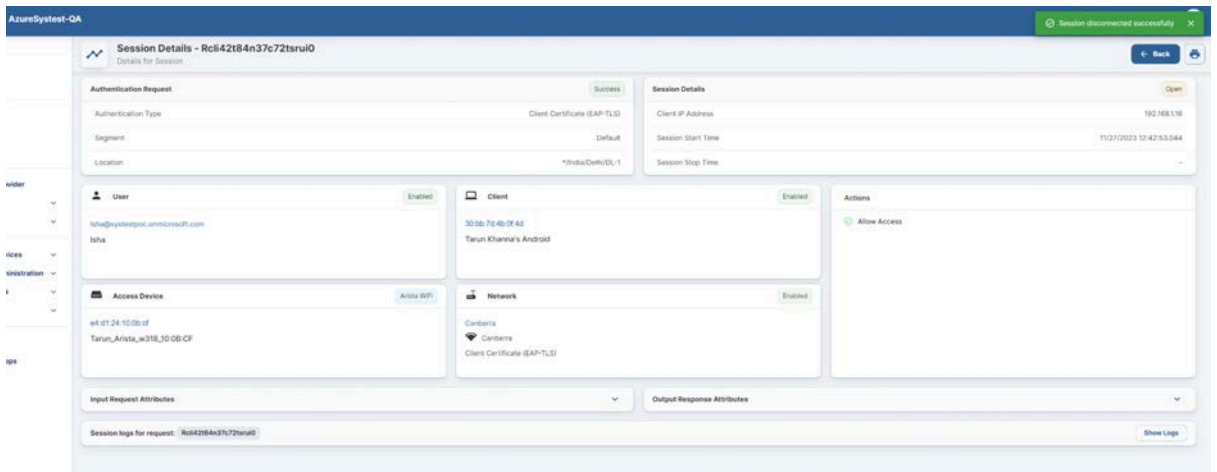
Session logs for request: Rcl3g0g4n37c72strtv0 Show Logs

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

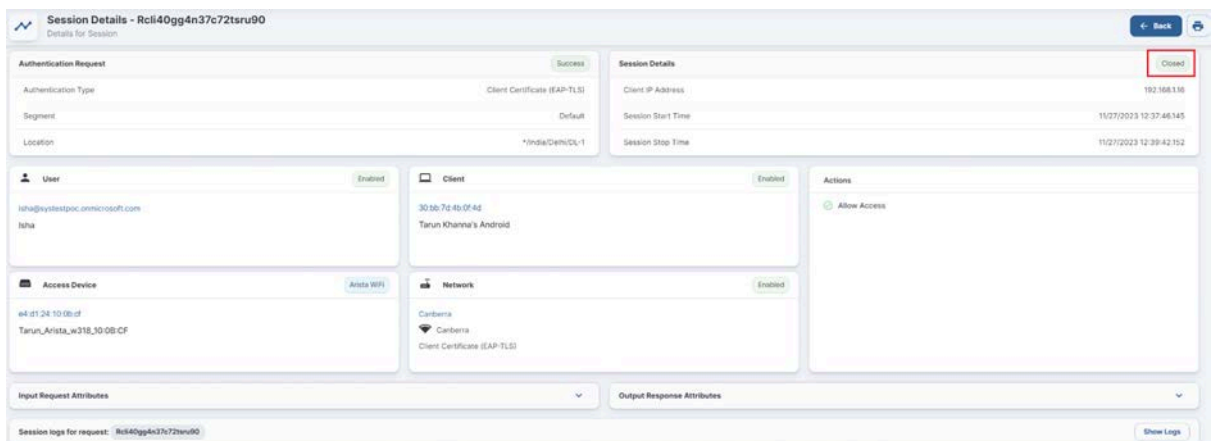


4. Click **Approve**.

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



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



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


```

Session logs for request: Rct3v84c3z72turvg
Download Hide Logs

@DisconnectFrom, terminateCause=, attr=Radius:ITP:NAS-IP-Address=192.168.1.2, Radius:ITP:NAS-Identifer=64-01-24-10-80-CF-Caberra) attempting CoA

11/27/2023 12:37:39.248 INFO [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] multiSessionID=380076400F4d1701068765] radius[acct] - acct-request[stop] code=accounting-Request attr=[Radius:ITP:Acct-Status-Type=, Radius:ITP:Acct-Authentic=, Radius:ITP:User-Name=sha, Radius:ITP:NAS-IP-Address=192.168.1.2, Radius:ITP:NAS-Identifer=64-01-24-10-80-CF-Caberra, Radius:ITP:Called-Station-Id=64-01-24-10-80-CF-Caberra, Radius:ITP:NAS-Port-Type=, Radius:ITP:Service-Type=, Radius:ITP:NAS-Port=, Radius:ITP:Calling-Station-Id=38-70-48-8f-4d, Radius:ITP:Connect-Info=CONNECT, 540bps, 802.11a, Radius:ITP:Acct-Session-Id=380076400F4d1701068765, Radius:ITP:HLAB-Profile-Cipher=1827876, Radius:ITP:HLAB-Group-Cipher=1827876, Radius:ITP:HLAB-Auth-Suite=1827876, Radius:ITP:Acct-Multi-Session-Id=380076400F4d1701068765, Radius:ITP:Class=113-184-937c721a-vg, Radius:ITP:Event-TimeStamp=2023-11-27 07:07:39 +0000 UTC, Radius:ITP:Acct-Delay-Time=, Radius:ITP:Acct-Session-Time=93, Radius:ITP:Acct-Input-Packets=92, Radius:ITP:Acct-Output-Packets=185, Radius:ITP:Acct-Input-Octets=18848, Radius:ITP:Acct-Input-Digets=18848, Radius:ITP:Acct-Output-Octets=18858, Radius:ITP:Acct-Output-Digets=18858, Radius:ITP:Frame-IPV4-Address=192.168.1.194, Radius:ITP:Frame-IPV4-Address=192.168.1.18, Radius:ITP:Acct-TermState-Cause=]

11/27/2023 12:37:39.257 INFO [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] multiSessionID=380076400F4d1701068765] radius[acct] - enqueue ClientDisconnectEvent[mac=380076400F4d ip=192.168.1.16]

11/27/2023 12:37:39.257 INFO [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] multiSessionID=380076400F4d1701068765] radius[acct] - db update acct[stop] mac=380076400F4d, acctSessionID=380076400F4d1701068765] acct[stop] multiSessionID=380076400F4d1701068765] in 7.56588ms

11/27/2023 12:37:39.257 INFO [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] multiSessionID=380076400F4d1701068765] radius[acct] - session completed in 7.81338ms

11/27/2023 12:37:39.259 DEBUG [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] eventProcessor(ClientDisconnect) - consumerGroup[concurrentEventProducer] ev disconnect[{"orgID":"666419ed-62c2-482d-871b-fa79a34837c","authMethod":"Radius:ITP:NAS-IP-Address=192.168.1.2","ip":"192.168.1.16"}] @ 2023-11-27 07:07:39 +0000 UTC processed in 2.43794ms

11/27/2023 12:37:39.260 DEBUG [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] eventProcessor(ClientDisconnect) - consumerGroup[ClientStateProducer] ev disconnect[{"orgID":"666419ed-62c2-482d-871b-fa79a34837c","authMethod":"Radius:ITP:NAS-IP-Address=192.168.1.2","ip":"192.168.1.16"}] @ 2023-11-27 07:07:39 +0000 UTC processed in 3.46088ms

11/27/2023 12:37:39.328 INFO [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] radius[coa] - added activity record for mac=380076400F4d in 2.82227ms

11/27/2023 12:37:39.328 INFO [v4d64a19ed-62c2-482d-871b-fa79a34837c] [v4d64a19ed-62c2-482d-871b-fa79a34837c] radius[coa] - user[orgID=666419ed-62c2-482d-871b-fa79a34837c, callingStation=38-70-48-8f-4d, mac=380076400F4d, ip=192.168.1.16] @ 2023-11-27 07:07:39 +0000 UTC processed in 1.84133ms
@DisconnectFrom, terminateCause=, attr=Radius:ITP:NAS-IP-Address=192.168.1.2, Radius:ITP:NAS-Identifer=64-01-24-10-80-CF-Caberra) completed in 14.133ms

```

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

The screenshot shows the 'Client Details - Auto registered with UPSK' interface. Under the 'Client Activity' section, there is a table with the following data:

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

The 'Details' section for the first activity shows the 'Access Device' as 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**

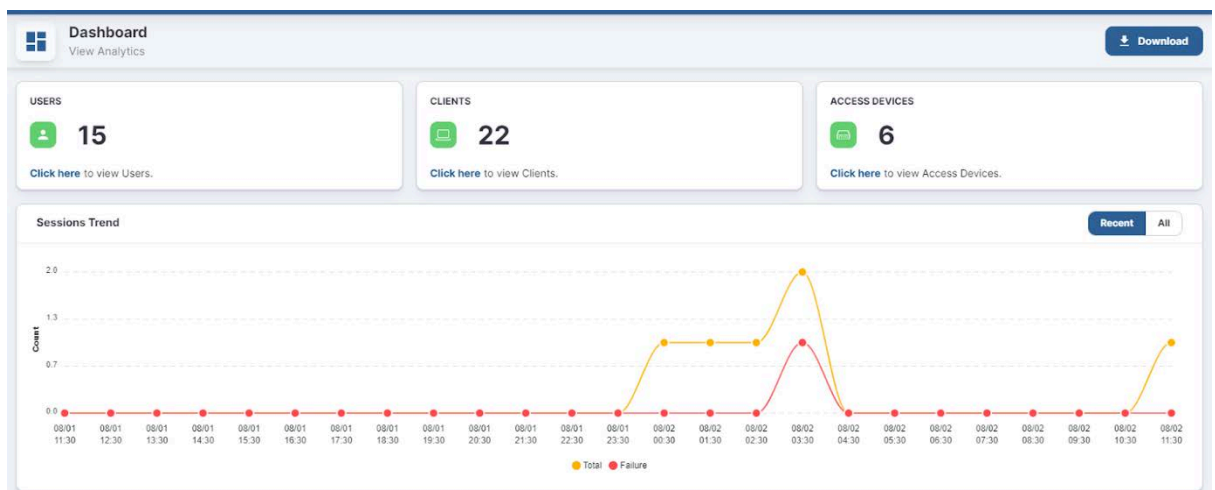


Figure: AGNI Dashboard and Session Trend

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.

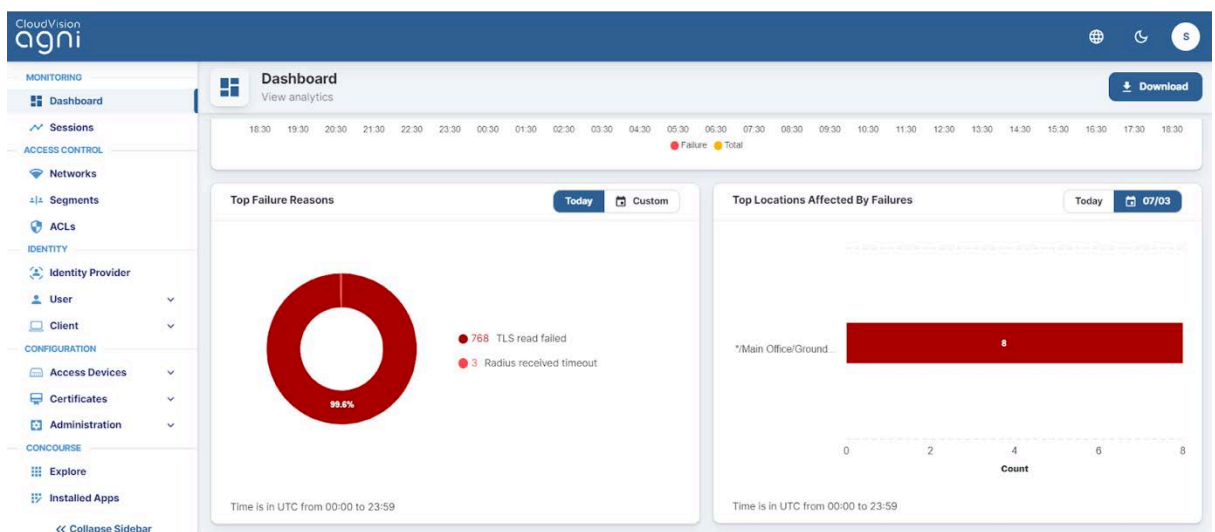


Figure: AGNI Dashboard and charts

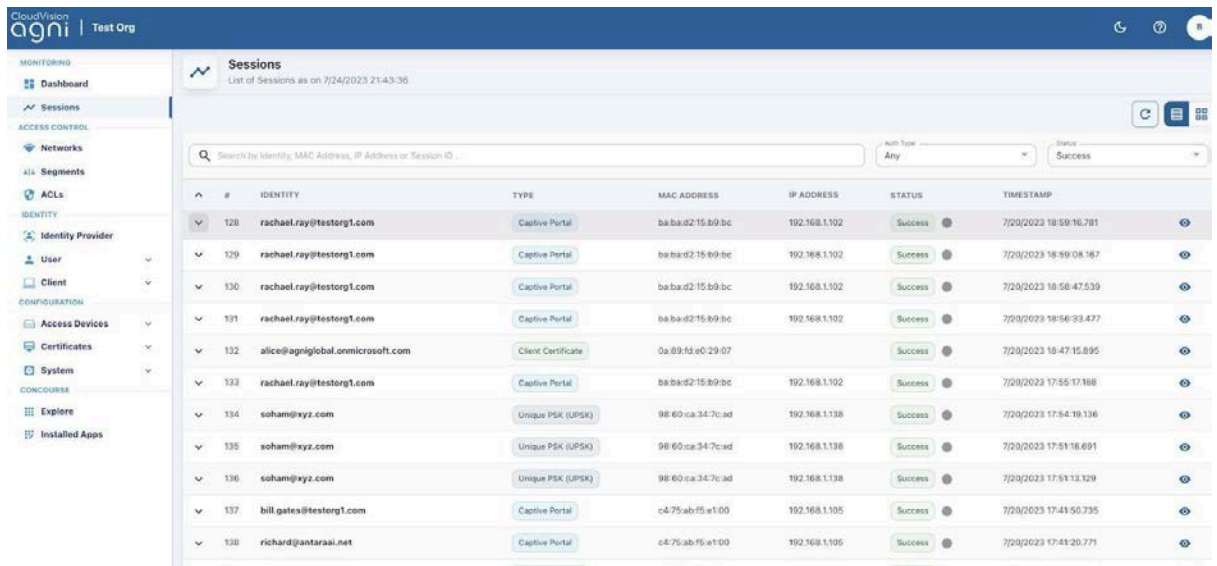
Sessions

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**.



#	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	Cleix Certificate	0a:89:a5: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 17:54:18.136
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.

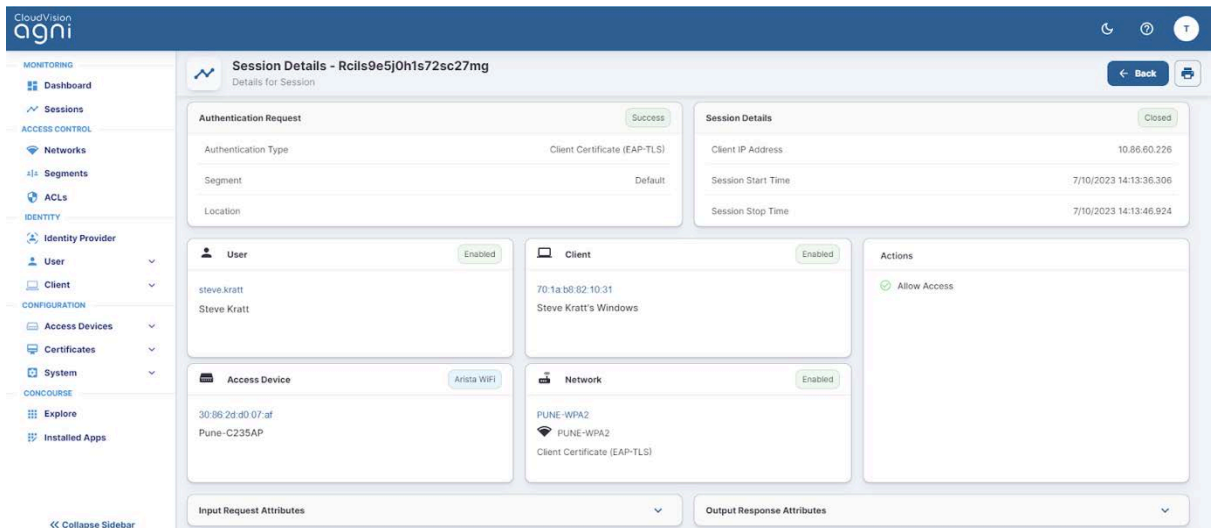


Figure: Session Details page-1

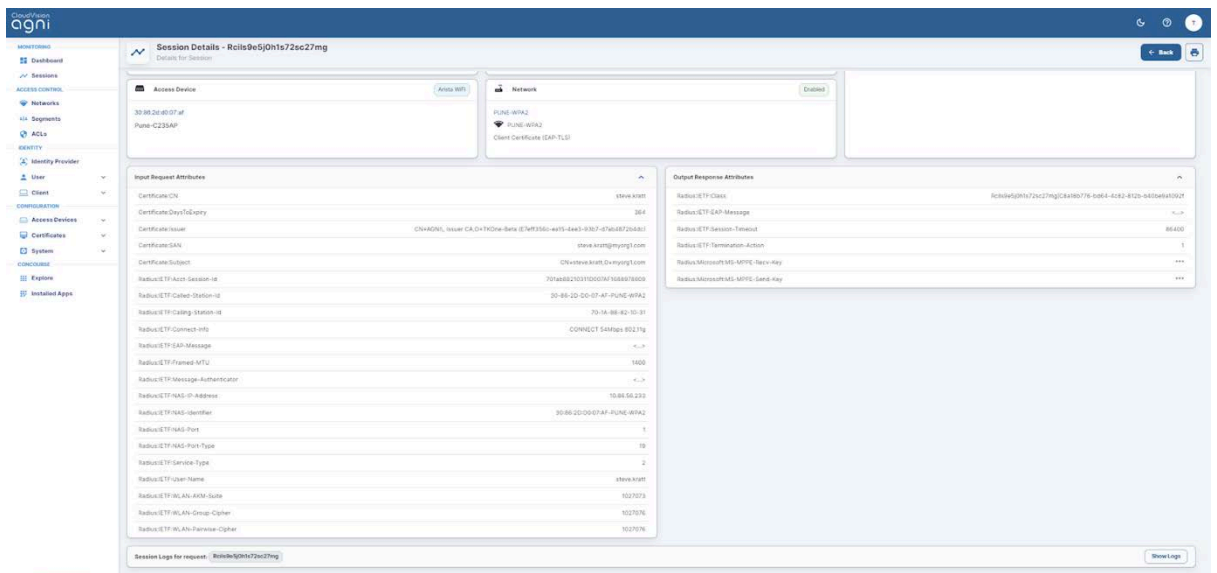


Figure: Session Details page-2

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.

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.

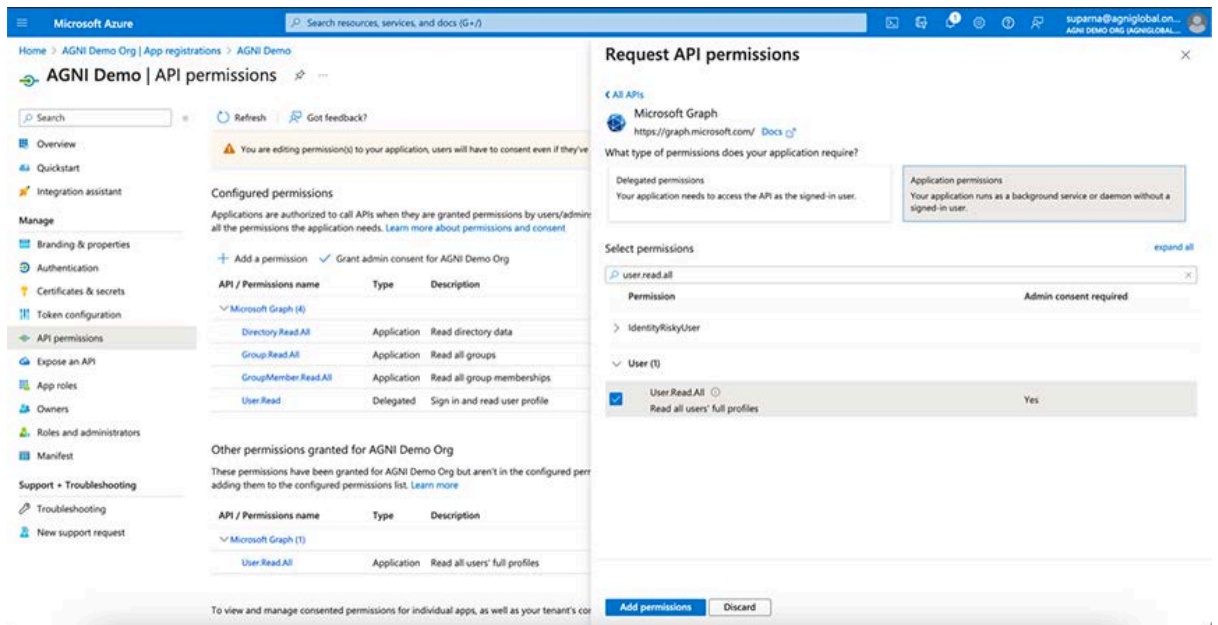


Figure: API Permissions

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