



Arista Guardian for Network Identity (AGNI) User Guide

Arista Networks

www.arista.com

*Arista AGNI Version 2024.4.0
DOC-06557-04*

Table of Contents

Introduction.....	6
Accessing the User Interface (UI).....	6
Viewing Licensing Details.....	8
User Interface (UI) Theme.....	8
Integrating with Concourse Applications (Internal).....	9
Arista CV-CUE Integration.....	9
Arista CloudVision Integration.....	11
Configuring CVaas Instances.....	12
Adding Multiple CVaaS Instances in AGNI.....	15
Arista NDR Integration.....	15
Configuring Arista NDR.....	17
Configuring Segment Policies.....	20
Using Risk Action in Segment Policies.....	23
Integrating with Concourse Applications (External).....	24
Palo Alto Cortex XDR Integration.....	24
Palo Alto Firewall Integration.....	25
Configuring the Palo Alto Firewall/Panorama.....	26
Palo Alto Firewall Configuration.....	26
Medigate Integration.....	28
Microsoft Intune Integration.....	30
Jamf Integration.....	31
ServiceNow CMDB Integration.....	31
Splunk Integration.....	33
Sumo Logic Integration.....	34
CrowdStrike Integration.....	35
Workspace ONE integration.....	36
Configuring Identity Providers (IDPs).....	39
Microsoft Entra ID 365 (Azure).....	39
OneLogin.....	42
Okta.....	44
Google Workspace.....	46
Local.....	48
Configuring the Networks.....	48
Configuring Client Certificate Network.....	48
Configuration Steps.....	49
Authenticating Users with Email Codes (as against IDP).....	52
Wireless Configuration on Devices.....	55
iPhone Configuration.....	56
MacBook Configuration.....	58
Android Configuration.....	60
Windows Configuration.....	63

Chromebook Configuration.....	65
Configuring Unique PSK (UPSK) Network.....	69
Configuring the UPSK Settings.....	69
Configuring the Device Count Limit for Authentication.....	71
Configuring Wireless Captive Portal Network.....	73
Configuration Steps.....	74
Configuring Wireless MAC Authentication Network.....	76
Configuration Steps.....	76
Configuring Wired 802.1X Network.....	77
Configuration Steps.....	78
Configuring Wired MAC Authentication Network.....	81
Configuration Steps.....	81
Configuring Wired Captive Portal Network.....	83
Configuration Steps.....	84
Configuring Guest Portal Network.....	85
Configuring AGNI.....	85
Configuring EOS.....	89
Configuring Segmentation Policies.....	89
Status.....	89
Conditions.....	90
Actions.....	90
Configuration.....	90
Sample Segments.....	90
Configuring the Devices.....	93
Adding an Access Device.....	93
Importing Devices in Bulk to AGNI.....	94
User Configurations.....	97
Users.....	97
All Users.....	97
External Users.....	97
Local User.....	98
User Groups.....	99
Local User Groups.....	99
Client Configuration.....	101
Clients.....	102
Client Details.....	104
Creating Client Certificates Manually in AGNI.....	105
Guest Onboarding Features.....	109
Guest Onboarding Using AGNI.....	109
Guest User in AGNI.....	109
Portal Users.....	109
UPSK Users.....	112

Guest Operator.....	114
Guest Sponsor.....	114
Guest Onboarding Offerings in AGNI.....	114
Portal Based Guest Onboarding.....	114
Clickthrough Portal-based Method.....	115
Support for Redirect URL in Guest Portal.....	116
Organizational User Login.....	117
Guestbook Based Onboarding.....	118
Guestbook Method.....	118
Self-Registration.....	120
Host Approval.....	122
UPSK Based Guest Onboarding.....	126
Configuring UPSK for Onboarding Guest (Wireless).....	126
Configuring AGNI.....	126
General Behavioral Guidelines:.....	129
Configuring CV-CUE.....	130
Onboarding the User.....	131
Configuring Guest Portal Using Guestbook (Wireless).....	132
Configuring the Portal on AGNI.....	132
Configuring the Network.....	138
Configuring CV-CUE.....	138
Configuring Role Profile.....	138
Configuring SSID.....	139
Configuring Guest Portal Using Guestbook-Host Approval (Wireless).....	143
Configurations on AGNI.....	143
Configuring the Network.....	147
Configuring CV-CUE.....	147
User Onboarding.....	147
Configuring Guest Portal Using Self Registration (Wireless).....	150
Configuring the Portal on AGNI.....	150
Configuring the Network.....	154
Configuring CV-CUE.....	154
User Onboarding.....	154
Configuring Guest Portal in AGNI for Wired Clients.....	154
Configuring AGNI.....	154
Configuring EOS.....	157
Configuring Guest Portal Using Guestbook (Wired).....	158
Configuring Guest Portal Using Guestbook-Host Approval (Wired).....	158
Configuring Guest Portal Using Self-Registration (Wired).....	158
Generating Client Certificates for RadSec.....	158
Viewing the Certificates.....	161
Configuring Device Groups.....	162

Configuring TACACS+ with AGNI.....	163
Installing Cloud Gateway.....	164
Debugging Workflow.....	165
Configuring Arista Cloud Gateway on Arista Switches.....	165
Configuring Arista Cloud Gateway on AGNI.....	168
Configuring TACACS+ on Arista Switches.....	171
Debug commands on Arista Cloud Gateway.....	172
Enabling Device Administration on AGNI.....	173
Configuring TACACS+ on AGNI.....	174
Monitoring TACACS+ on AGNI.....	176
Accessing Self Service Portal on AGNI.....	177
System.....	180
Audit Viewer.....	180
License.....	181
Self-Service Portal Settings.....	181
RadSec Settings.....	185
Support Logs.....	186
System Events.....	186
Notification Settings.....	187
Configuring Email Settings.....	187
Configuring SMS Gateway.....	190
Configuring the Twilio SMS Gateway.....	191
Configuring the MSG91 SMS Gateway.....	192
Sessions.....	193
On-Demand Disconnecting a Client from the Network.....	194
Troubleshooting.....	197
Monitoring.....	197
Dashboards.....	197
Sessions.....	198
Appendix.....	201
OIDC Vs SAML.....	201
Identity Providers.....	201
Microsoft Azure Active Directory.....	201
Google Workspace.....	202
OneLogin.....	203
Okta.....	203
URLs and Open Ports in Firewall.....	204

Introduction

This document provides information about Arista Networks' Arista Guardian for Network Identity (AGNI) software and explains the various configuration options 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 an administrator to access and configure the AGNI portal.

Accessing the User Interface (UI)

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

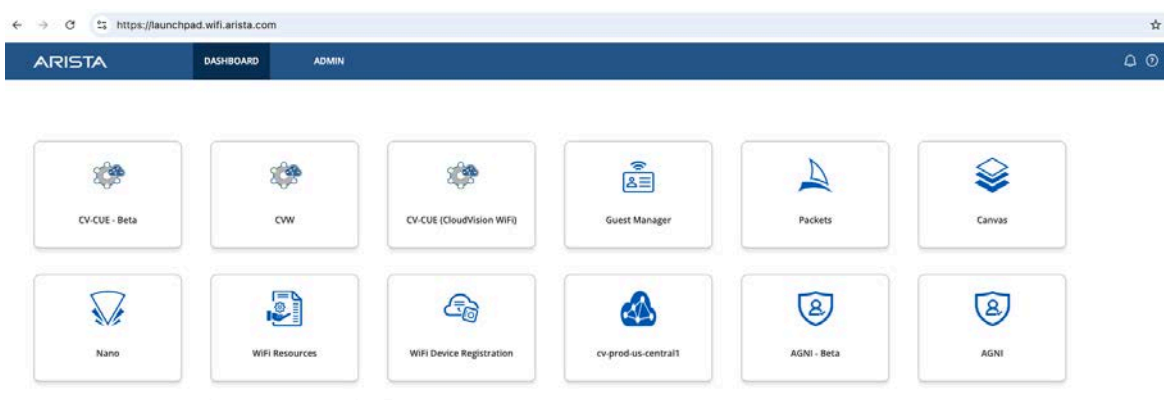


Figure: Arista Launchpad Displaying AGNI and Other Applications

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

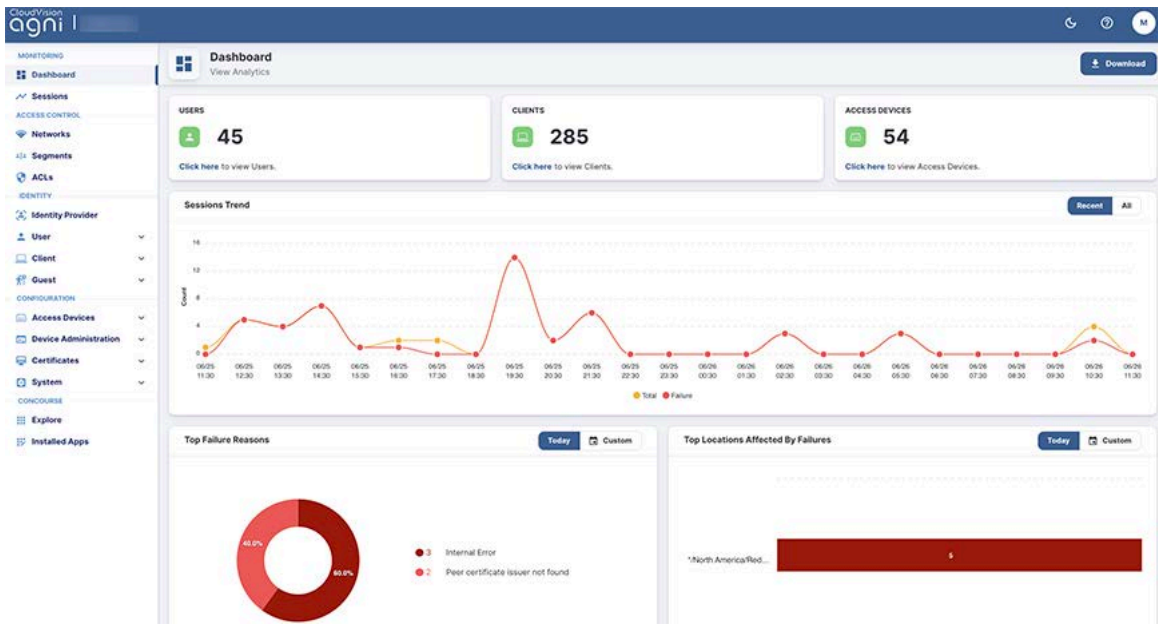


Figure: AGNI Dashboard

Viewing Licensing Details

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

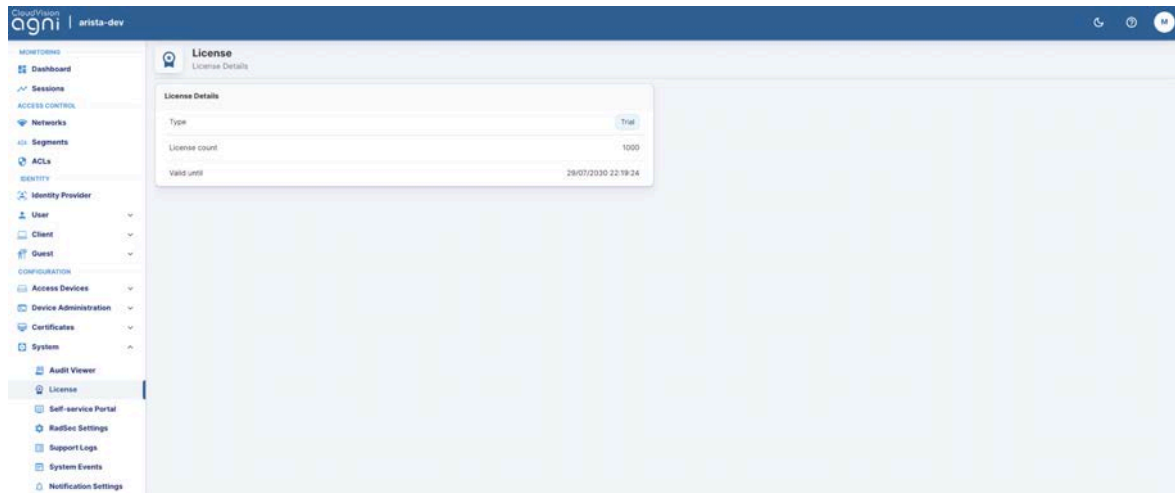


Figure: AGNI License Details

User Interface (UI) Theme

AGNI user interface (UI) offers different themes and modes, and as an admin, you can use any theme you prefer. Then, by default, the system theme gets applied to AGNI UI. You can also change the placement of options on the UI by moving 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).

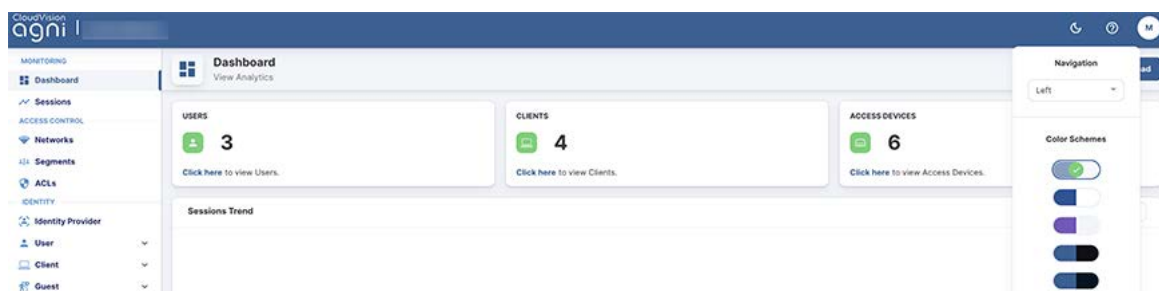


Figure: AGNI UI Theme (Navigation & Color) Settings

Integrating with Concourse Applications (Internal)

AGNI can integrate with other Arista applications by configuring that application from the Concourse Application (see image) page on the AGNI portal.

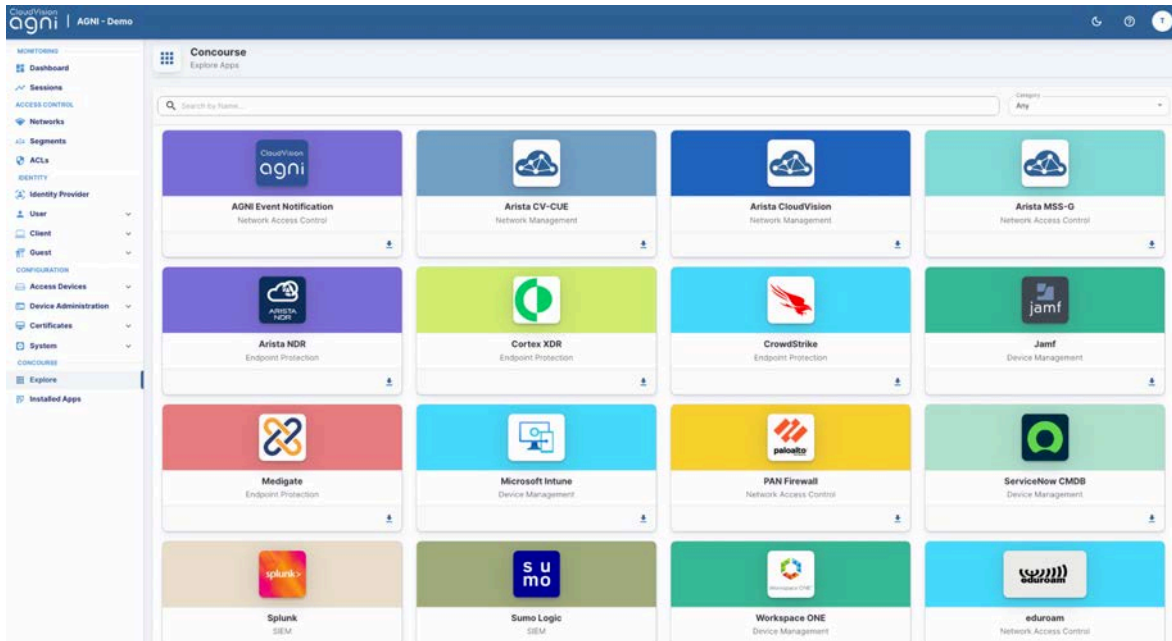


Figure: AGNI Concourse Applications

Arista CV-CUE Integration

Arista's CloudVision Cognitive Unified Edge (CV-CUE) delivers an integrated network 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 the 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**, select Arista **CV-CUE**.
2. Click the down arrow to install the **Arista CV-CUE** application.
3. Enter the following parameters (see the [document](#) to get the Key ID and Value):
 - a. Arista CV-CUE in the **Name** field
 - b. CV-CUE Key ID
 - c. CV-CUE Key Value

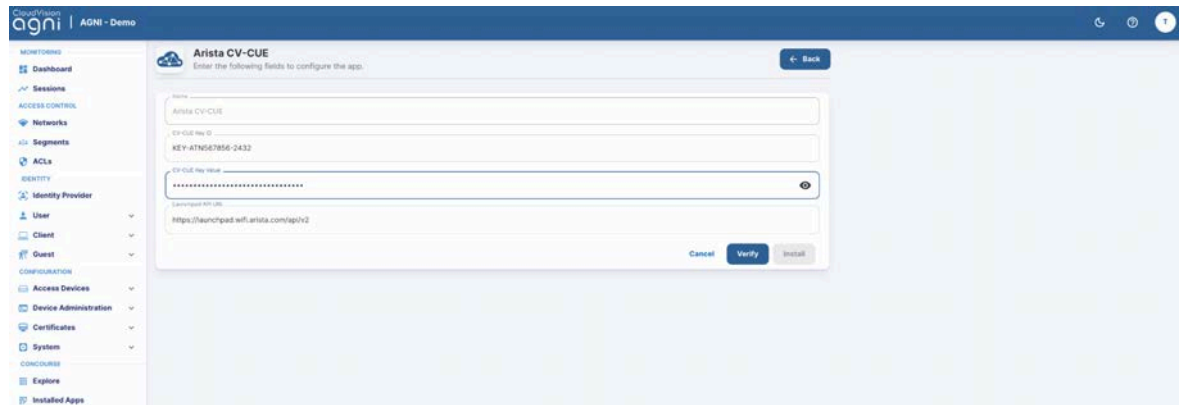
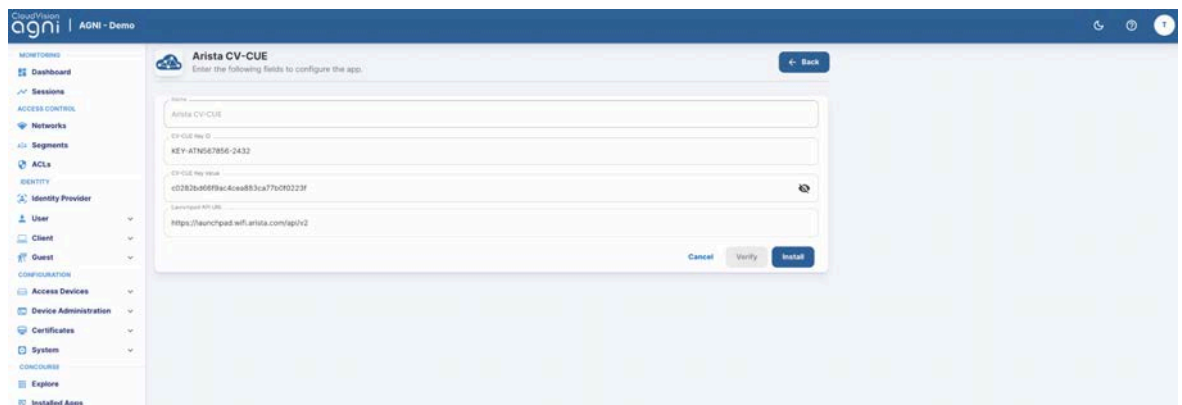


Figure: Installing CV-CUE Application

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



The CV-CUE application is displayed as an installed application on the Concourse page.

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

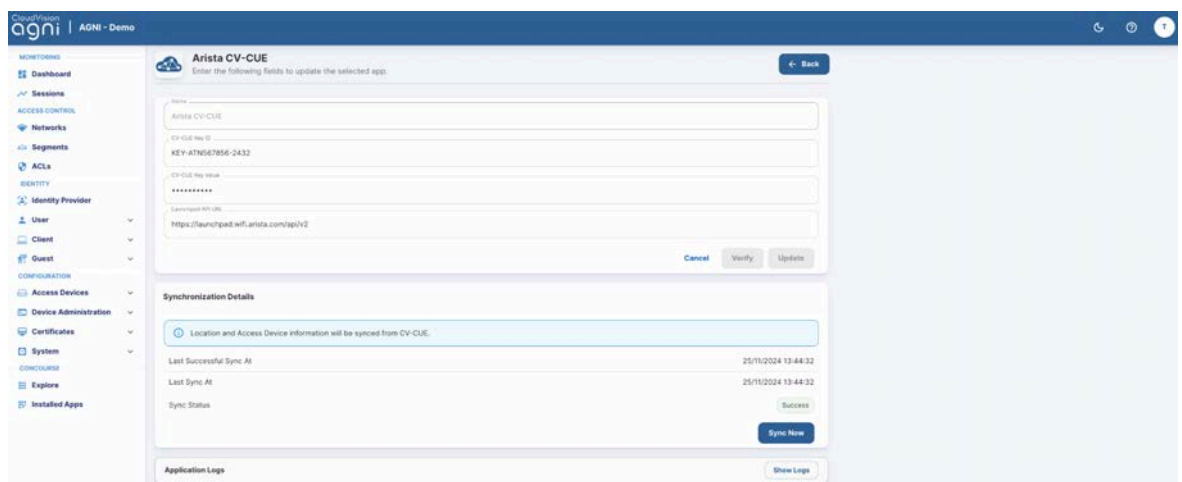


Figure: Synchronizing CV-CUE App

You can view the synchronized Access Points by navigating to: **Configuration -> Access Devices -> Devices** (see image).

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADIUS STATUS	UPDATE TIME
1	KK_Arista_A5-8B-2F	30-86-28-a5-8b-2f	Arista WFI	*India/Bengaluru/Marathalli	●	25/1/2024 13:42:38
2	Pradip_Arista_13-2A-8F	88-b1-e1-13-2a-8f	Arista WFI	*India/Bengaluru/Koramangala	●	25/1/2024 13:42:38
3	Arista_50-2C-FF	e4-d1-24-10-2c-ff	Arista WFI	Arista Cognitive WFI/India/GGN	●	25/1/2024 13:42:38
4	Madhu_10-13-1F	e4-d1-24-10-13-1f	Arista WFI	*India/Bengaluru/Banashankari	●	25/1/2024 13:42:38
5	Arista_AD-F3-0F	30-86-28-a0-f3-0f	Arista WFI	*India/PUNE-HN	●	25/1/2024 13:42:38
6	Arista_Pune_D0-07-4F	30-86-28-00-07-4f	Arista WFI	Arista Cognitive WFI/India/Pune	●	25/1/2024 13:42:38
7	Pradip-C230-62-77-0F	30-86-28-62-77-0f	Arista WFI	*India/Bengaluru/TC	●	25/1/2024 13:42:38
8	Arista_13-3A-5F	88-b1-e1-13-3a-5f	Arista WFI	*India/Bengaluru	●	25/1/2024 13:42:38
9	Arista_10-2A-8F	e4-d1-24-10-2a-8f	Arista WFI	*India/Uttarakhand	●	25/1/2024 13:42:38
10	Prem_D235_Arista_D0-7E-8F	30-86-28-00-7e-8f	Arista WFI	*India/Bengaluru/Hennur	●	25/1/2024 13:42:38
11	TARUN_Arista_C360-80-12-...	30-86-28-80-12-3f	Arista WFI	Arista Cognitive WFI/India/GGN	●	25/1/2024 13:42:38
12	rajg-Arista_7D-FF-4F	30-86-2d-7d-ff-4f	Arista WFI	Arista Cognitive WFI/India/Cochin	●	25/1/2024 13:42:38

Figure: Synchronized Access Points

Arista CloudVision Integration

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

The AGNI-CloudVision integration allows AGNI to fetch the details of all the managed wired switches. These details are synchronized with AGNI, and the MAC address and network device name are available as premium entities within AGNI when you configure segmentation policies.

Pre-requisites

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

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.
3. Enter the following parameters:
 - a. Arista CloudVision in the **Name** field.
 - b. The URL of the CloudVision application.
 - c. API Token value.

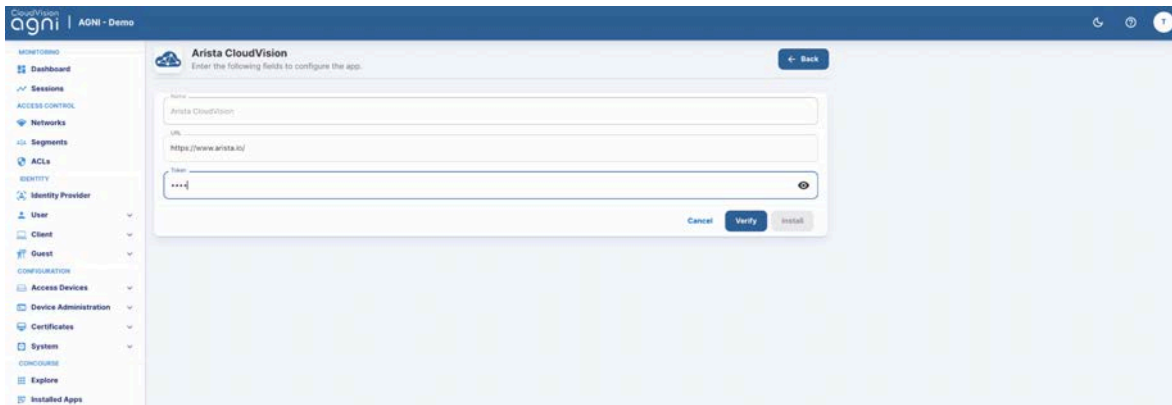


Figure: Installing Arista CloudVision Concourse Application

4. Click the **Verify** button to validate the credentials.
 5. Click the **Install** button to complete the installation process.
- The CloudVision application is displayed as an installed application on 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: **Configuration -> Access Devices -> Devices** (See image Synchronized Access Points).

Configuring CVaaS Instances

To configure 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 **Verify** and then **Update** to save the profile.
4. To add multiple CVaaS instances, click **here** while editing the previously added CVaaS profile (see the image).

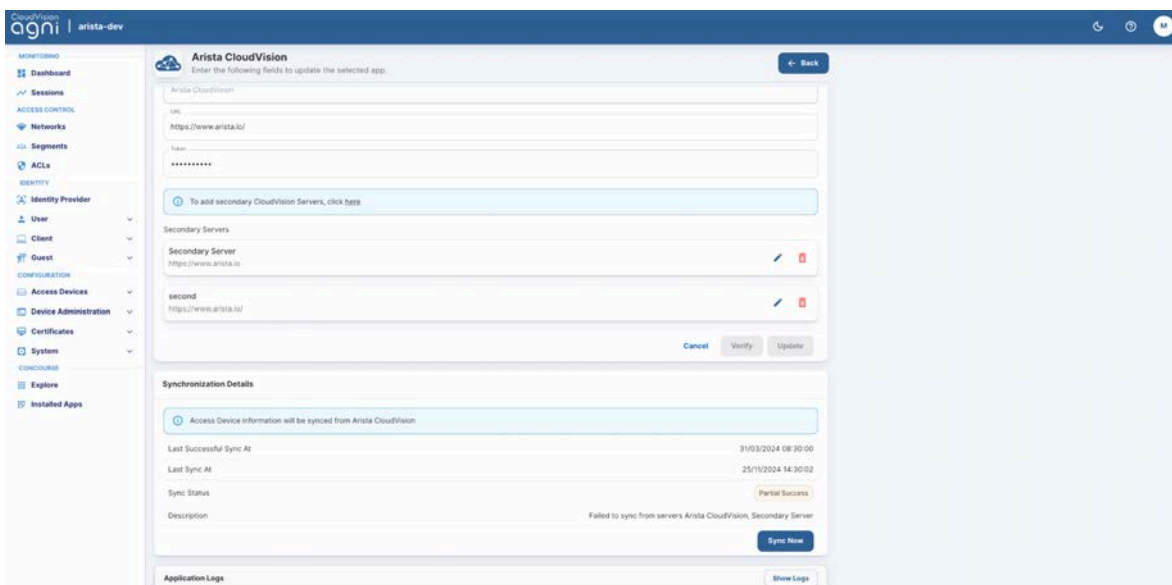
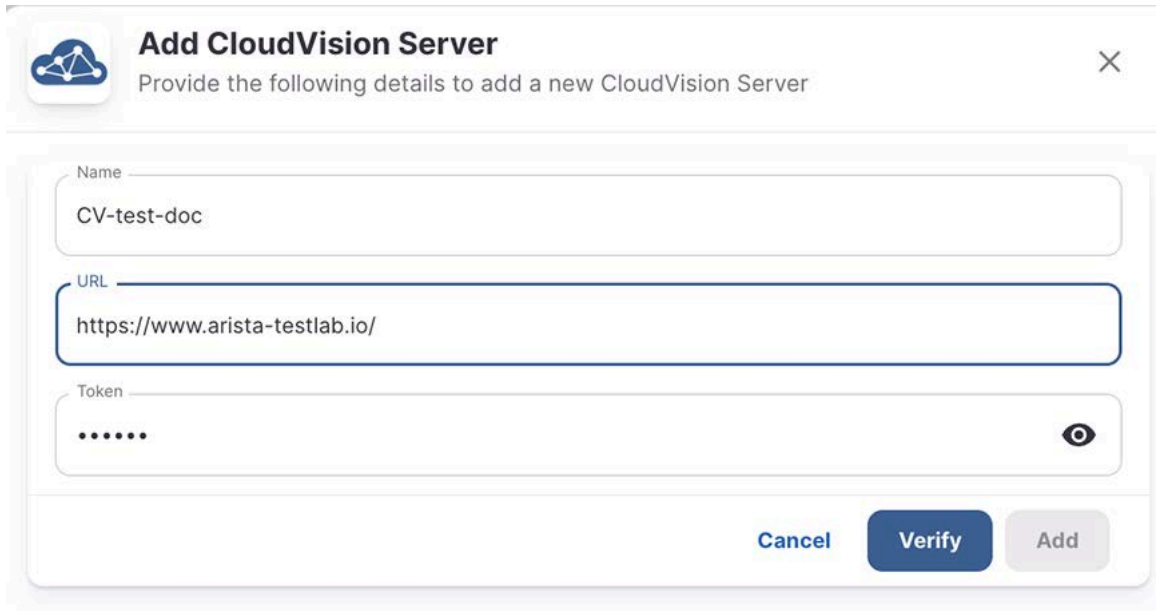


Figure: Adding Secondary Servers (CVaaS Instances)

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



The screenshot shows a pop-up window titled "Add CloudVision Server" with a close button (X) in the top right corner. Below the title is a subtitle: "Provide the following details to add a new CloudVision Server". The form contains three input fields: "Name" with the value "CV-test-doc", "URL" with the value "https://www.arista-testlab.io/", and "Token" with masked characters "....." and a toggle icon (an eye) on the right. At the bottom right of the form are three buttons: "Cancel", "Verify" (highlighted in blue), and "Add" (disabled, shown in light gray).

Figure: Adding Secondary Servers

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

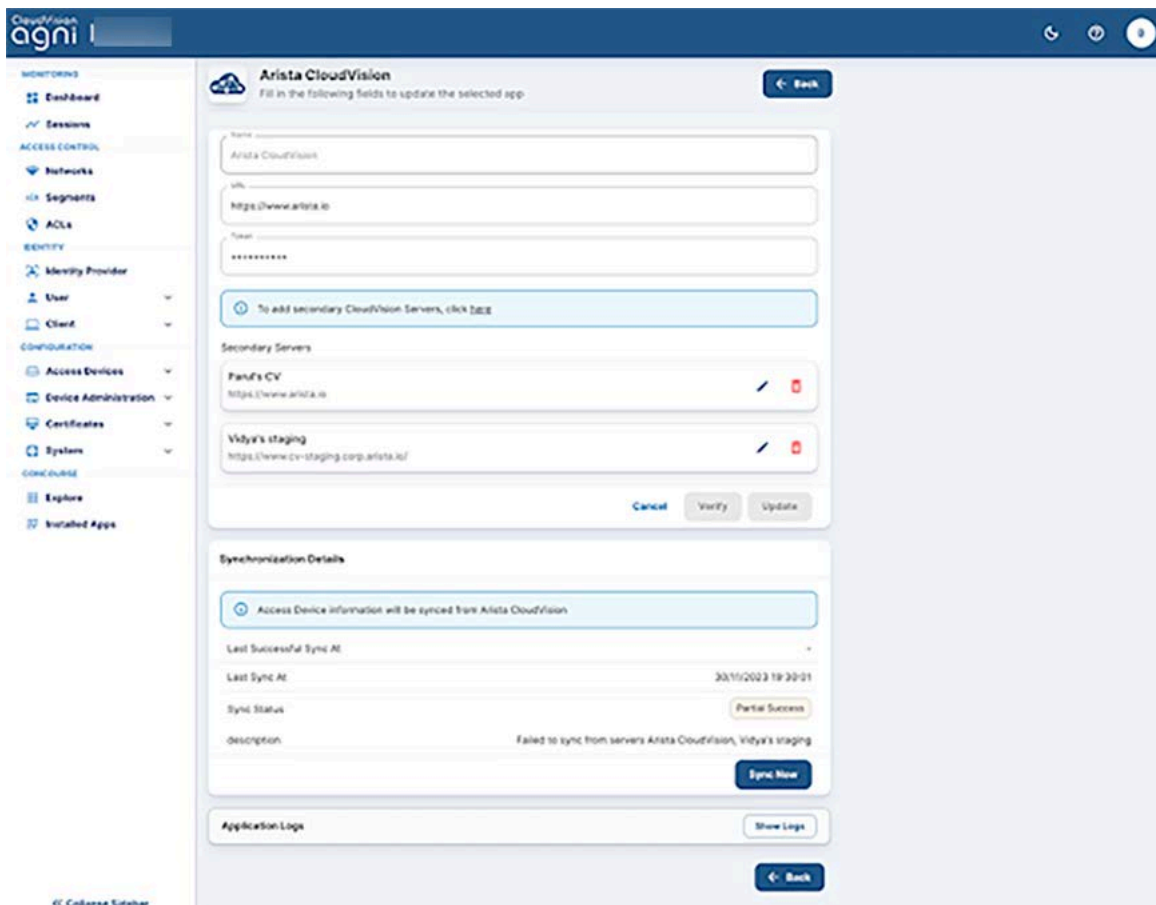


Figure: CVaaS Synchronization Details

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.

#	NAME	MAC ADDRESS	VENDOR	LOCATION	RADSEC STATUS	UPDATE TIME
1	arista-710P	2c-dd-e9-ff-39-d4	Arista Switch	Secondary Server/Tenant/San Jose	●	31/03/2024 08:30:00
2	agni-720xp-24-1	c0-d6-82-16-3f-59	Arista Switch	Secondary Server/Tenant/Bassett	●	31/03/2024 08:30:00
3	agni-720dp48-1	2c-dd-e9-ff-d4-a5	Arista Switch	Secondary Server/Tenant/Bassett	●	31/03/2024 08:30:00
4	agni-720dp-24-1	28-e7-1d-ca-0e-f1	Arista Switch	Secondary Server/Tenant/Bassett	●	31/03/2024 08:30:00
5	at-arista720dp	28-e7-1d-ca-0e-fb	Arista Switch	Secondary Server/Tenant/AGNI_HQ	●	31/03/2024 08:30:00
6	agni-722xpm-48	ac-3d-94-c8-27-9c	Arista Switch	Secondary Server/Tenant/AGNI_HQ	●	31/03/2024 08:30:00
7	CV-CUE-12P-1	2c-dd-e9-fe-0f-ea	Arista Switch	Secondary Server/Tenant/Undefined	●	31/03/2024 08:30:00
8	Arista Switch		Arista Switch		●	29/01/2024 11:04:49

Figure: View Access Devices (Switches)

Adding Multiple CVaaS Instances in AGNI

You can configure multiple CVaaS instances that are linked to AGNI. As 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. For more details, refer to the [document](#).

Arista NDR Integration

You can integrate Arista NDR version 5.1.0 or later with AGNI for post-authentication profiling. To integrate Arista NDR with AGNI:

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

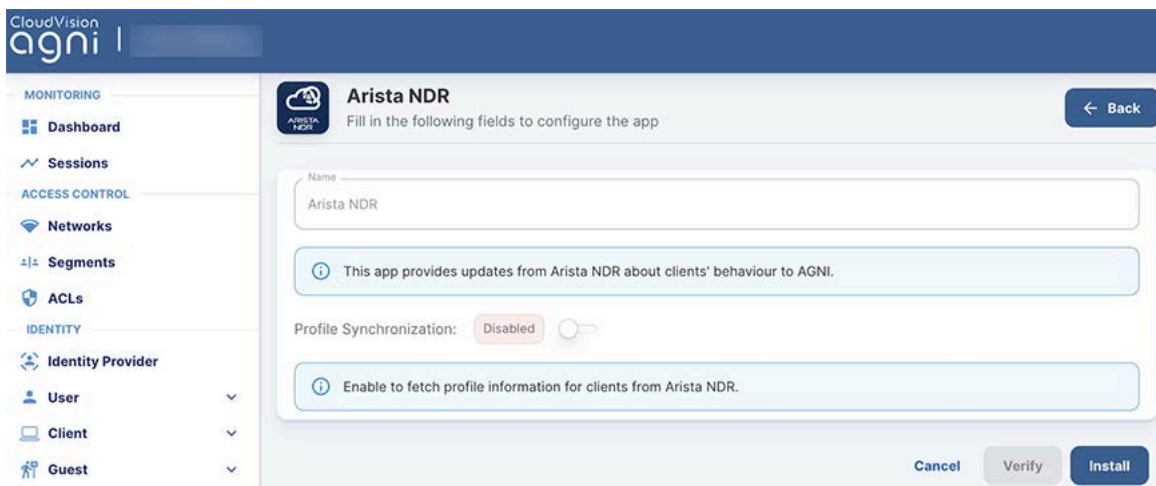


Figure: Arista NDR Integration

2. Click the **Install** button to Install the application. The AGNI API URL is displayed.
 3. Click the **Generate Token** button to generate the API.
- The API URL and API Token are used in the NDR solution to integrate with AGNI.
Note: The Token is displayed only once at the install time (see image).

CloudVision agni I

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client
- Guest

CONFIGURATION

- Access Devices
- Device Administration
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

Arista NDR

Fill in the following fields to update the selected app

← Back

Name

Arista NDR

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

Profile Synchronization: Disabled

Enable to fetch profile information for clients from Arista NDR.

Notification API details

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

API URL

https://systest.agnieng.net/api/concourse.app.aristaNDR.notification

Copy

No API token is present.

Generate Token

Application Logs

Show Logs

Cancel Verify Update

Figure: Arista NDR Integration API Details

CloudVision agni I

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client
- Guest

CONFIGURATION

- Access Devices
- Device Administration
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

Arista NDR

Fill in the following fields to update the selected app

← Back

Name

Arista NDR

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

Profile Synchronization: Disabled

Enable to fetch profile information for clients from Arista NDR.

Notification API details

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

API URL

https://systest.agnieng.net/api/concourse.app.aristaNDR.notification

Copy

For security reasons, API token is shown only once. Use the following token henceforth.

API Token

.....

Copy

Application Logs

Show Logs

Cancel Verify Update

Figure: Arista NDR Integration API and Token Details

Configuring Arista NDR

To configure Arista NDR:

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

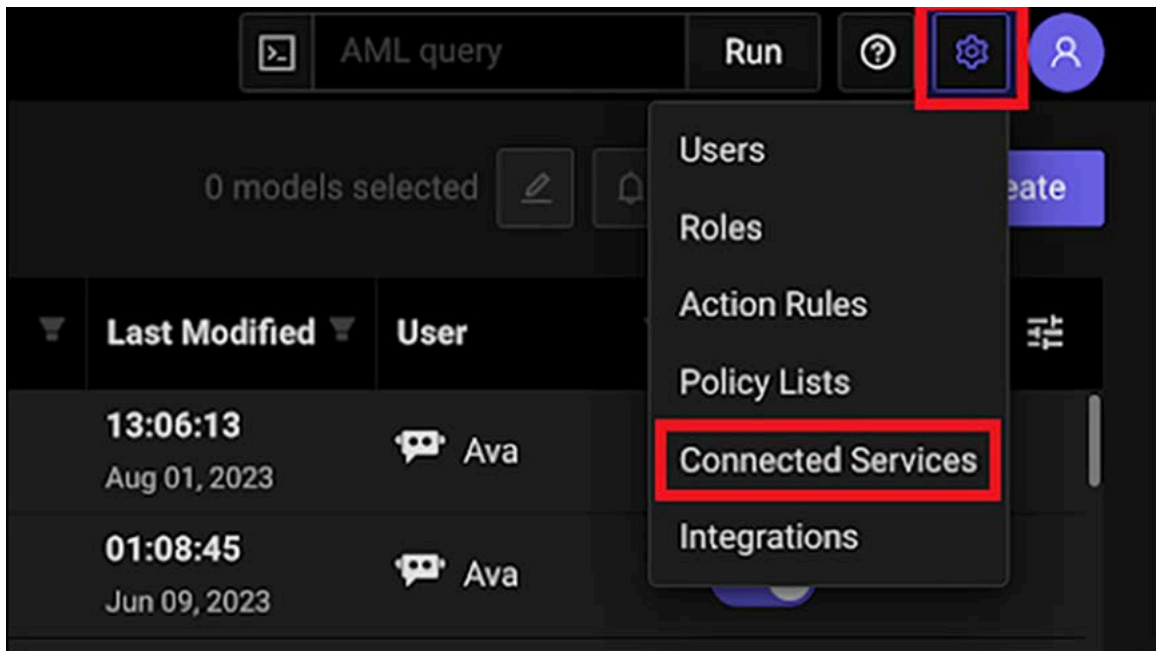


Figure: Arista NDR Settings Page

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

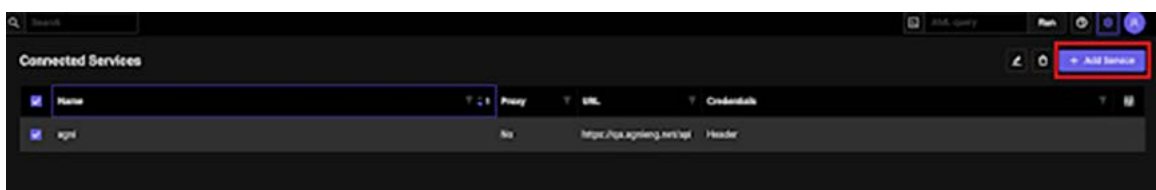
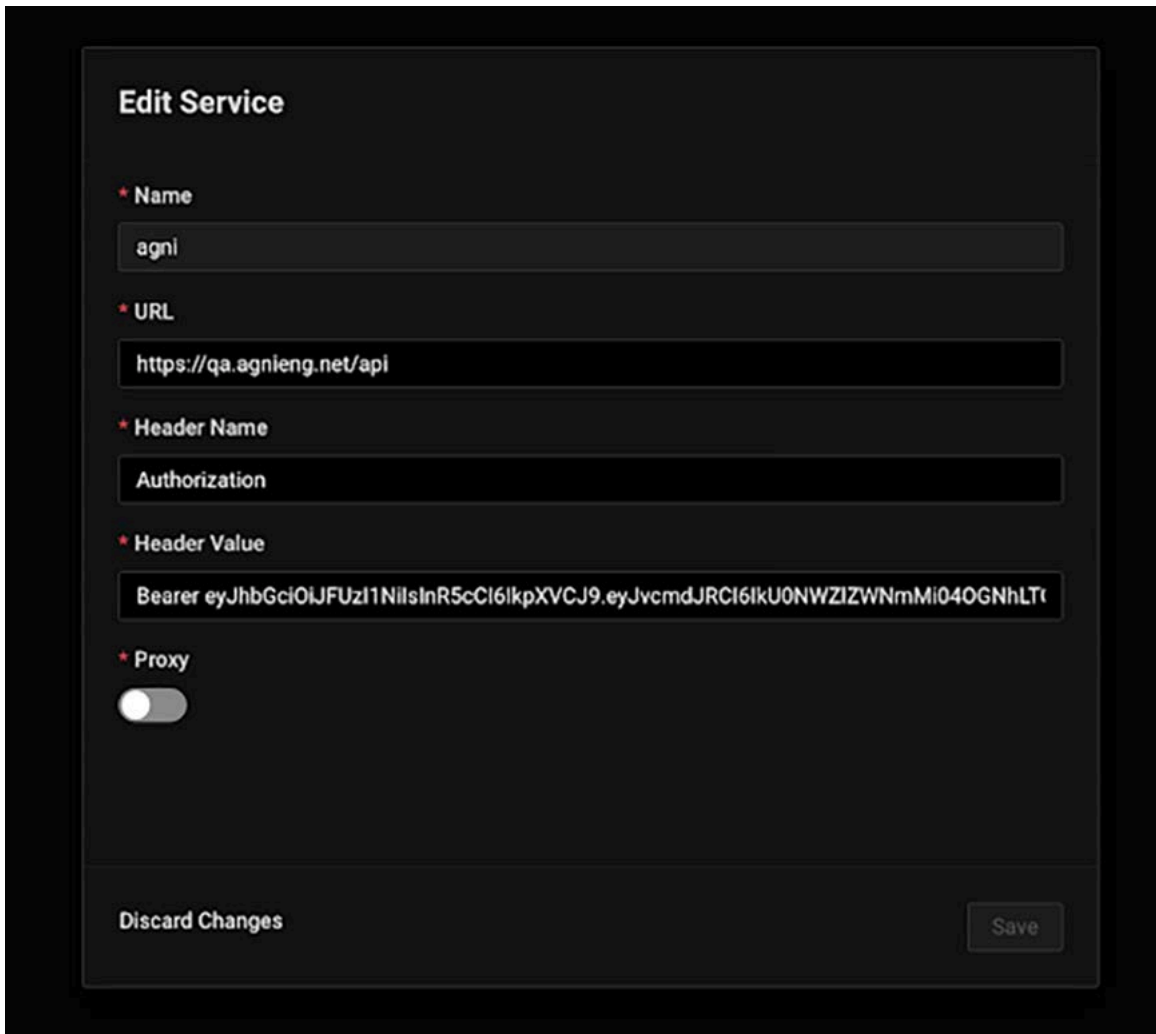


Figure: Arista NDR Configuration - Add Service

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



The image shows a dark-themed 'Edit Service' dialog box. It contains five labeled input fields: 'Name' with the value 'agnl', 'URL' with 'https://qa.agnleng.net/api', 'Header Name' with 'Authorization', and 'Header Value' with a long Bearer token. A 'Proxy' toggle switch is shown in the 'off' position. At the bottom, there are two buttons: 'Discard Changes' on the left and 'Save' on the right.

Edit Service

* Name
agnl

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

* Header Name
Authorization

* Header Value
Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IklU0NWZIZWNmMi04OGNhLTt

* Proxy
☐

Discard Changes Save

Figure: Arista NDR Configuration Details

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

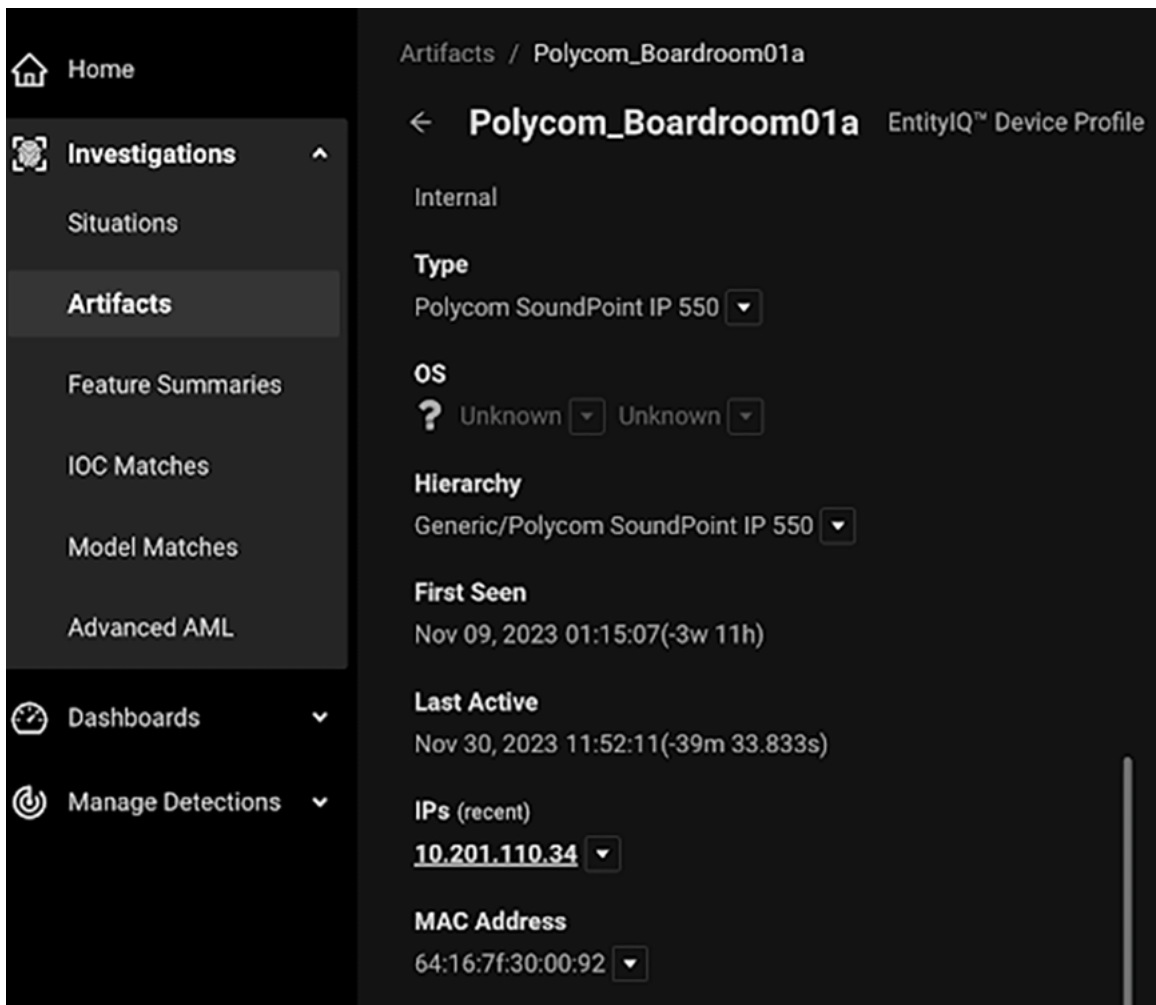


Figure: Arista NDR Configuration Artifacts Details

6. 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 with Arista NDR.

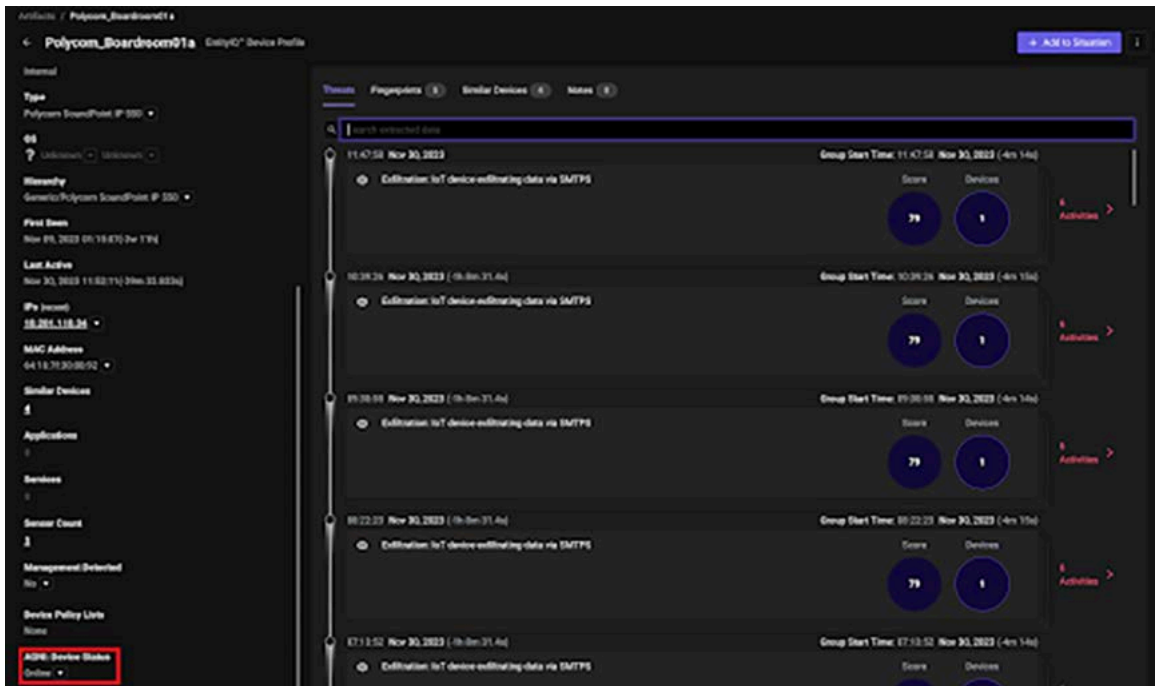


Figure: Arista NDR - AGNI Integration Status

Configuring Segment Policies

After the successful integration of AGNI with Arista NDR, as an admin, you can configure the segments in AGNI based on the parameters synchronized 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 the MAC address of the device.

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 06:37:49.810
2	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 05:37:49.540
3	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 04:37:49.267
4	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 03:37:48.997
5	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 02:37:48.725
6	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 01:37:48.455
7	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	26/06/2024 00:37:48.183
8	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	25/06/2024 23:37:47.912
9	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	25/06/2024 22:37:47.630
10	Laptops	MAC Authentication	38:ca:84:b4:d5:0b		Success	25/06/2024 21:37:47.358

Figure: Sessions Details

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

Session Details - Rcptmjpdttc4c72slant0

Details for Session

Authentication Request (Success)

Authentication Type: MAC Authentication

Segment: Default

Location: Pune/ABZ

Session Details (Closed)

Client IP Address: -

Session Start Time: 26/06/2024 06:37:49.810

Session Stop Time: 26/06/2024 06:47:36.016

User

Not available

Client (Enabled)

38:ca:84:b4:d5:0b

WindowsLaptop

Laptops

Access Device (Arista Switch)

fc:bd:67:0e:f8:f5

PLM-Switch01-10.87.33.41

PLM-Switches

Network (Enabled)

MAC-AUTH

Wired

MAC Authentication

Actions

Allow Access

Input Request Attributes

Output Response Attributes

Session logs for request: Rcptmjpdttc4c72slant0

Show Logs

Figure: Sessions Client Details

- Add the details and click Update Client:

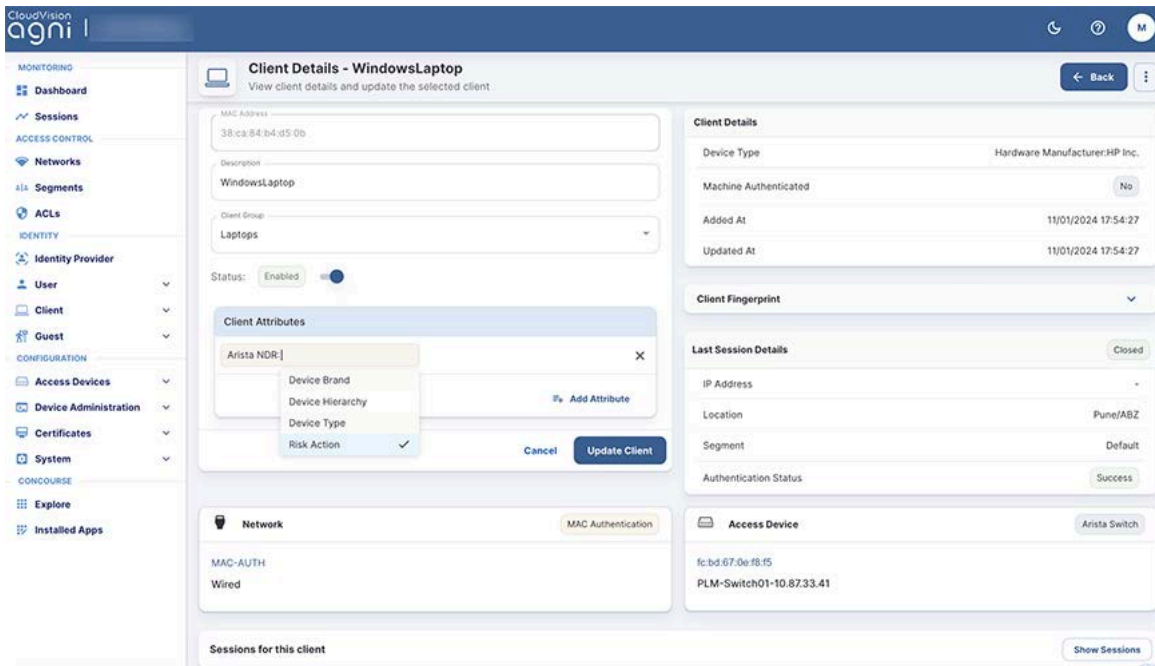


Figure: NDR Client Details

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

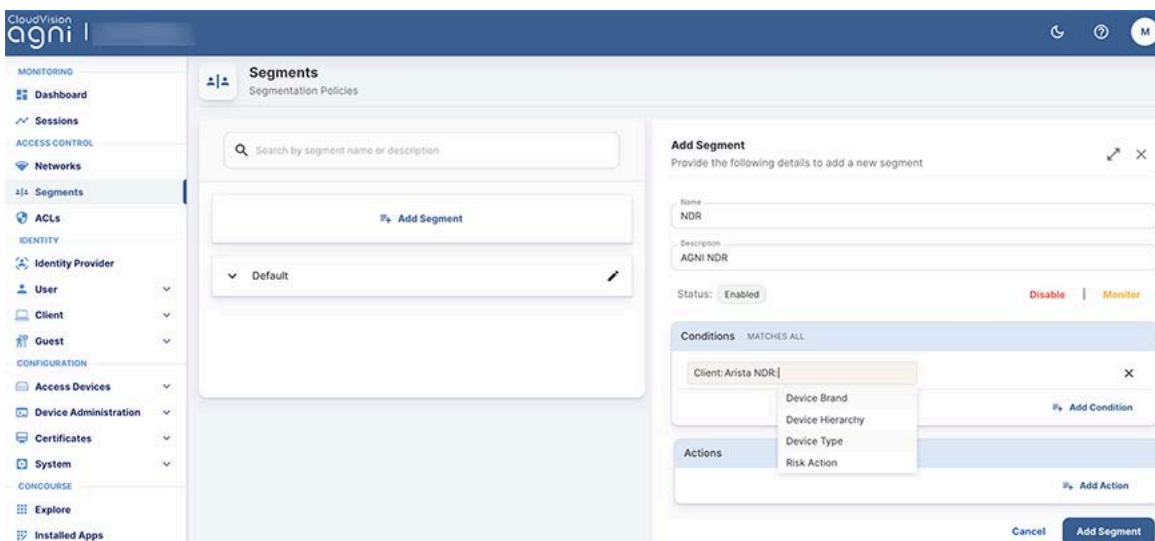


Figure: Add Segment Details

Using Risk Action in Segment Policies

To use Risk Action in segmentation policy:

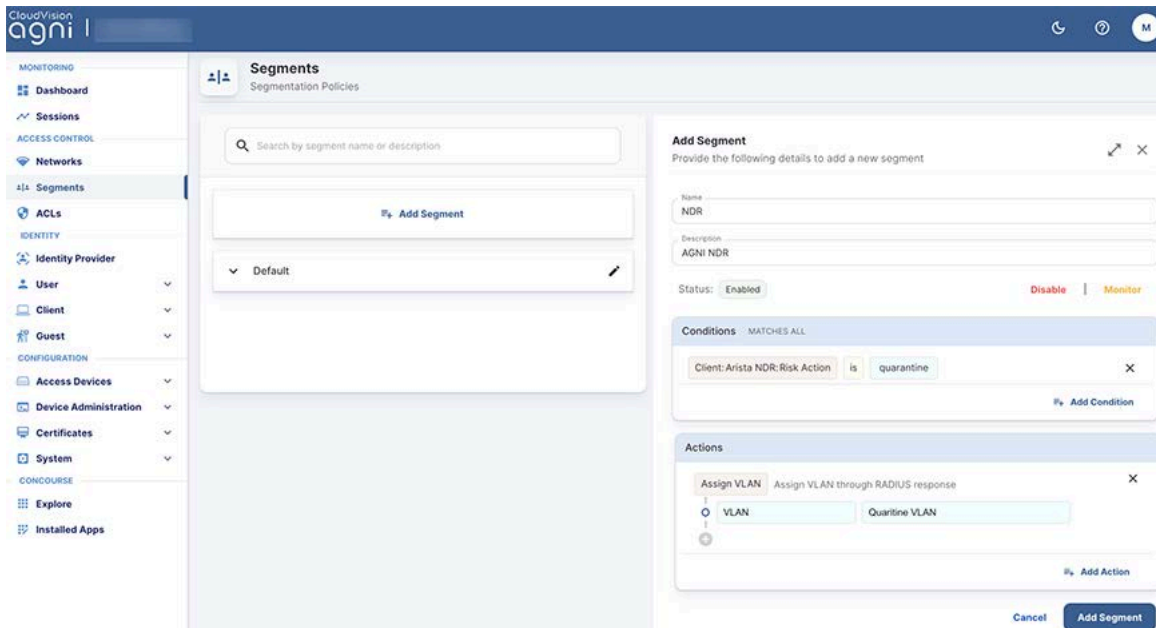


Figure: Add Segment Details for Risk Action

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.

After a risk analysis, if the client is not *at risk*, then either the NDR admin or the AGNI admin can de-quarantine the client. If AGNI admin decides to change the status, go to **Identity > Client > Clients** on AGNI UI. Select the client and change the **Arista NDR: Risk Action** to **deQuarantine** in the **Client Attributes** tab (see image below).

To validate the client status on Arista NDR, check if the **AGNI:Device Status** value is **Online**.

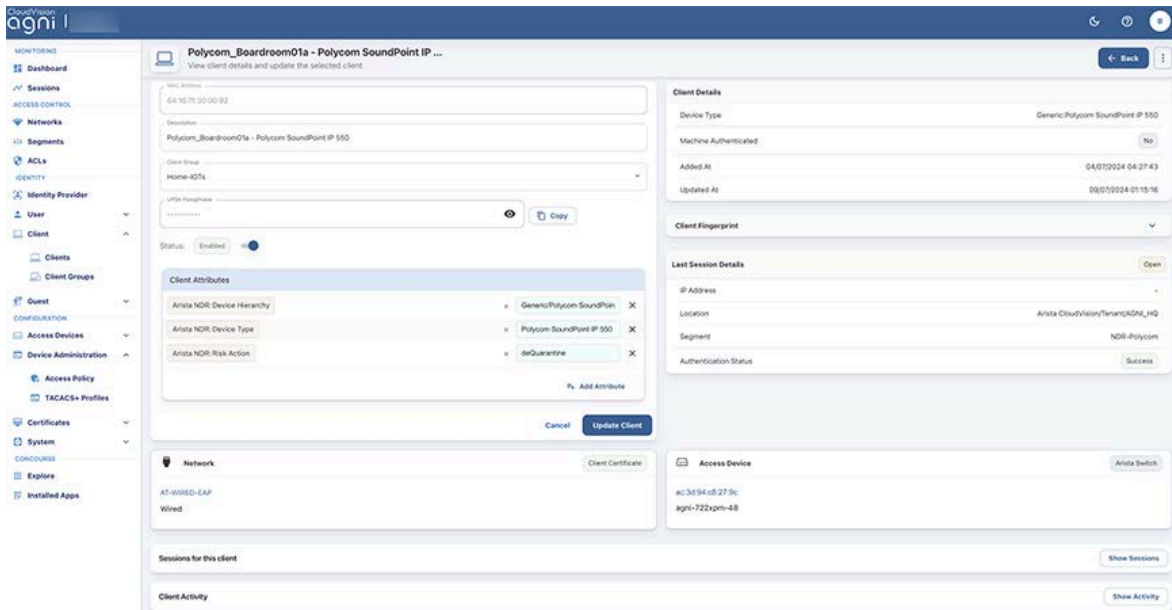


Figure: Update Client Details for Risk

Integrating with Concourse Applications (External)

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's retrieval of 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

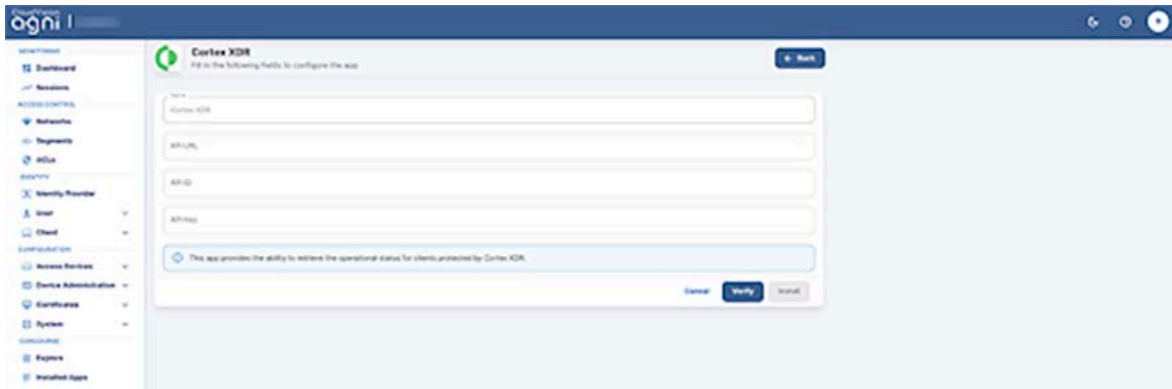


Figure: Installing Palo Alto Cortex XDR Concourse Application

4. Click the **Verify** button to validate the credentials
5. Click the **Install** button to complete the installation process.
6. The Palo Alto Cortex XDR application is displayed as an installed application on the Concourse page.
7. Click the **Sync Now** button on the Cortex XDR page to initiate the synchronization process.

Palo Alto Firewall Integration

This section describes the integration of Palo Alto's Next-Generation Firewall (NGFW) and Panorama devices with AGNI.

Palo Alto Firewall provides contextual security to users, allowing finely tuned control over application access. For this to happen, firewalls require a correlation between the user and its assigned IP address. AGNI is capable of relaying this information to firewalls to fill the gap. This process implements granular policy enforcement at the perimeter through the firewall.

Usually, in customer deployments, the firewalls are deployed at the perimeter in large numbers. In such scenarios, AGNI can interface with Palo Alto Panorama for the user ID and context updates.

Benefits:

The AGNI-Palo Alto Firewall integration provides the following capabilities:

- Ability to configure multiple Palo Alto firewall details.
- Ability to configure multiple Panorama details.
- Ability to configure specific instances of Panorama or Palo Alto firewall in the segment configuration for user-ID updates. For example:
 - Corporate Access Segment for SJC updates should be part of Panorama-SJC.

- Corporate Access Segment for BLR updates should be part of Panorama-BLR.

Note: The same applies to firewalls when customers are not using Panorama.

- As the Palo Alto integration with AGNI is done through the Cloud Gateway, AGNI uses the information in the PAN FW configuration to select the Cloud Gateway for sending the userID updates.

Pre-requisites:

- AGNI must have reachability access to the Palo Alto firewall or Panorama endpoints over port 443. However, this may not happen in some scenarios, as the firewall entities may not have inbound internet access. AGNI uses the Edge Gateway (Cloud Gateway) route to communicate with the firewalls.
Note: AGNI Edge Gateways are deployed as SWIX extensions on Arista EOS switches. They establish a secure tunnel with AGNI facilitating the communication of user-ID updates to on-premises Palo Alto Firewall or Panorama devices.
- Enable RADIUS accounting on the network access devices. The client's IP address is relayed through the RADIUS accounting packets. AGNI needs this information to relay user-ID bindings to Palo Alto Firewall or Panorama devices.

You can integrate the Palo Alto PAN Firewall or Panorama with AGNI through the Concourse Application page on the AGNI portal.

Configuring the Palo Alto Firewall/Panorama

After you install the PAN Firewall application, configure the firewall or the Panorama devices as below:

Palo Alto Firewall Configuration

To configure the Palo Alto firewall, enter the following details:

- **Server Type** - Select Firewall.
- **Server Name** - Enter the server name or identifier for the firewall (server configuration name or entity to identify the instance).
- **Hostname** - Hostname or IP address of the firewall.
- **Username** - User name part of the user credentials to authenticate with the firewall.
- **Password** - Password part of the user credentials to authenticate with the firewall.
- **Cloud Gateway** - Choose the Cloud Gateway to communicate with this firewall
- Click the **Verify** button to verify and validate the credentials.

CloudVision agni | myorg1.com

PAN Firewall
Enter the following fields to configure the app.

← Back

Name: PAN Firewall

Server Type: ☒ Firewall ☐ Panorama

Server Name: _____

Hostname: _____

Username: _____

Password: _____

Cloud Gateway: _____

Cancel Verify Update

After successfully validating the credentials, you can update the device and add additional servers using the same process.

To add additional firewall servers, click the [here](#) link.

CloudVision agni | myorg1.com

PAN Firewall
Enter the following fields to update the selected app.

Name: PAN Firewall

Server Type: Firewall

Server Name: PAN FW_90

Hostname: 34.145.15.90

Username: antara

Password:

Cloud Gateway: ACG_HQ_139

To add additional Firewalls, click [here](#)

Cancel

Add Firewall
Provide the following details.

Server Name: _____

Hostname: _____

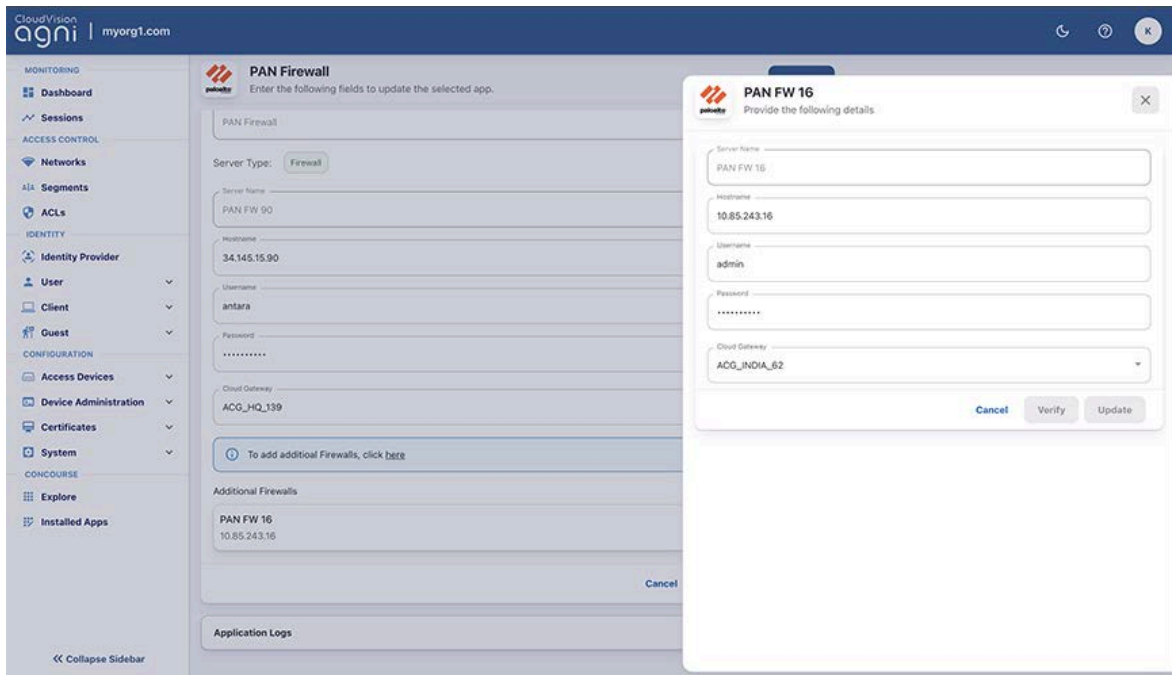
Username: _____

Password: _____

Cloud Gateway: _____

Cancel Verify Update

To update the firewall details, click the **Update** button.



For more details on the Palo Alto Firewall/Panorama integration and configuration, see the [document](#).

Medigate Integration

Medigate is an Endpoint Profiling 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 the 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)

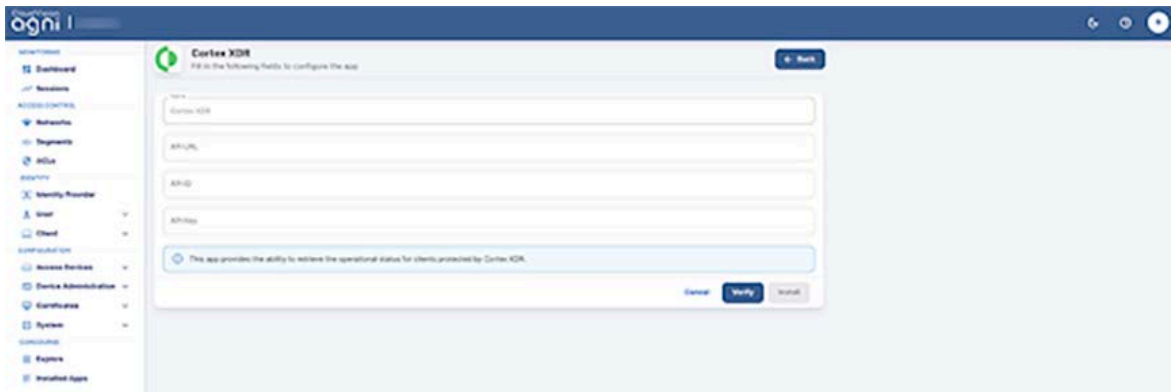


Figure: Installing Medigate Concourse Application

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 is displayed as an installed application on the Concourse page.
6. Click the **Sync Now** button on the Medigate page to initiate the synchronization process (see image below).

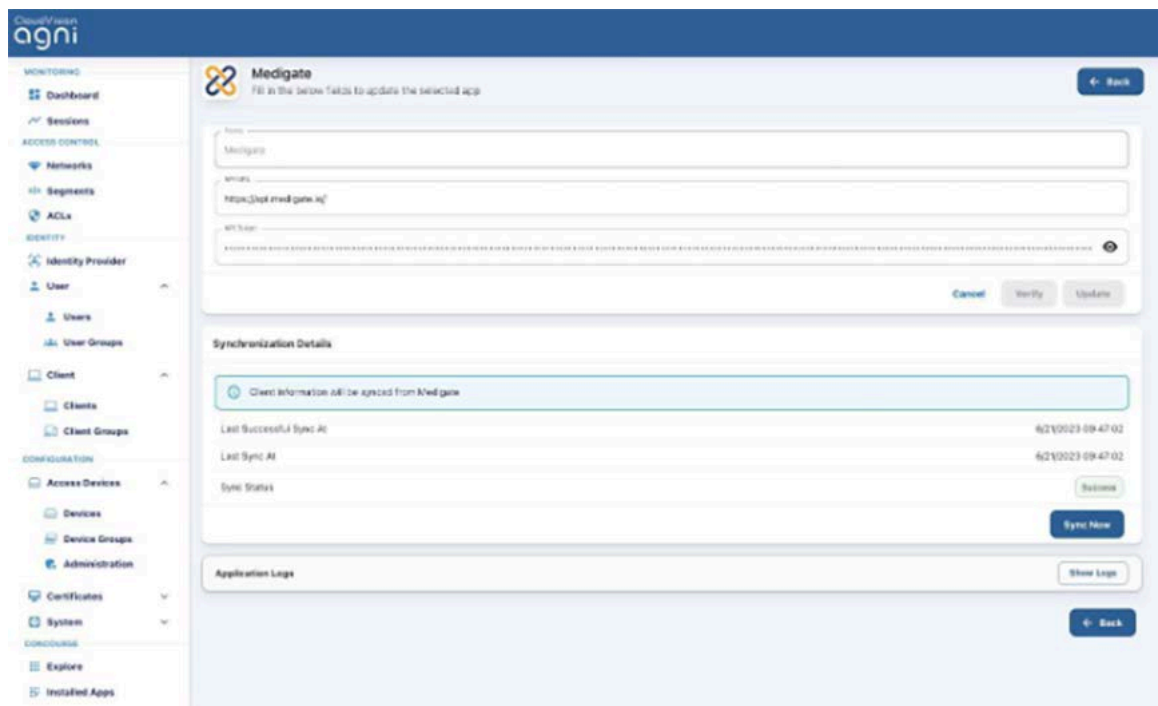


Figure: Installed Medigate Concourse Application

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).

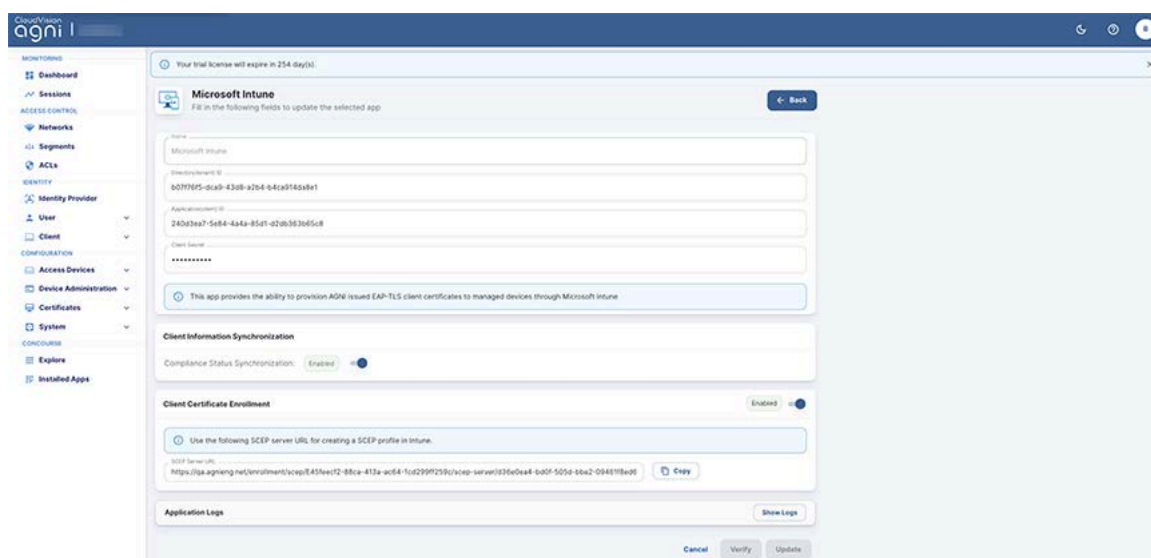
The screenshot shows the AGNI portal interface. On the left is a navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Device Administration, Certificates, System), and CONCOURSE (Explore, Installed Apps). The 'Explore' option is selected. The main panel displays the 'Microsoft Intune' application configuration form. At the top, it says 'Your trial license will expire in 254 day(s)'. Below this is a 'Back' button. The form has several input fields: 'Name' (pre-filled with 'Microsoft Intune'), 'Directory (Tenant) ID' (pre-filled with '60779f5-dca6-43b8-a2b4-44ca916d3a81'), 'Application (Client) ID' (pre-filled with '240d3ea7-5e84-444a-85d1-a2b6363b65c8'), and 'Client Secret' (masked with asterisks). A checkbox is checked with the text 'This app provides the ability to provision AGNI issued EAP-TLS client certificates to managed devices through Microsoft Intune'. Below this are sections for 'Client Information Synchronization' and 'Client Certificate Enrollment', both with 'Enabled' toggle switches. The 'Client Certificate Enrollment' section includes a text box with a generated SCEP URL and a 'Copy' button. At the bottom are 'Application Logs' and 'Show Logs' buttons. The bottom right of the form has '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 is displayed as an installed application on the Concourse page.

Jamf Integration

Jamf is a Device Management concourse application that facilitates the 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.

Prerequisites: The Jamf integration requires the SCEP challenge and the URL generated in AGNI to be configured in the Jamf administration portal. Refer to vendor documentation for details on configuring 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).

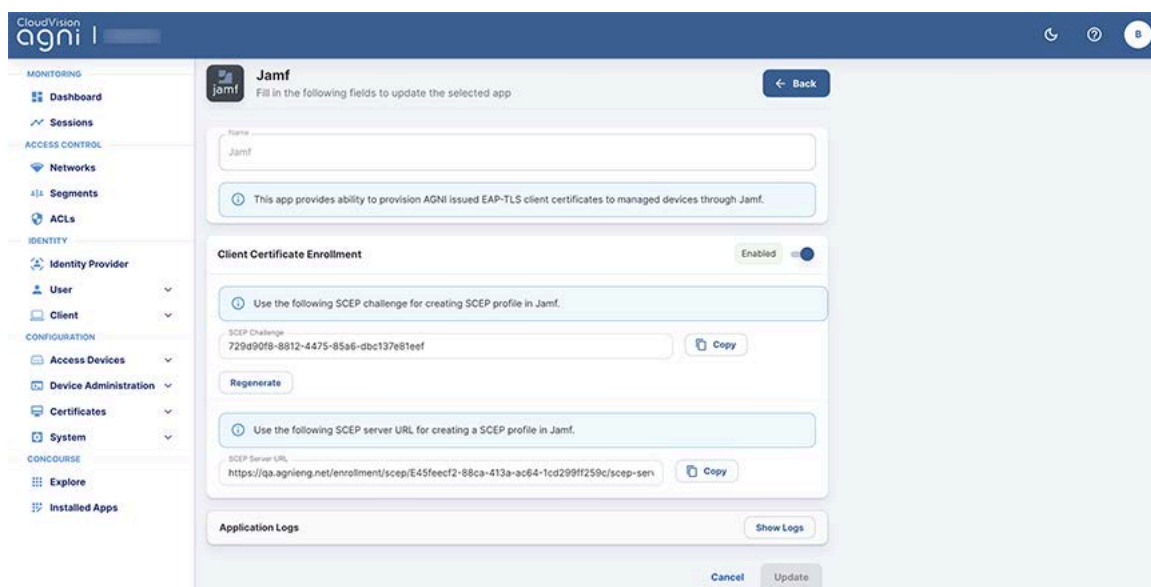
The screenshot shows the AGNI portal interface. On the left is a sidebar with a menu containing sections like MONITORING, ACCESS CONTROL, IDENTITY, CONFIGURATION, and CONCURSE. The 'CONCURSE' section is expanded, showing 'Explore' and 'Installed Apps'. The main area displays the 'Jamf' application configuration page. At the top, there's a header 'Jamf' and a sub-header 'Fill in the following fields to update the selected app'. Below this is a 'Name' field with 'Jamf' entered. A description box states: 'This app provides ability to provision AGNI issued EAP-TLS client certificates to managed devices through Jamf.' The 'Client Certificate Enrollment' section has an 'Enabled' toggle set to 'On'. It contains two text areas: one for 'SCEP Challenge' with the value '729d90f8-8812-4475-85a6-dbc137e81eef' and a 'Copy' button, and another for 'SCEP Server URL' with the value 'https://qa.agnieng.net/enrollment/scep/E45feecf2-88ca-413a-ac64-1cd299ff259c/scep-ser' and a 'Copy' button. There are 'Regenerate' and 'Show Logs' buttons. At the bottom are 'Cancel' and 'Update' buttons.

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 them into the Jamf administration portal to create the SCEP profile.
The Jamf application is displayed as an installed application on the Concourse page.

ServiceNow CMDB Integration

ServiceNow CMDB is an asset management database that enterprise IT teams use to manage corporate assets. In an organization, IT teams create assets, group them, and manage them under different classes. The integration of AGNI with CMDB enables the IT team to fetch the devices in AGNI and authorize device access based on the

segment policies.

This requires a configuration change in AGNI and ServiceNow CMDB.

To configure ServiceNow for AGNI integration:

1. Login to the ServiceNow CMDB portal.
2. Click the **All** tab and search for Application Registry Under the System OAuth option.

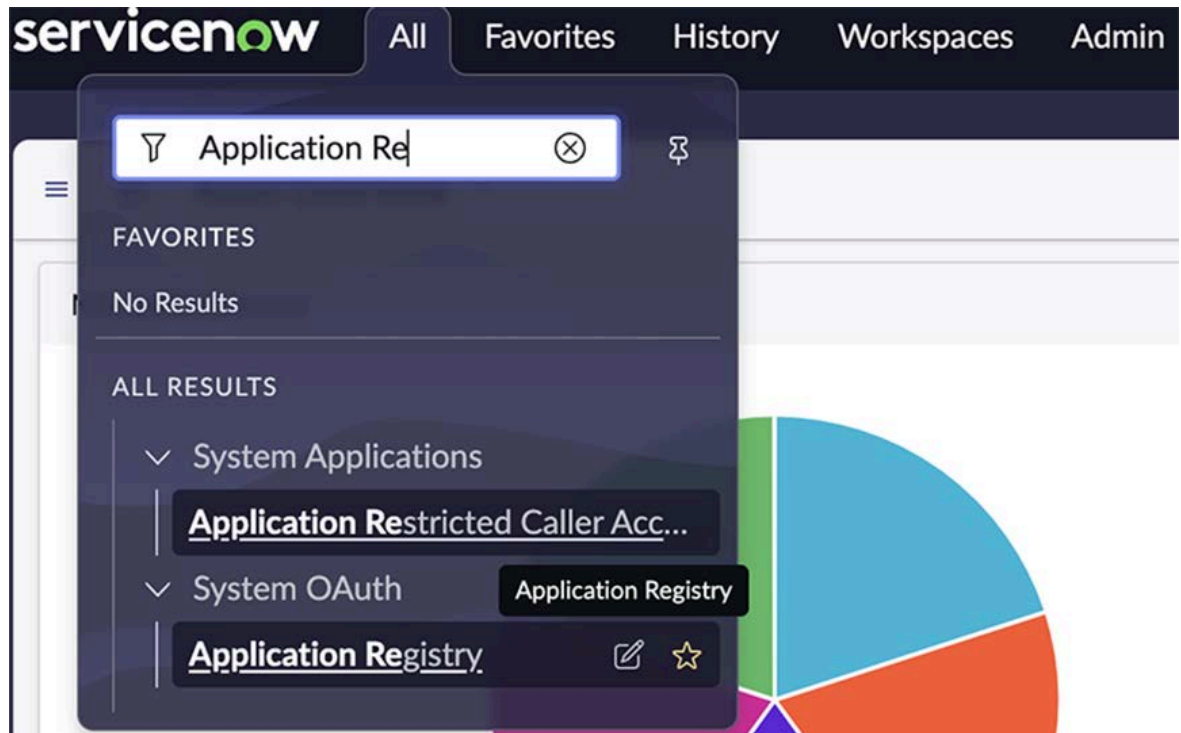


Figure: Accessing ServiceNow Application Registry

3. Click **Application Registry**. A new window with a list of applications is displayed.
4. Click the **New** button at the top right corner to add a new application for AGNI.

A screenshot of the ServiceNow 'Application Registries' page. The page shows a table with columns: Name, Active, Type, Client ID, and Comments. The table lists various applications, including Azure AD, Azure OAuth OIDC Entity, cmdb oauth provider, jwt_auth, Mobile API, ServiceNow Agent, ServiceNow Classic Mobile App, ServiceNow Request, ServiceNow Virtual Agent Example App, Sidebar Microsoft Teams Graph, Sidebar Teams Token Auth, snow-cvp-app-oauth, and WebKit HTML to PDF. A 'New' button is visible in the top right corner.

Name	Active	Type	Client ID	Comments
Azure AD	true	OAuth Provider	Enter Client ID	
Azure OAuth OIDC Entity	true	External OIDC Provider	<Provide Azure Application ID URI>	Used for Azure to Servicenow Integration
cmdb oauth provider	true	OAuth Client	90487a8324ce461090d01d6488ce1744	
jwt_auth	true	OAuth Client	0698aa91cad242502139be8761d0f475	
Mobile API	true	OAuth Client	ac0dd3408c1031006907010c2cc6ef6d	Used by the mobile app to allow access L...
ServiceNow Agent	true	OAuth Client	ff97fbb4da3313004591cc3a291b47fd	
ServiceNow Classic Mobile App	false	OAuth Client	3e57bb02663102004d010ee8f561307a	
ServiceNow Request	true	OAuth Client	5c54dc934a022300cb7946e6ec6ec172	
ServiceNow Virtual Agent Example App	true	OAuth Client	2c403f19ac901300b303eef6c8b842d3	
Sidebar Microsoft Teams Graph	true	OAuth Provider		
Sidebar Teams Token Auth	true	External OIDC Provider	common	
snow-cvp-app-oauth	true	OAuth Client	e549d0364133a11094f1eba01faee685	
WebKit HTML to PDF	true	OAuth Client	1624ac93b46221009eb8191f0e41680d	Used by the service WebKit HTML to PDF

Figure: Create a new Application for AGNI

5. Select *Create an OAuth API endpoint for external clients* from the list of OAuth application types.

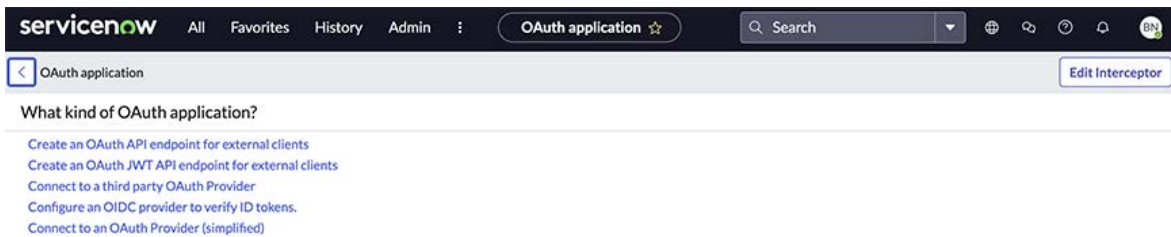


Fig 3: Select OAuth API Endpoint for External Clients

6. Enter the relevant details and click the Submit button to save the application.

Figure: Provide CMDB OAuth details for AGNI

Note: Copy and save the Client ID and Client secret for future reference.

Splunk Integration

Splunk is a SIEM concourse application. Enabling Splunk integration with AGNI facilitates retrieving the session log updates for 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.

Prerequisites: The integration requires Splunk SIEM credentials to be configured as part of the concourse application configuration. Refer to vendor documentation for details on configuring 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).

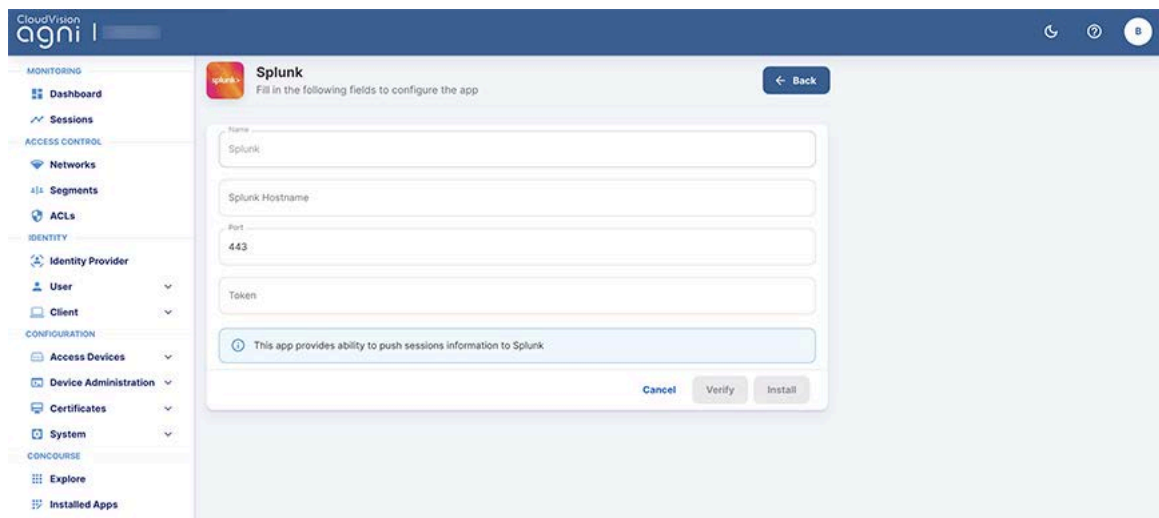


Figure: Installing Splunk Concourse Application

3. Enter the following parameters:
 - a. Splunk in the **Name** field
 - b. Splunk Hostname
 - c. Port (default is 443)
 - d. Token
4. Click the **Verify** button to validate the credentials.
5. Click the **Install** button to complete the installation process.
The Splunk application is displayed as an installed application on 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).

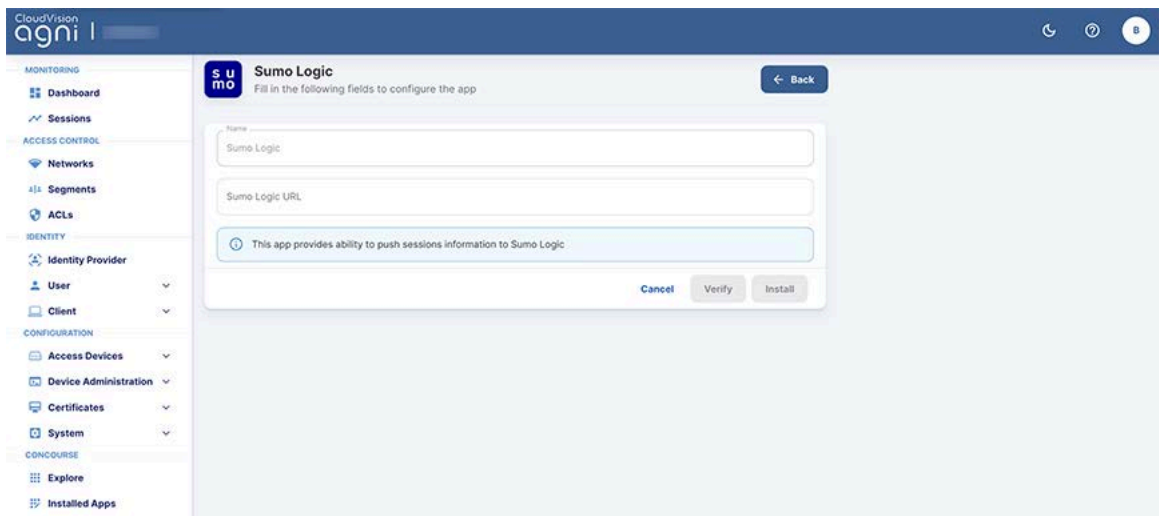


Figure: Installing Sumo Logic Concourse Application

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 and click the **Verify** button to verify the application.
For details, see the documentation [here](#).

Figure: Installing CrowdStrike Concourse Application

The Event Notification enables AGNI to receive notification status from CrowdStrike whenever the device details change.

4. Copy and save the Notification URL and Notification Secret (required while configuring CrowdStrike Falcon Console).

Figure: Event Notification Configuration for CrowdStrike

Workspace ONE integration

Workspace ONE is an enterprise Mobile Device Management (MDM) solution to manage corporate owned devices. 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.

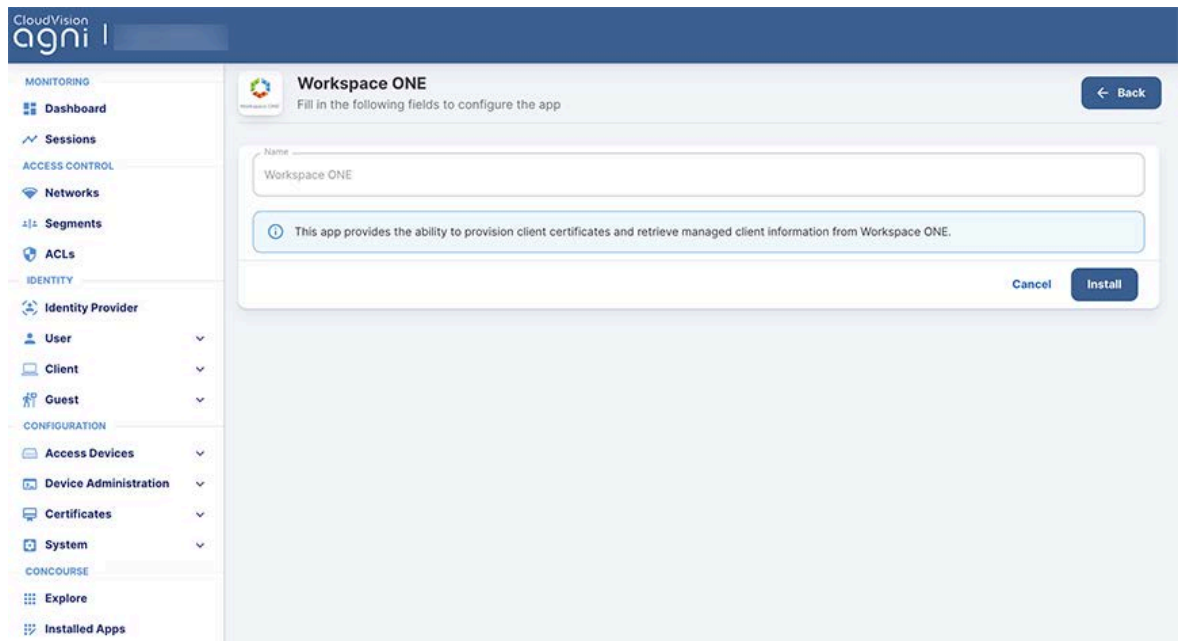


Figure: Installing Workspace ONE

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. For details, see the documentation [here](#).

Workspace ONE

Fill in the following fields to update the selected app

Name: Workspace ONE

This app provides the ability to provision client certificates and retrieve managed client information from Workspace ONE.

Client Information Synchronization

Client Information Synchronization: Enabled

API URL

Client ID

Client Secret

Verify

Event Notification: Disabled

Enable to allow Workspace ONE to send notifications to AGNI for managed clients.

Client Certificate Enrollment: Disabled

Application Logs

Show Logs

Cancel Update

Figure: Configuring Workspace ONE parameters

- 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.

- Enable the **Client Certificate Enrollment** and copy and save the **SCEP URL** and **SCEP Challenge** to be required later for configuring Workspace ONE.

Workspace ONE

Fill in the following fields to update the selected app

Client ID

Client Secret

Verify

Event Notification: Enabled

Use the following details in Workspace ONE to send notifications to AGNI.

Notification URL: https://api.agrieng.net/api/concourse/app/workspaceone/notification/ea13f9a9-2a76-44a3-ba16-2a27c944a045

Copy

Notification Username: ee2a2d56-8a1e-4430-acc7-8ae0fedc79c

Copy

Notification Password: 729c0fbc-7c79-4801-b799-9411c83034f4

Copy Regenerate

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

Client Certificate Enrollment: Enabled

Use the following SCEP challenge for creating SCEP profile in Workspace ONE.

SCEP Challenge: 9160488b-6c61-4062-b3ca-e7677840c3d9

Copy Regenerate

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

SCEP Server URL: https://api.agrieng.net/enrollment/scep/ea13f9a9-2a76-44a3-ba16-2a27c944a045/scep-server/748f4a9-5eb2-55e3

Copy

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

Application Logs

Show Logs

Cancel Update

Figure: Configuring Workspace ONE parameters

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
 - Device Administration 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 Entra ID 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. Sync Interval (hours)
6. Click the **Verify** button. Once the operation is successful, the system fetches the list of groups from the IDP, which can be used in the policy creation.

Add Identity Provider
Fill in the fields below to add a new Identity Provider

Name: Azure Demo

Domain Name: systestpoc.onmicrosoft.com

Identity Provider: Microsoft 365 (Azure)

Identity Information Synchronization: Enabled

Directory (tenant) ID: b2fde07-420e-479f-b66f-c86569a27542

Application (client) ID: b4c0696d-fc7a-4501-a8b8-468a2c35b980

Client Secret:

Sync Interval (hours): 24

Buttons: Cancel, Verify, Add

Figure: Adding Identity Provider

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

Identity Provider
Identity Access Management

Identity Provider	Domain	Updated At	Last Sync Scheduled At	Sync Status
okta	acme.org	21/10/2023 00:45:38	06/12/2023 17:30:00	Success
b0776f5-dca9-43d8-a2b...	antaraalieng.onmicrosoft.com	06/09/2023 03:30:13	06/12/2023 12:30:00	Success

Local Users:

Identity Provider	Domain
local	local

Figure: Edit or Update Identity Provider

- 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.

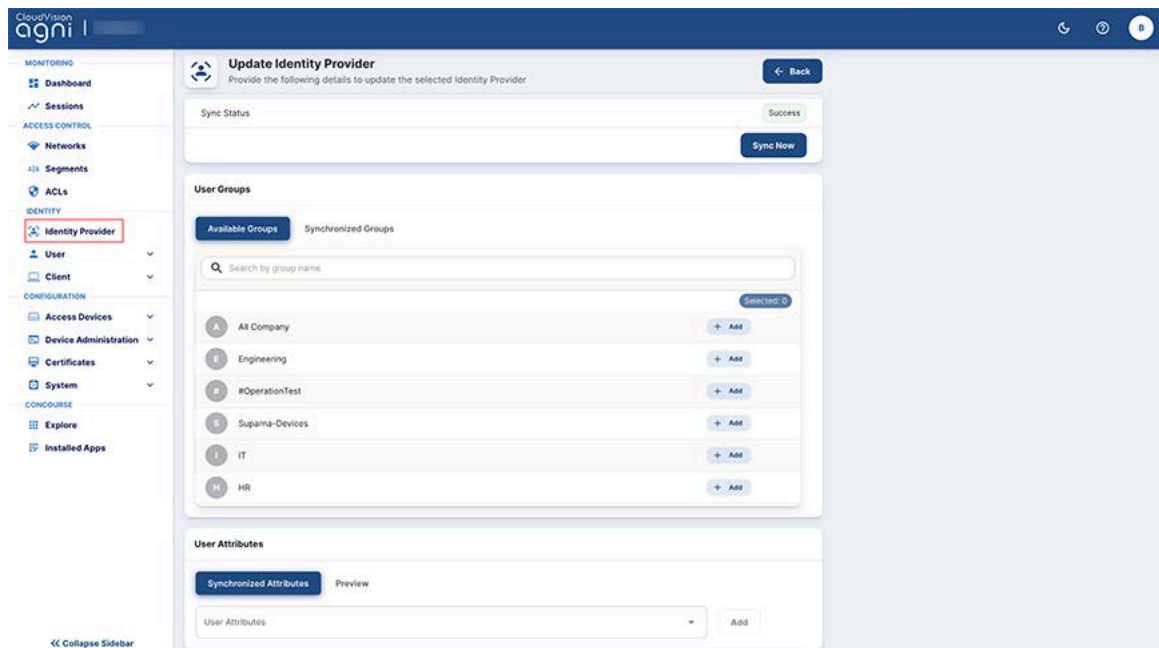


Figure: Identity Provider Available Groups

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.

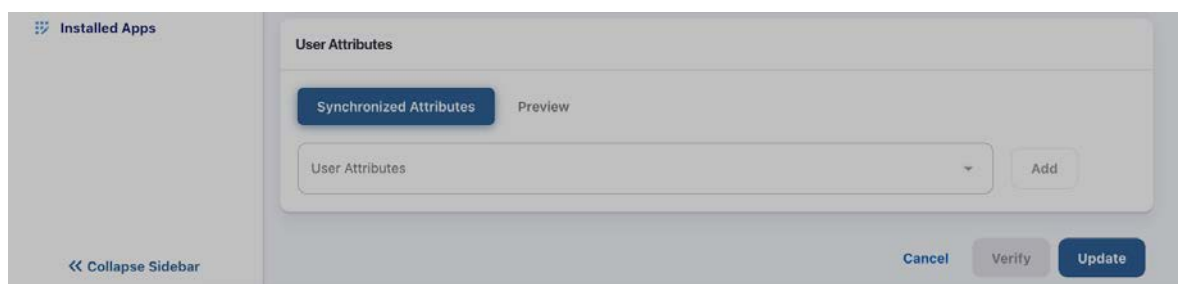


Figure: Identity Provider and User Attributes

- **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.

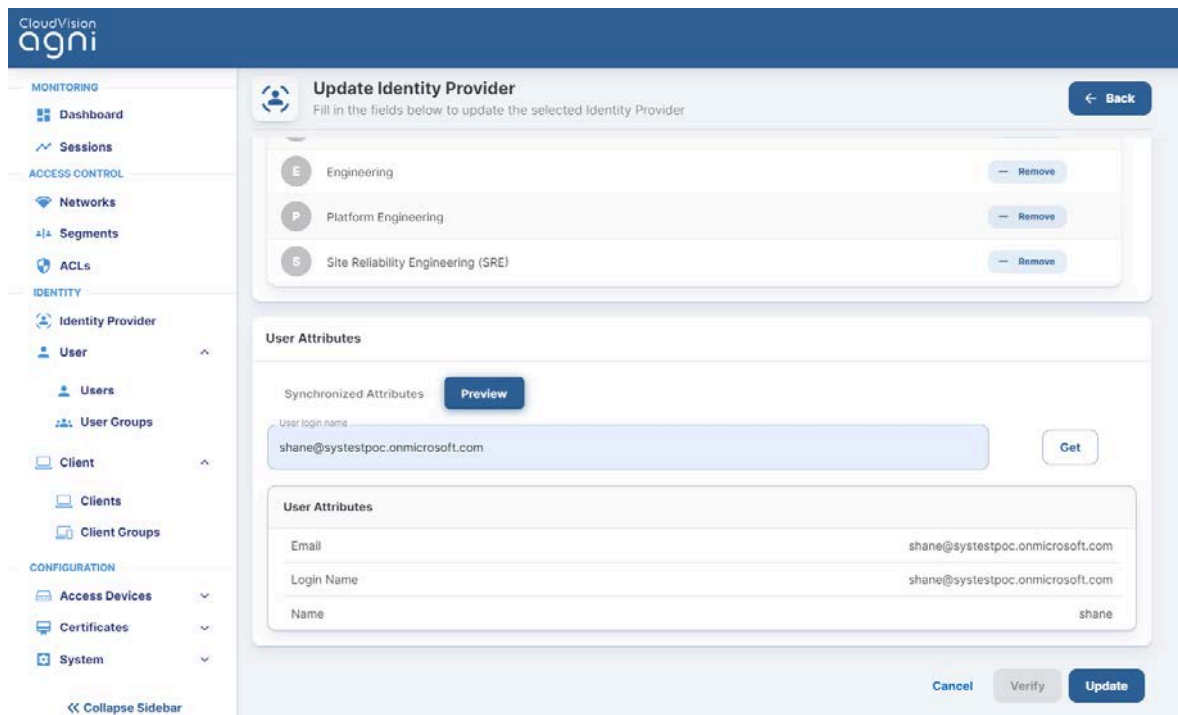


Figure: Identity Provider and User Preview

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' interface in the CloudMason AGNI console. The left sidebar contains navigation links for Monitoring, Access Control, and Identity. The main form area is titled 'Add Identity Provider' and includes a 'Back' button. The form fields are as follows:

- Name:** One-Login Demo
- Domain Name:** myorg1.com
- Identity Provider:** OneLogin (selected from a dropdown)
- Identity Information:**
 - OIDC Issuer URL:** https://antara.onelogin.com/oidc/2
 - OIDC Client ID:** 1ba71213411e53356u5a545ca7d8227e0387ba65d57413075c044a8f0cd34d8
 - Redirect URI:** https://beta.agni.arista.io/soo/login/oidcback (with a 'Copy' button)
- Identity Information Synchronization:** A toggle switch currently set to 'Disabled'.

At the bottom right, there are three buttons: 'Cancel', 'Verify', and 'Add'.

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).

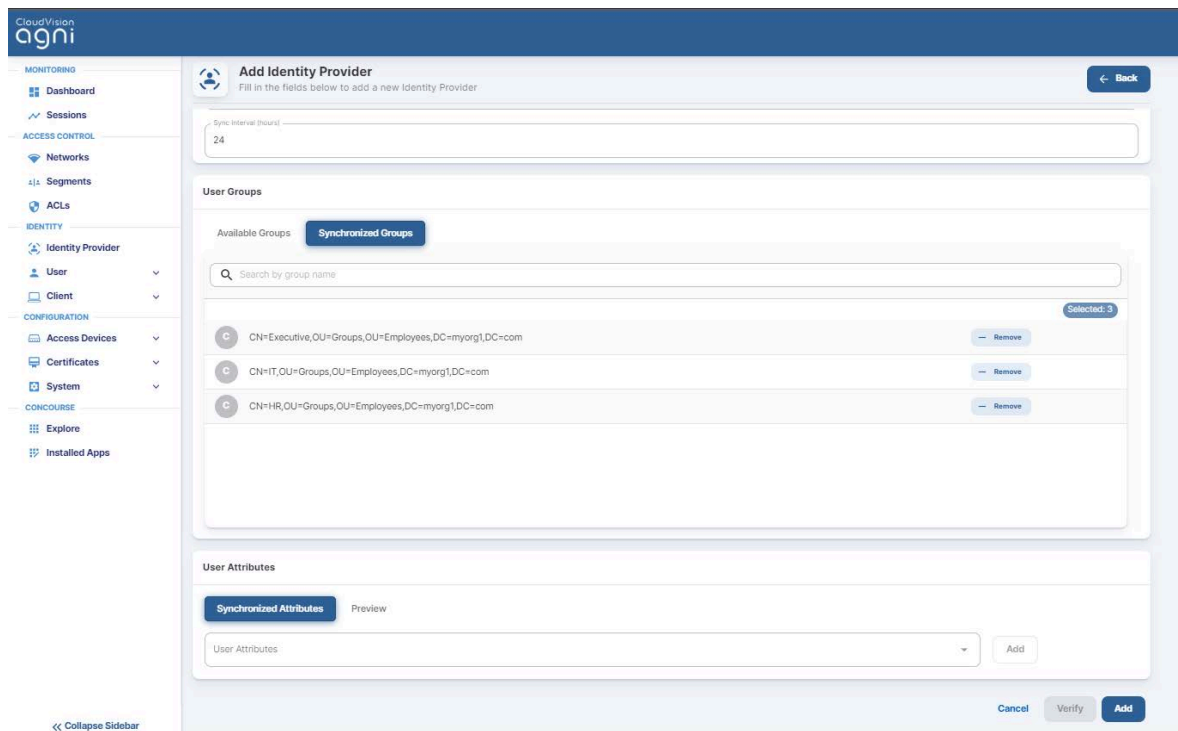


Figure: OneLogin Identity Provider Synchronization

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

The screenshot displays the 'Add Identity Provider' configuration page in the Agni Cloud/Sec interface. The left sidebar contains navigation menus for MONITORING, ACCESS CONTROL, IDENTITY, CONFIGURATION, and CONCOURSE. The main content area is titled 'Add Identity Provider' and includes a 'Back' button. The form contains the following sections:

- Basic Information:**
 - Name: Okta Demo
 - Domain Name: myorg1.com
 - Identity Provider: Okta (selected from a dropdown)
- Identity Information:**
 - OIDC Domain: https://dev-01259439.okta.com/oauth2/default
 - Application Client ID: 00a4ten8gv0fr0qy5c7
 - Redirect URL: https://beta.agni.arista.io/soo/login/callback (with a 'Copy' button)
- Identity Information Synchronization:**
 - Status: Enabled (toggle switch)
 - API Key: [Redacted]
 - Sync Interval (hours): 24

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

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 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 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).

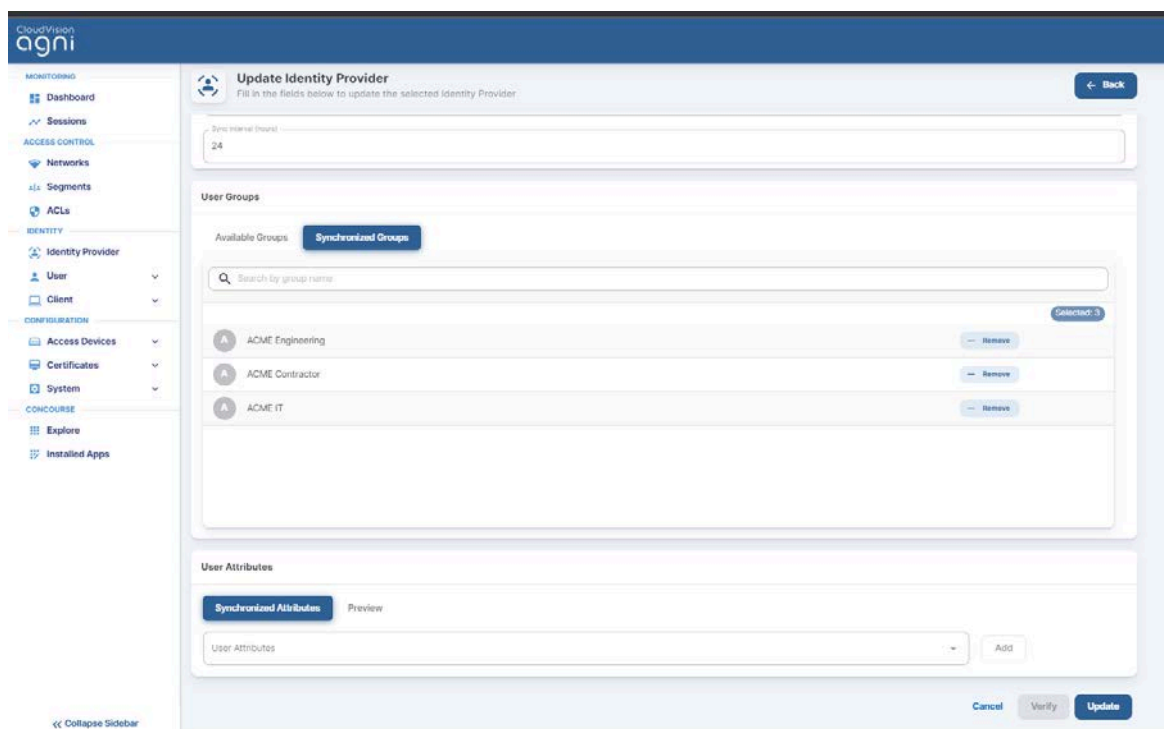


Figure: Okta Identity Provider Synchronization

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 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 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).

CloudVision
agni | Test Org

MONITORING

Dashboard

Sessions

ACCESS CONTROL

Networks

Segments

ACLs

IDENTITY

Identity Provider

User

Client

Clients

Client Groups

CONFIGURATION

Access Devices

Certificates

System

CONCOURSE

Explore

Installed Apps

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

Update Identity Provider

Provide the following details to update the selected Identity Provider

Back

Name

AntaraAI

Domain Name

antaraai.net

Identity Provider

Google Workspace

Identity Information Synchronization

Enabled

Customer ID

003gxmreiv

Account Email

bhagya2@antaraai.net

Upload Service Account Credentials

Update Service Account

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

Sync Interval (hours)

24

Synchronization Details

Last Sync At

8/1/2023 23:32:01

Sync Status

Success

Sync Now

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.

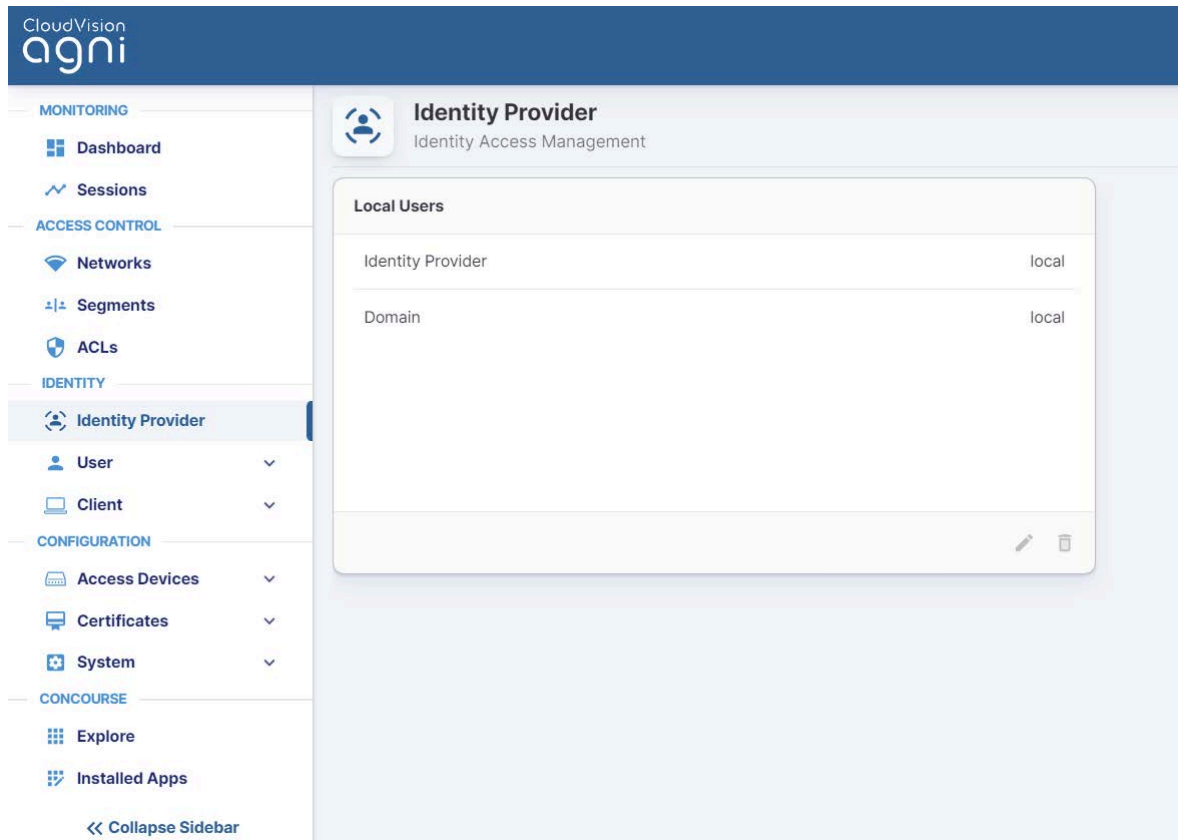


Figure: Local IDP Configurations

Configuring the 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.

Configuring Client Certificate Network

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

Configuration Steps

To configure Networks:

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

The screenshot shows the AGNI configuration interface for a network named 'ACME-CORP'. The interface is divided into a left sidebar with navigation menus and a main configuration area. The sidebar includes sections for MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Certificates, System), and CONOURSE (Explore, Installed Apps). The main configuration area is titled 'ACME-CORP' and contains the following fields and sections:

- Network Name:** A text field containing 'ACME-CORP'.
- Connection Type:** Radio buttons for 'Wireless' (selected) and 'Wired'.
- SSID:** A text field containing 'ACME-Corp'.
- Status:** A toggle switch set to 'Enabled'.
- Authentication:**
 - Authentication Type:** A dropdown menu set to 'Client Certificate (EAP-TLS)'.
 - Domain Machine Authentication:** A toggle switch set to 'Enabled'.
 - Help:** A blue box with a question mark icon and text: 'Enable to allow machine authentication with domain machine certificates.'
- Trust External Certificates:**
 - CRL Verification:** A toggle switch set to 'Enabled'.
 - Help:** A blue box with a question mark icon and text: 'CRL Verification would work only if the Issuer cert has CRL URL added or CRL file uploaded.'
 - OCSP Verification:** A toggle switch set to 'Enabled'.
 - User Identity Binding:** Radio buttons for 'Required' (selected) and 'Optional'.
 - Help:** A blue box with a question mark icon and text: 'Allow authentication only when the certificate has a valid user identity.'

Figure: Wireless EAP-TLS Network

2. Enter the **Network Name** and choose **ConnectionType** as **Wireless**
3. Enter the **SSID** name. Ensure that the name matches the SSID configured in wireless APs.
4. **Status**
 - a. **Enabled** - Enables this network to honor incoming requests.
 - b. **Disabled** - Disables this network.
5. **Authentication** - Set the Type of authentication to the **Client Certificate**. This enables the system to honor EAP-TLS authentication requests.

6. **Domain Machine Authentication** - Enable this setting to process the domain machine authentication (via EAP-TLS) requests if the certificate is issued by an external agency.

Note: AGNI allows you to configure more than one machine domain names when machine authentication is enabled (see image).

The screenshot shows the AGNI configuration interface for a network named 'NSE-CORP'. The interface is titled 'NSE-CORP' and includes a subtitle 'Provide the following details to update the selected Network'. There are 'Back' and menu icons in the top right. The configuration fields include: 'Name' (NSE-CORP), 'Connection Type' (Wireless selected, Wired unselected), 'SSID' (NSE-CORP), and 'Status' (Enabled with a toggle switch). Below these is the 'Authentication' section, which includes 'Authentication Type' (Client Certificate (EAP-TLS)), 'Domain Machine Authentication' (Enabled with a toggle switch), and 'Allowed Machine Domains' (domain.xyz and pepsico.com, both with red 'x' icons). A note at the bottom states 'Optional. Press ENTER after each domain.'

7. Trusted External Certificates

- 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.
- The setting assumes external PKI root and issuer certificates are imported into AGNI.
- User Identity Binding**
 - Required** - When set, the certificate has a valid query-able user identity for request authorizations.
 - 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

- Enable** this setting if using AGNI PKI
- 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.
- Allow Local User Self Registration:**
 - 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 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.

Figure: Wireless EAP-TLS Network User Onboarding

Note: AGNI allows multiple user authentication using AGNI PKI on a shared desktop. That is, on a client device (Mac, Windows, Linux, etc), user A can connect with EAP-TLS network using AGNI PKI certification. After user A logs out, User B can connect using the same method with a new PKI certificate. Subsequently, if User A reconnects to AGNI network, AGNI reattaches the client certificate associated with user A and reconnects to the network.

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 'Test-docs' network configuration page in the CloudVision AGNI interface. The left sidebar contains navigation links for Monitoring, Access Control, Identity, and Configuration. The main content area is divided into sections: General, Authentication, Trust External Certificates, and Onboarding. The 'Onboarding' section is expanded, showing the 'Allow Email Code Login for IDP User' toggle set to 'Enabled'. Below this, there is a dropdown for 'Authorized User Groups' and a text box for the onboarding URL, which is 'https://dev.agnienet.net/onboard/Eb9107b0d-c35f-42e8-ad1f-48f2c39f6686/network/378'. A 'Copy' button is next to the URL. At the bottom right, there are 'Cancel' and 'Update Network' buttons.

Figure: Updating the Network details

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

CloudVision
agni | My Self Service Portal

Sign In

UserID or Email

alan-test-docs@arista.com

Proceed

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

CloudVision
agni | My Self Service Portal

Sign In

UserID or Email

alan-test-docs@arista.com

Use one-time password

SSO Login

6. Check your registered email for OTP details:

Arista Guardian for Network Identity (AGNI)

Hello [redacted] [@arista.com](#)

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

Login using the following details:

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

OTP: yx57xa

The one-time passord (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 'My Self Service Portal' header in yellow. Below it, the 'Verify one-time password' section is displayed. It includes an information box with an 'i' icon and the text 'Check your email for one-time password.' Below this is a text input field labeled 'One-time password' with the value 'yx57xa' entered. A red 'Submit' button is positioned below the input field. At the bottom of the form, there is a red text link that says 'Resend one-time password'.

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

CloudVision
agni | My Self Service Portal

Register Client

Provide the following details to register your client

Description: i's Mac OS X

Register

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.

CloudVision
agni | My Self Service Portal

Register Client

Your client is registered. To connect your client:

1. Click the **Download** button to proceed.
2. A network profile will be downloaded to your device.
3. Go to the **Settings** application.
4. Click **Profile Downloaded**
5. Click **Install** to install the downloaded profile.
6. Now you can connect to the secure network.

Download

Wireless Configuration on Devices

Installing a configuration profile pushes the device identity certificate, the AGNI issuer CA and the AGNI Root CA certificate on the client. The device certificate is signed by the AGNI issuer CA, which in turn is signed by the AGNI Root CA that is self-signed. Hence, profile installation adds the AGNI Root CA to the trusted store on a device.

During the EAP-TLS authentication process, the client device presents the entire chain of certificates to AGNI and because the issuer CA and the root CA are trusted by AGNI, the client authentication succeeds. Similarly, server authentication also succeeds as the client adds the AGNI Root CA to its trusted store.

Apart from the chain of certificates, the configuration profile also pushes the WiFi network details (i.e SSID name, encryption, and EAP method) to the device.

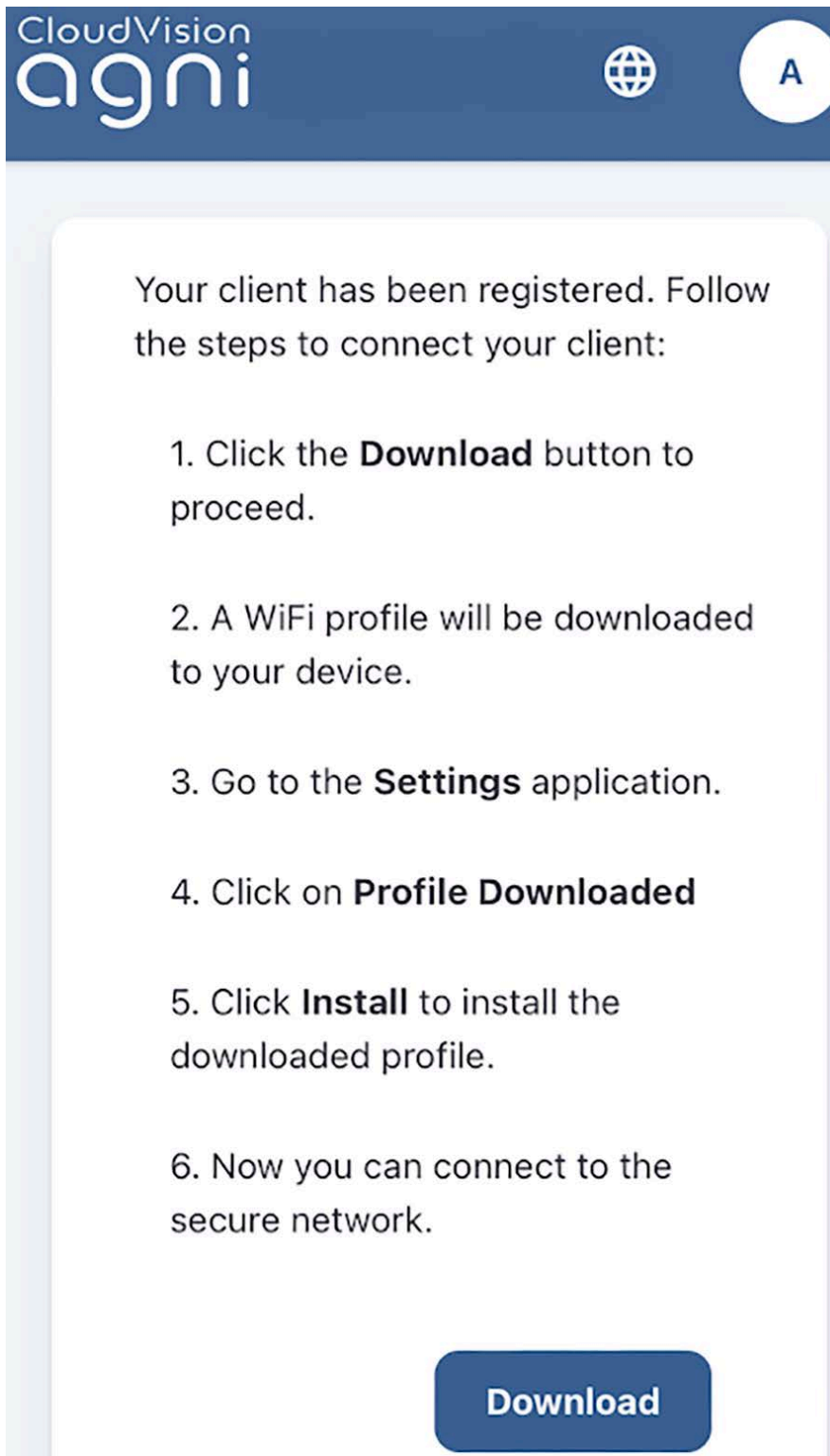
The profile installation process varies based on the client device operating system. AGNI supports the following devices and the instructions are provided:

- iPhone
- MacBook
- Android
- Windows
- Chromebook

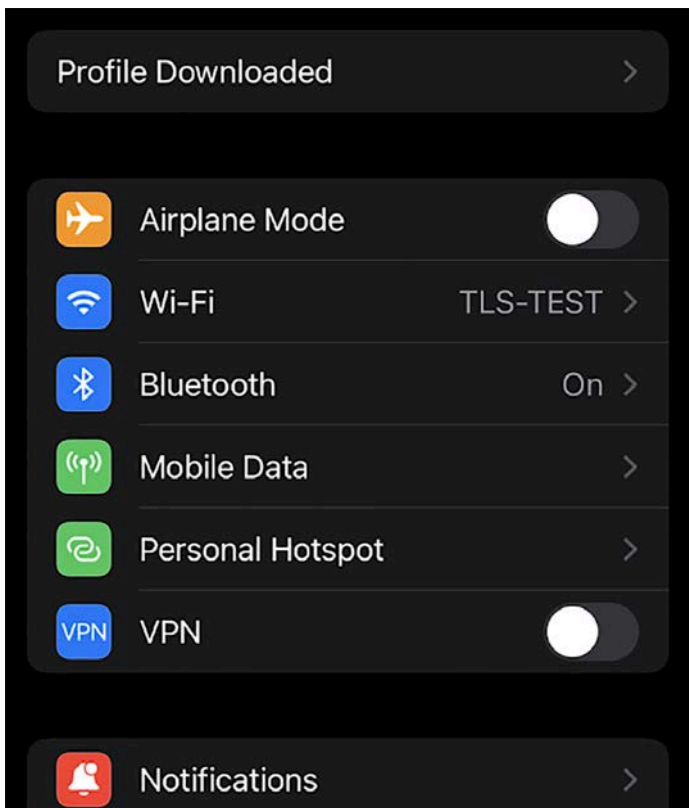
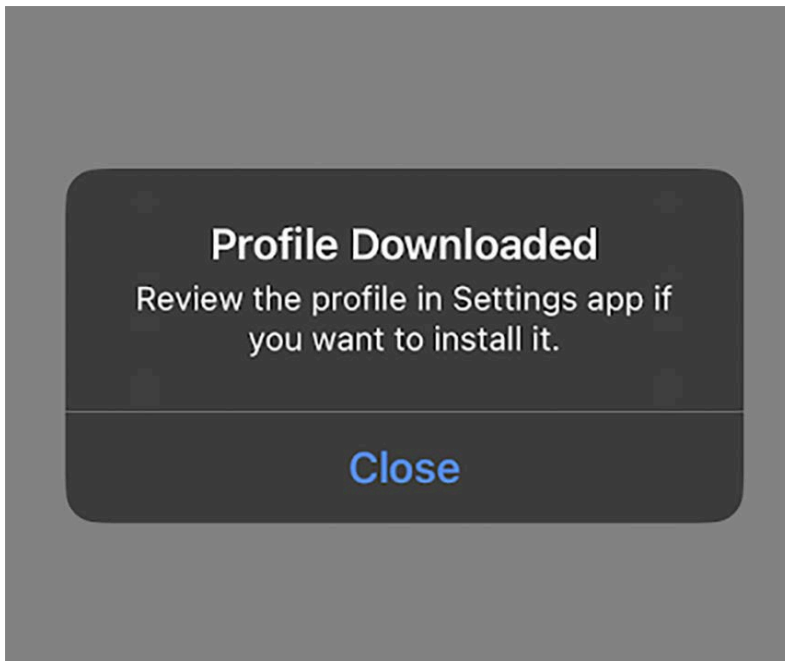
iPhone Configuration

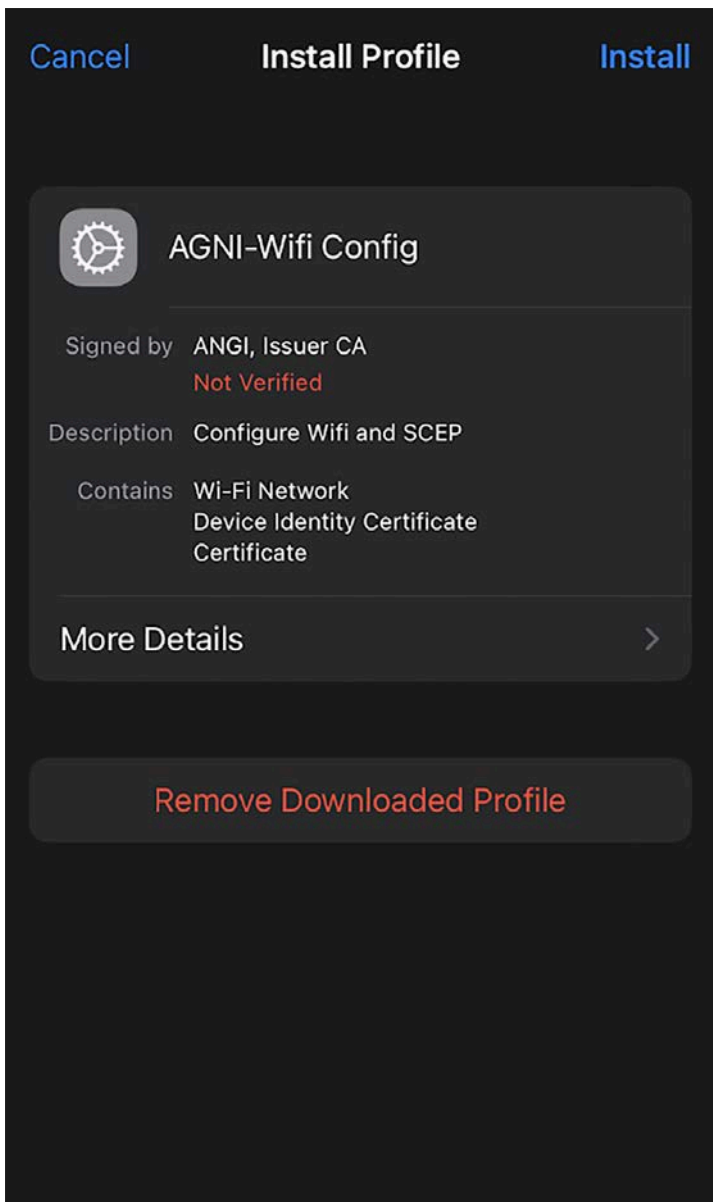
To configure AGNI on an iPhone:

1. Click the register button to get redirected to the page from where you can download the Wireless configuration profile.



2. Click the **Download** button to download the configuration profile, which is available in the settings page for review and installation.



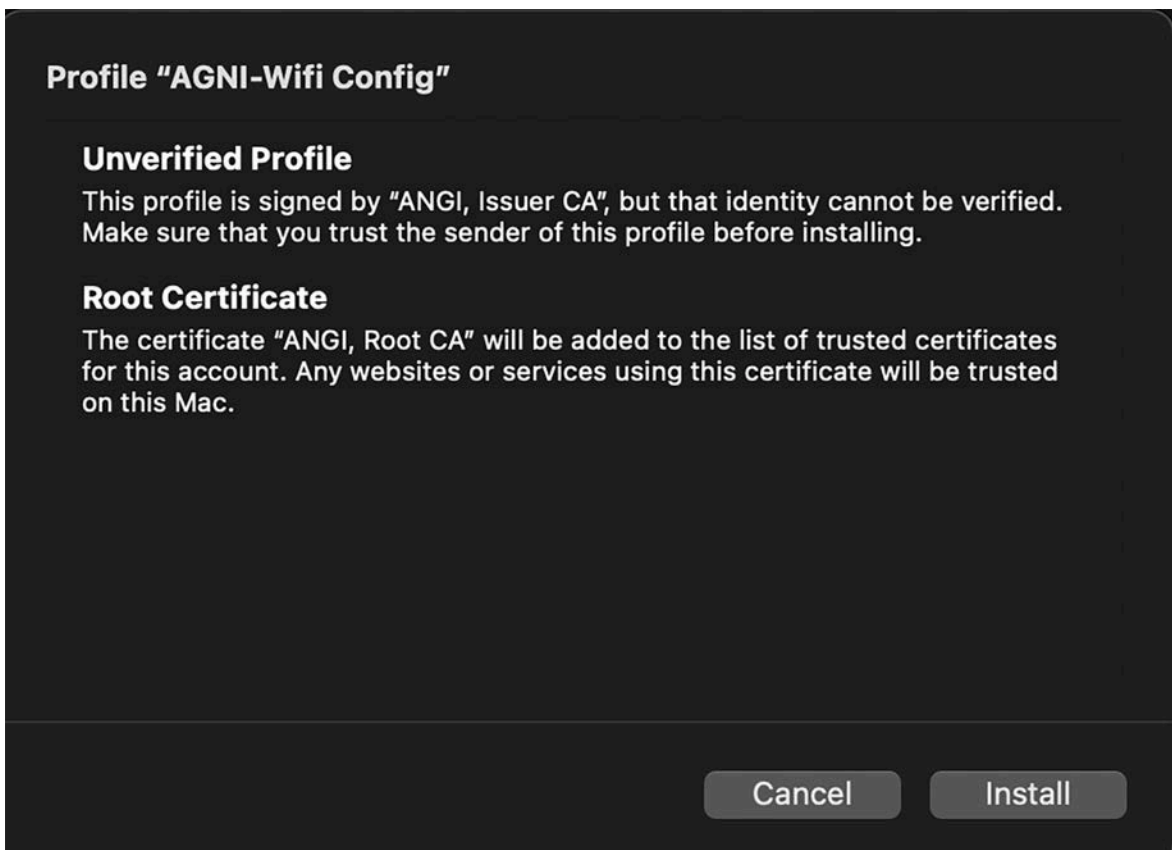
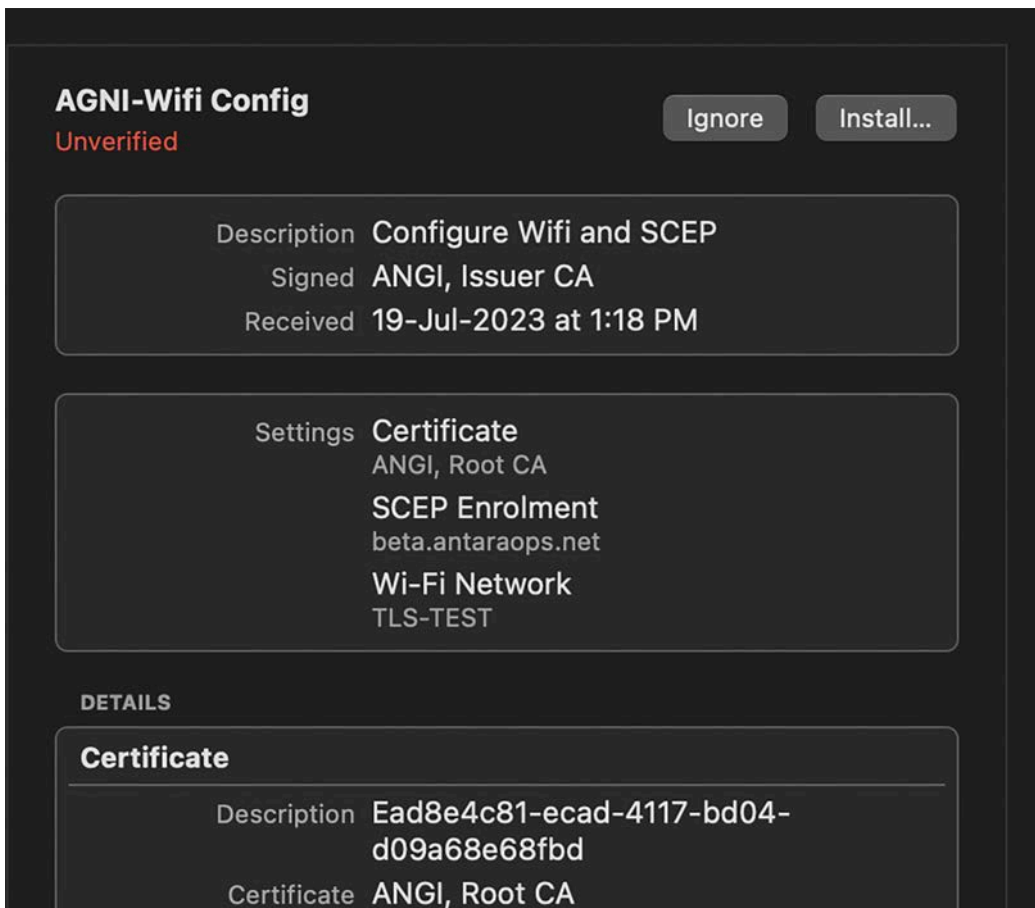


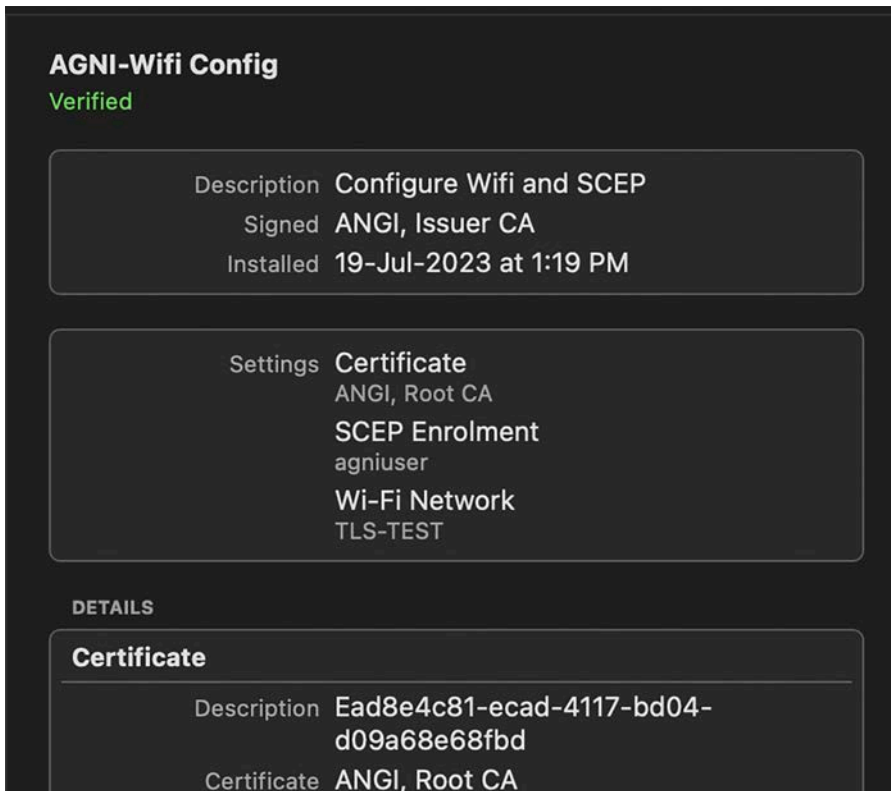
3. After the profile is installed, the device automatically connects to the network in range.

MacBook Configuration

The configuration process on the MacBook is similar to the iPhone. To configure:

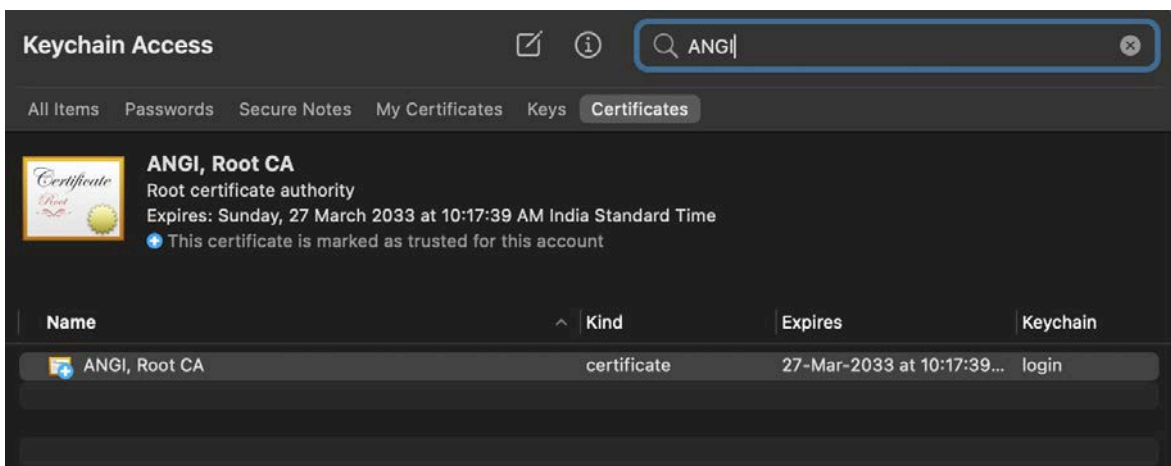
1. Click the **Register** button, the device gets redirected to the page from where you can download the Wireless configuration profile.
2. Open the downloaded configuration file. The profile will be available in **System Preferences -> Profiles** for review and installation.





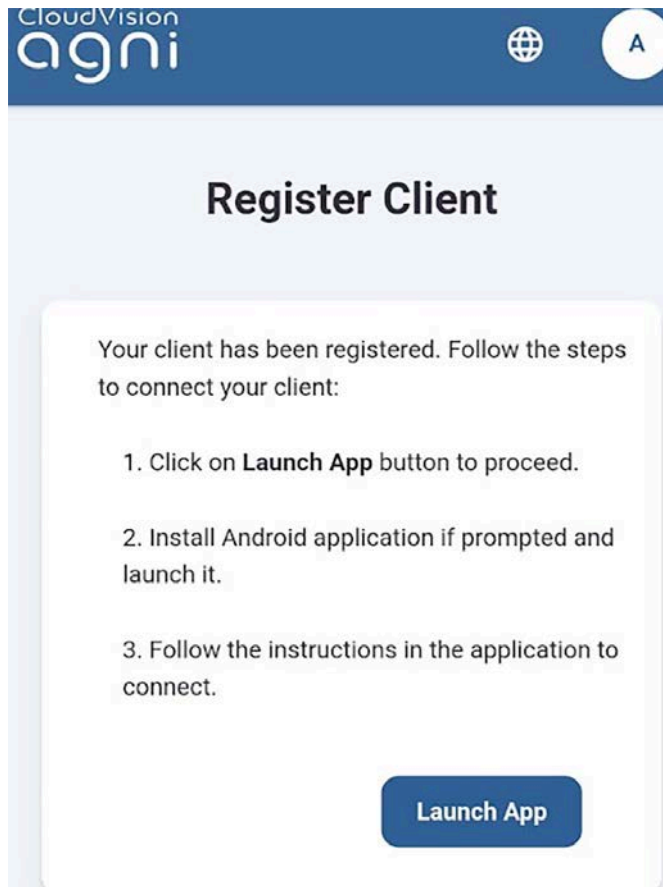
- Once the profile is installed, the device automatically connects to the network in range.

For further verification on the RootCA installation, us the KeyChain Access application.



Android Configuration

- For android devices, the wireless configuration profile is pushed via the AGNI Onboard application, which is available on Google Play Store.
After client registers, the user is prompted to launch the application:



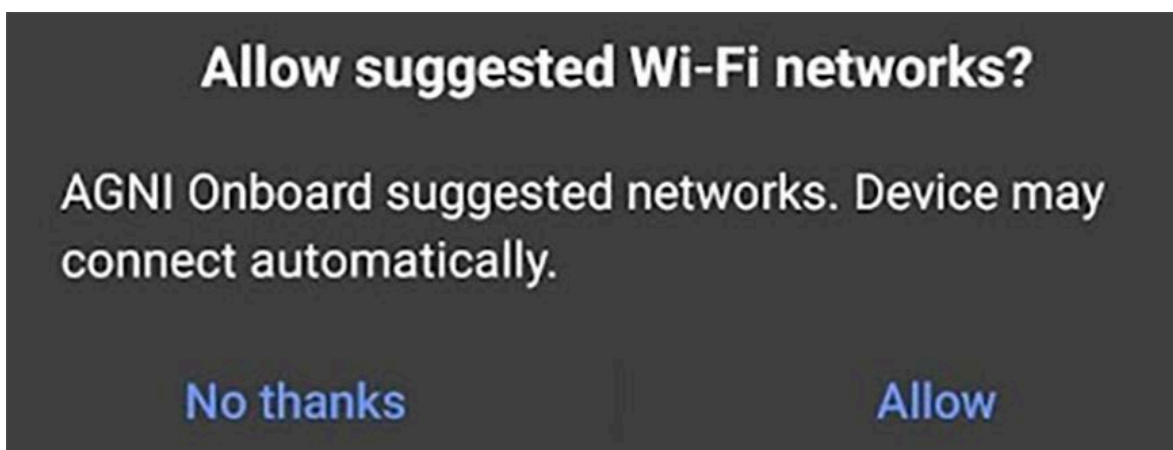
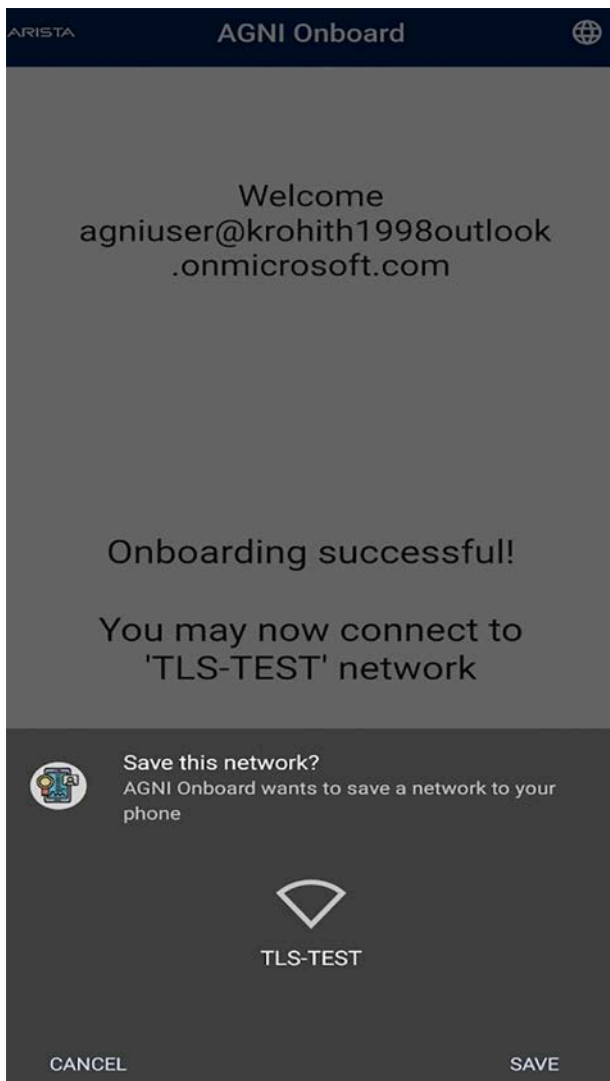
- Click the Start button on this application to install the profile. The user is then to save the network settings after which the user can connect to the SSID.



Welcome
agniuser@krohith1998outlook
.onmicrosoft.com

Onboard your client
to connect to
'TLS-TEST' network



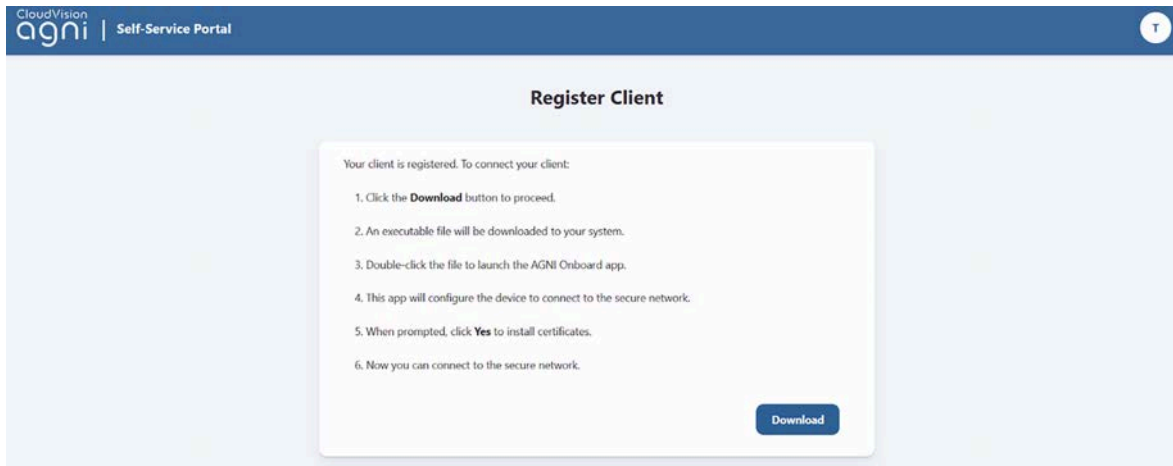


After the application is allowed to suggest networks, the device automatically connects to the network in range.

Windows Configuration

Similar to android clients, the wireless configuration profile for windows clients is pushed via an AGNI onboard application. The application is available as an executable file (.exe) as part of the client onboarding process.

- You can download this .exe file once the client is registered on the self service portal.



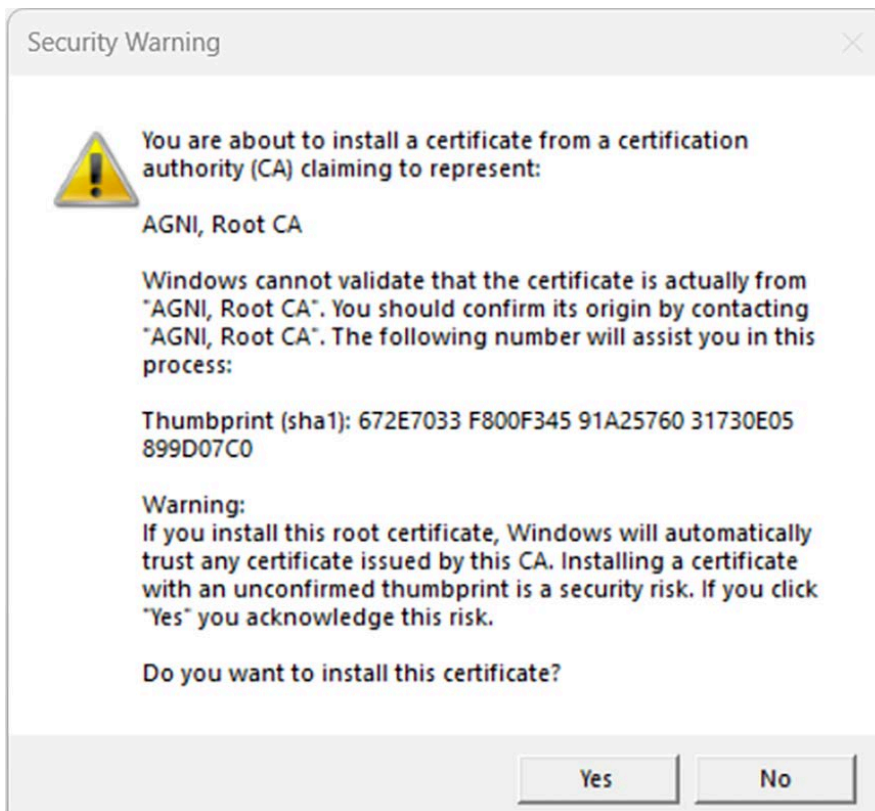
- After you run the exe file as an administrator, click the **Start** button to install the the profile. During the profile installation, the AGNI Root CA certificate is installed in the device's trusted certificate store.



Welcome
test@test.com

Onboard your client
to connect to
'ssid-test' network

Start



- After the profile is installed the device connects to the EAP-TLS network.



Welcome
test@testuser.com

Onboarding successful.

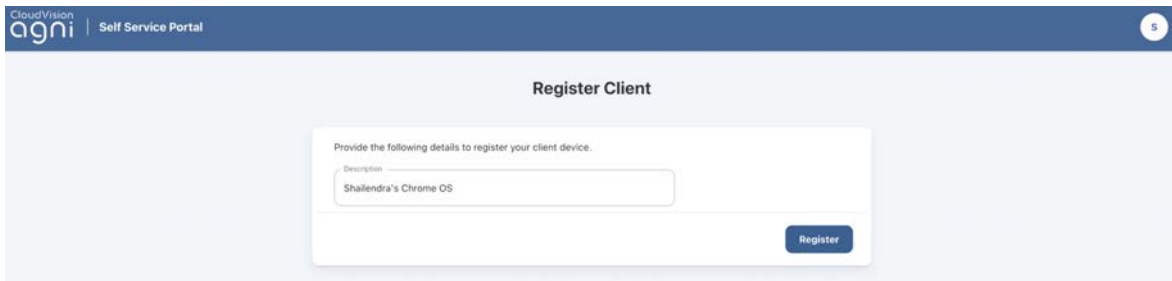
You may now connect to
'ssid-test' network

Close

Chromebook Configuration

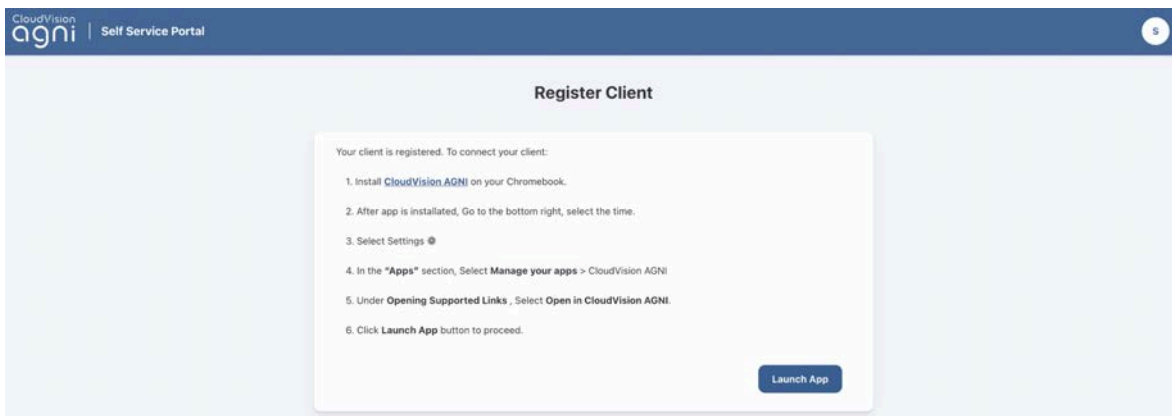
As an admin, use the self-service portal to onboard the Chromebook OS clients. To configure Chromebook:

- Login to Chromebook and navigate to the browser.
- Open the AGNI onboarding URL in the browser. You are redirected to the Self-Service Portal.



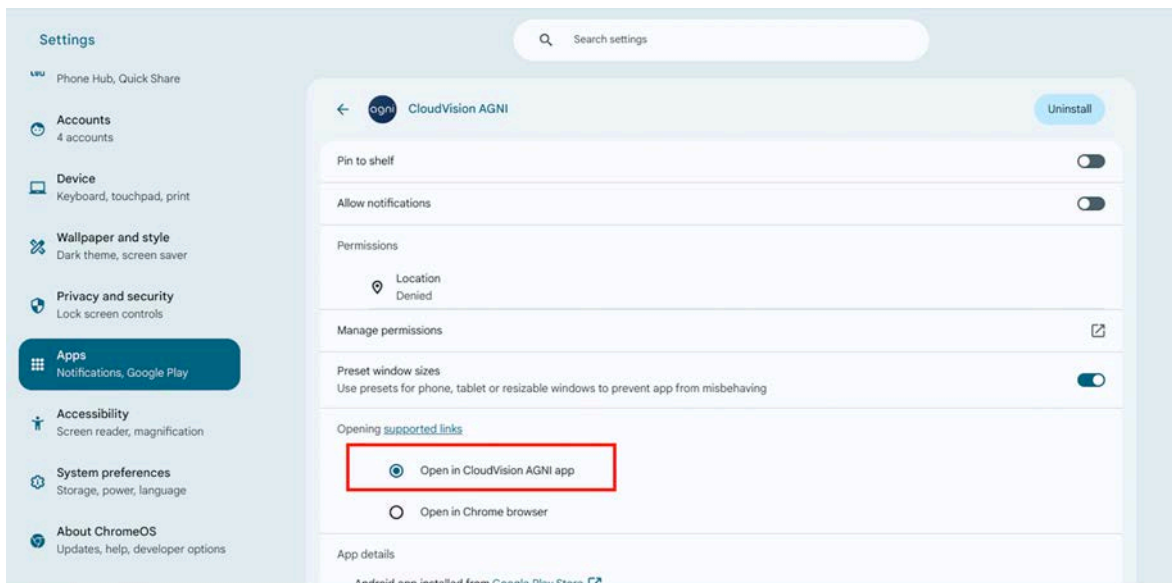
The screenshot shows the 'Register Client' page of the CloudVision AGNI Self Service Portal. The page has a blue header with the 'CloudVision agni' logo and 'Self Service Portal' text. A white card in the center contains the text 'Provide the following details to register your client device.' Below this is a text input field labeled 'Description' with the value 'Shallendra's Chrome OS'. A blue 'Register' button is at the bottom right of the card.

- Click the **Register** button. After successful login, the user receives a set of instructions to download the Cloud Vision AGNI application. Follow the instructions.

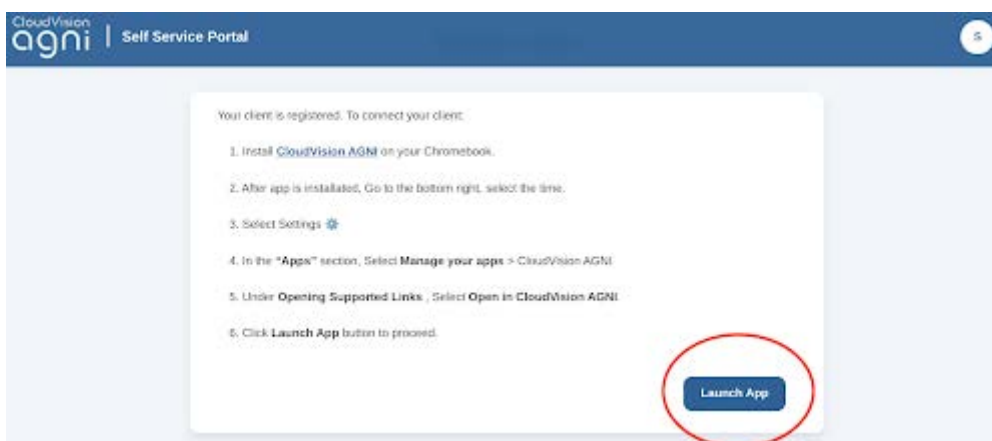


The screenshot shows the 'Register Client' page after a successful registration. The page has a blue header with the 'CloudVision agni' logo and 'Self Service Portal' text. A white card in the center contains the text 'Your client is registered. To connect your client:' followed by a numbered list of six steps: 1. Install CloudVision AGNI on your Chromebook. 2. After app is installed, Go to the bottom right, select the time. 3. Select Settings @. 4. In the "Apps" section, Select Manage your apps > CloudVision AGNI. 5. Under Opening Supported Links , Select Open in CloudVision AGNI. 6. Click Launch App button to proceed. A blue 'Launch App' button is at the bottom right of the card.

- Download the AGNI Onboarding application from the play store.
- Click the **Settings** from the bottom right options and navigate to **Apps > Manage Apps**.
- Select the AGNI application and open the settings.
- Select the **Open in CloudVision AGNI app** from the Opening supported links.



- Click the **Launch App** button from the Self Service Portal.



- The CloudVision AGNI application is displayed and proceeds with the rest of the configuration.



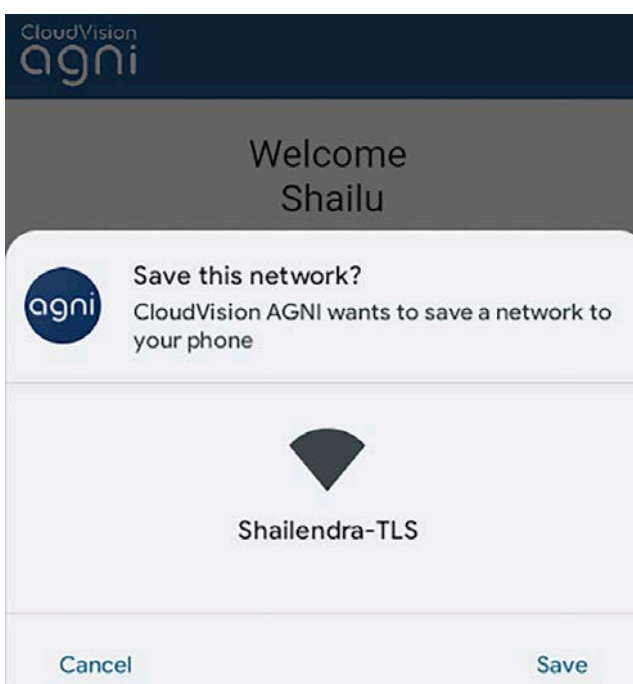
Welcome
Shailu

Onboard your client
to connect to
'Shailendra-TLS' network

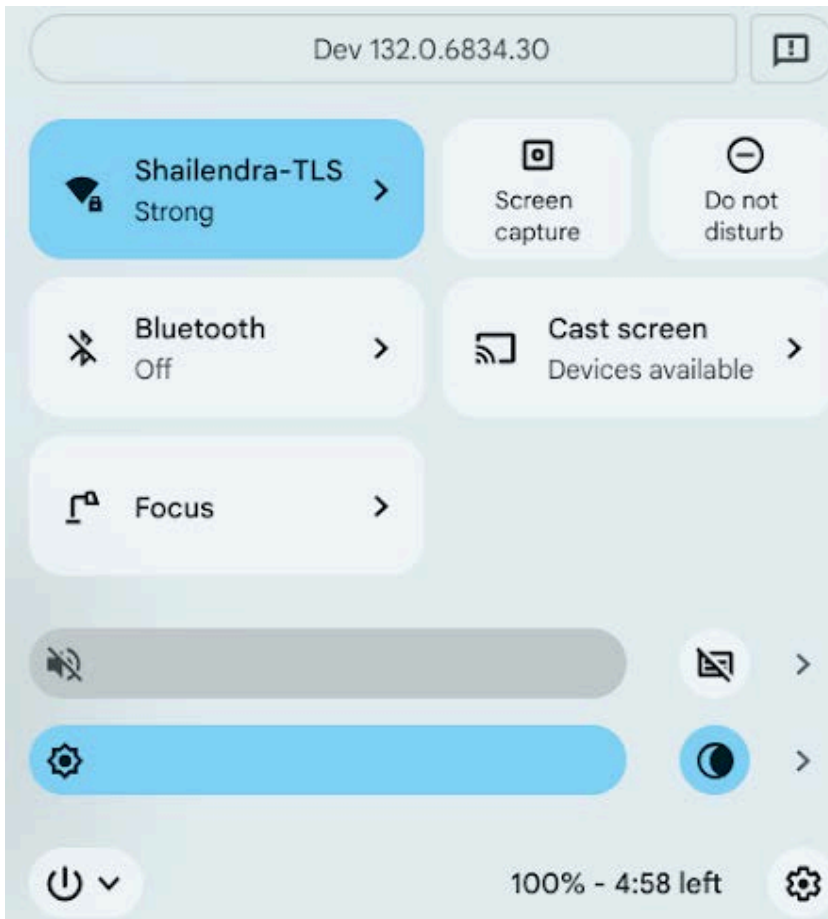
Start

App Version 1.0.4

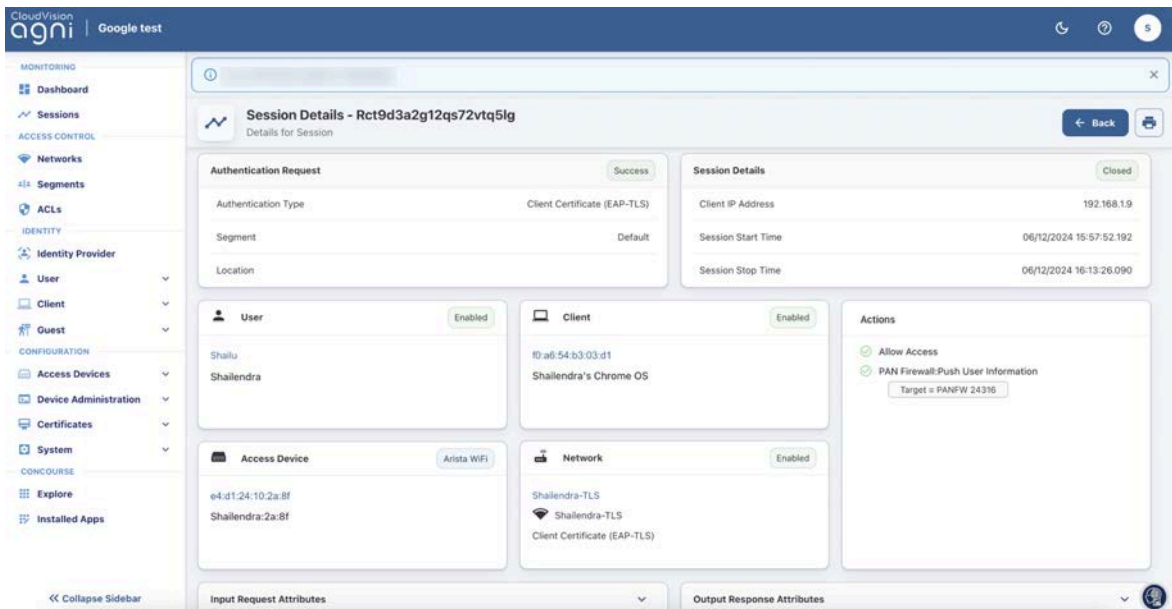
- Allow the application to configure the wireless profile and install certificates.



- The network profile gets installed with the required certificates.



- The client is displayed in the session list in AGNI.



Configuring Unique PSK (UPSK) Network

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

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 in Step 7c below).

Configuring the UPSK Settings

To configure the :

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

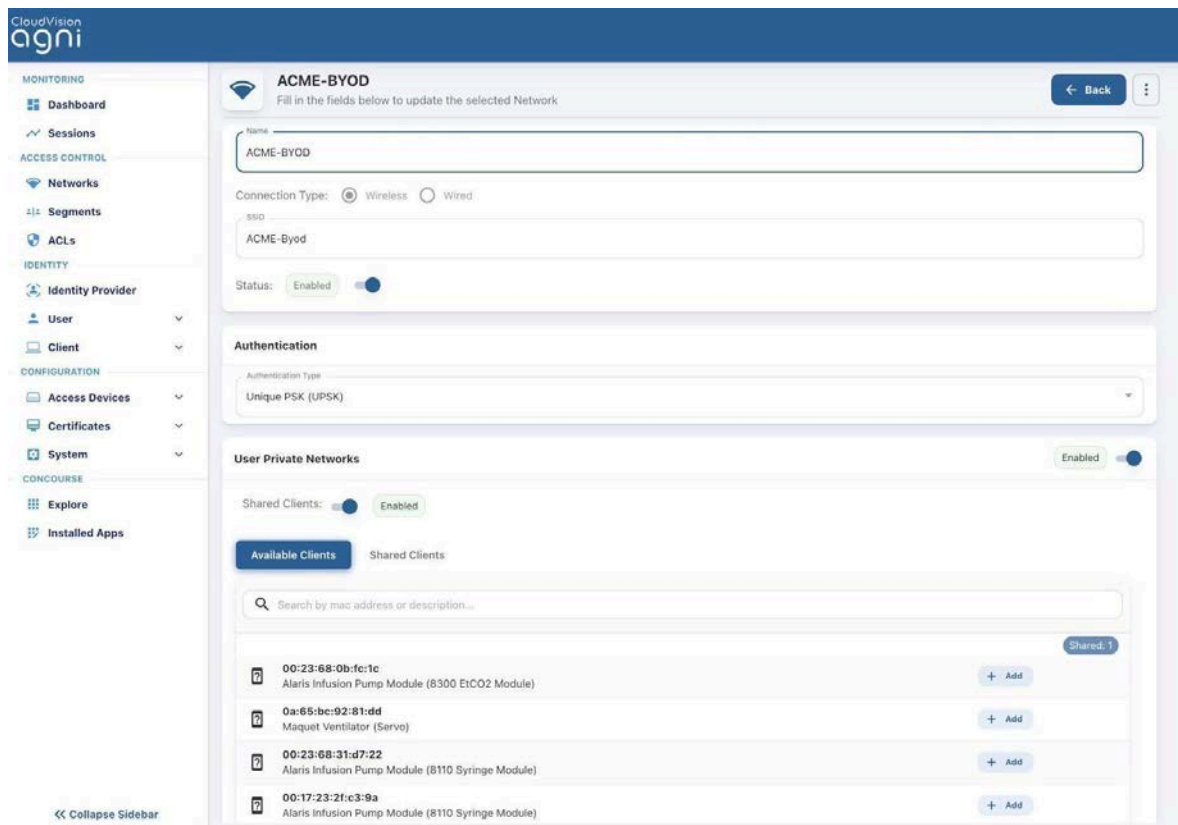


Figure: Configuring Wireless UPSK Network

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.

Figure: Wireless UPSK Network User Onboarding

8. Click on the **Add Network** button. The process:
 - a. Creates the network
 - b. 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.
 - c. 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) and UPSK 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).

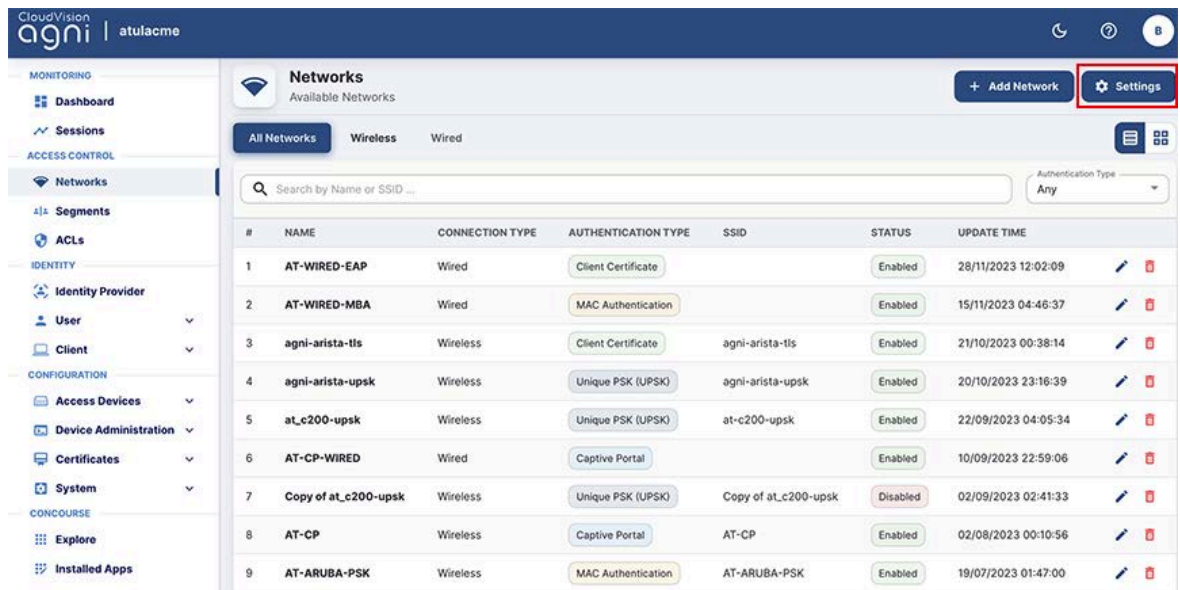


Figure: List of Networks Page

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

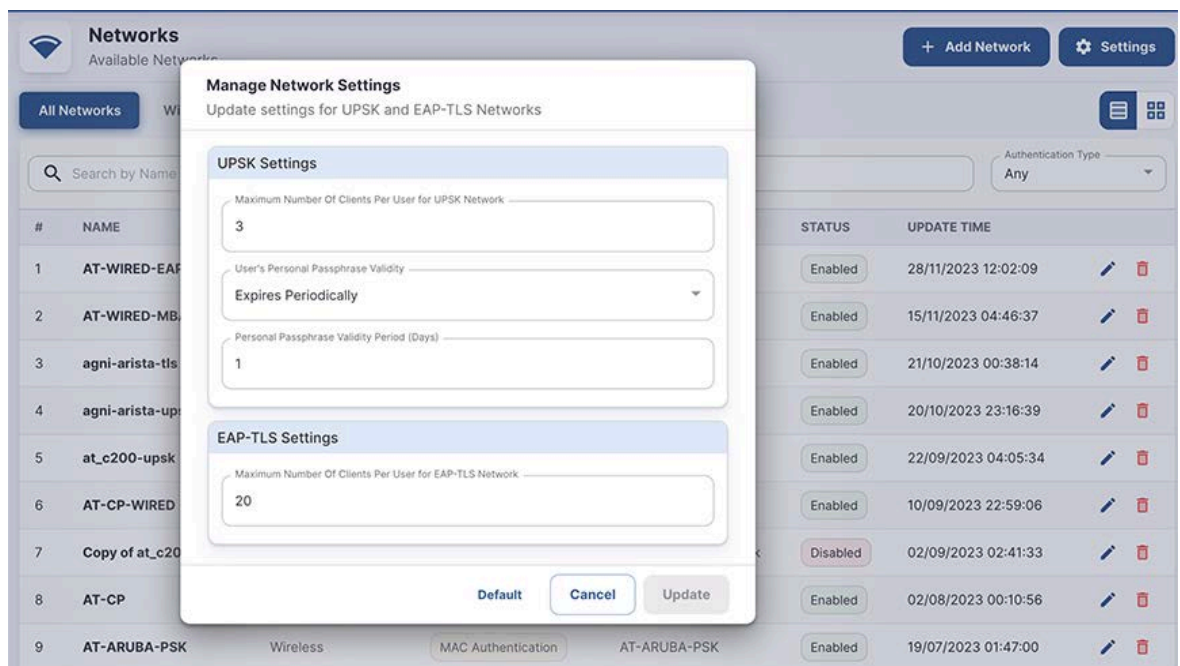


Figure: Manage Network Settings

- 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:

CloudVision
agni | Self Service Portal

Register Client

Provide the following details to register your client

Description
Bob Smith's Mac OS X

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

Register

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.

Configuring Wireless Captive Portal Network

Captive Portal provides network access based on the authentication mechanism through the web browsers. The credentials are either validated locally (for local users) or via SSO (for 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).

Configuration Steps

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.

CloudVision
agni

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client

CONFIGURATION

- Access Devices
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

ACME-Guest
Fill in the fields below to update the selected Network.

Name: ACME-Guest

Connection Type: ☒ Wireless ☐ Wired

SSID: ACME-Guest

Status: Enabled

Authentication

Authentication Type: Captive Portal

User Type: ☒ Organizational user ☐ Guest user

Captive Portal

Initial Role for Portal Authentication: agni-guest [Show Domains](#)

Authorized User Groups:

Re-Authenticate Registered Clients: Periodic

Re-Authentication Period (days): 1

Figure: Wireless Captive Portal Network-page-1

CloudVision
agni

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

- Identity Provider
- User
- Client

CONFIGURATION

- Access Devices
- Certificates
- System

ACME-Guest
Fill in the fields below to update the selected Network.

Name: ACME-Guest

Status: Enabled

Authentication

Authentication Type: Captive Portal

User Type: ☐ Organizational user ☒ Guest user

Guest portal:

Default Portal: ASU-GUEST-2023-01-31_12-01-17

Figure: Wireless Captive Portal Network-page2

10. Click on the **Add Network** button. The process:

- Creates the network.
- Creates an **Onboarding URL**, which should be set as a captive portal URL in the WiFi configuration of your AP. Clients are redirected to this URL for onboarding.

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

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

Cancel Update Network

Figure: Wireless Captive Portal Network Onboarding

Configuring Wireless MAC Authentication Network

Wireless network configuration enables you to authenticate end clients connected to the network through client MAC addresses. This helps clients 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 Steps

To configure:

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 for the previously onboarded clients is rejected.

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

The screenshot displays the CloudVision AGNI web interface for configuring a network. The left sidebar shows a navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Client), CONFIGURATION (Access Devices, Certificates, System), and CONFORMANCE (Explore, Installed Apps). The main content area is titled 'ACME-MACAUTH' and includes a 'Back' button. The configuration fields are as follows:

- Name:** ACME-MACAUTH
- Connection Type:** ☒ Wireless, ☐ Wired
- SSID:** ACME-MacAuth
- Status:** Enabled (toggle switch)
- Authentication:**
 - Authentication Type:** MAC Authentication
- MAC Authentication Settings:**
 - MAC Authentication Type:** Allow Registered Clients and Authorized OUIs
 - Disallow user associated clients:** Enabled (toggle switch)
 - Enable to disallow user associated clients on this network.** (Info icon)
 - Authorized OUIs:** A text input field with an 'Add' button.
 - Selected Authorized OUIs:** A list showing '00052A' and '00052B' with red 'X' icons.
 - Add New Clients To Group:** A dropdown menu showing 'IOT-Segment'.

Figure: Wireless MAC Authentication Network

Configuring Wired 802.1X Network

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 Steps

1. Navigate to **Access Control** → **Networks**. Click 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.

Figure: Add Network (Authentication)

6. Trust External Certificates:

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

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.
- c. **CRL Verification** - Select this option to verify the certificate revocation through CRLs.
- d. **OCSP Verification** - Select this option to verify the certificate

revocation through OCSP.

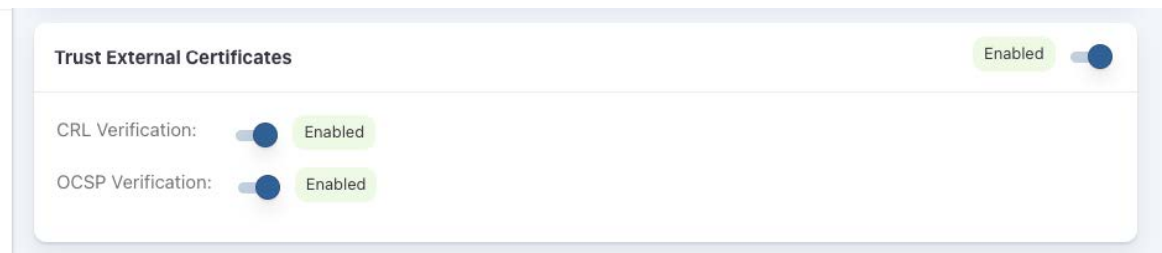


Figure: Add Network (Trusted External Certificates)

7. Fallback to MAC Authentication

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

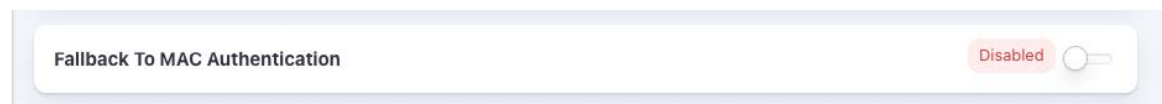


Figure: Add Network (Fallback To MAC Authentication)

- 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.

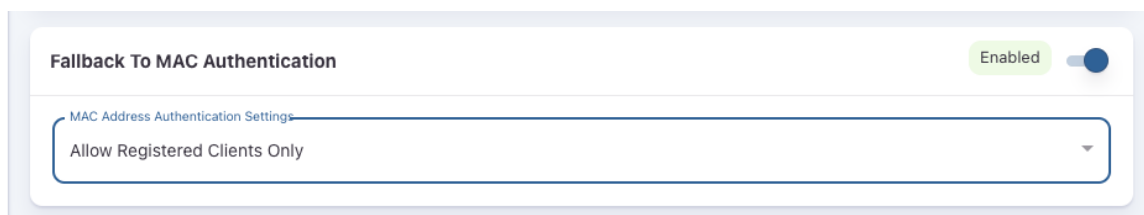


Figure: Add Network (Fallback to MAC Authentication)

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 displays the 'Add Network' configuration interface in the CloudVision AGNI Test Org. The interface is divided into a left sidebar and a main configuration area. The sidebar contains a navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Users, User Groups), CONFIGURATION (Access Devices, Certificates, System), and CONCOURSE (Explore, Installed Apps). The main configuration area is titled 'Add Network' and includes a 'Back' button. It contains several sections: 'Status' (Enabled), 'Authentication' (Authentication Type: Client Certificate (EAP-TLS), Domain Machine Authentication: Enabled), 'Trust External Certificates' (Disabled), 'Fallback To MAC Authentication' (Enabled), and 'Onboarding' (Disabled). Each section has a toggle switch and a description. At the bottom right, there are 'Cancel' and 'Add Network' buttons.

Figure: Sample Wired 802.1X configuration

Configuring Wired MAC Authentication Network

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 Steps

- Navigate to **Access Control** → **Networks**. Click on the **Add Networks** button.
- Enter the **Network Name** and choose **ConnectionType** as Wired
- 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 image shows a web interface titled "MAC Authentication Settings". It features a dropdown menu labeled "MAC Authentication Type" with "Allow All Clients" selected. Below this is a text input field labeled "Add New Clients To Group" with a dropdown arrow and a plus icon on the 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 image shows the "MAC Authentication Settings" interface. The "MAC Authentication Type" dropdown is set to "Allow Registered Clients Only". Below it, the "Disallow user associated clients:" toggle is turned on, with the label "Enabled". At the bottom, there is a light blue information box with an 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.



MAC Address Authentication Settings

MAC Address Authentication Settings

Allow Authorized OUIs Only

Authorized OUIs

Add

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

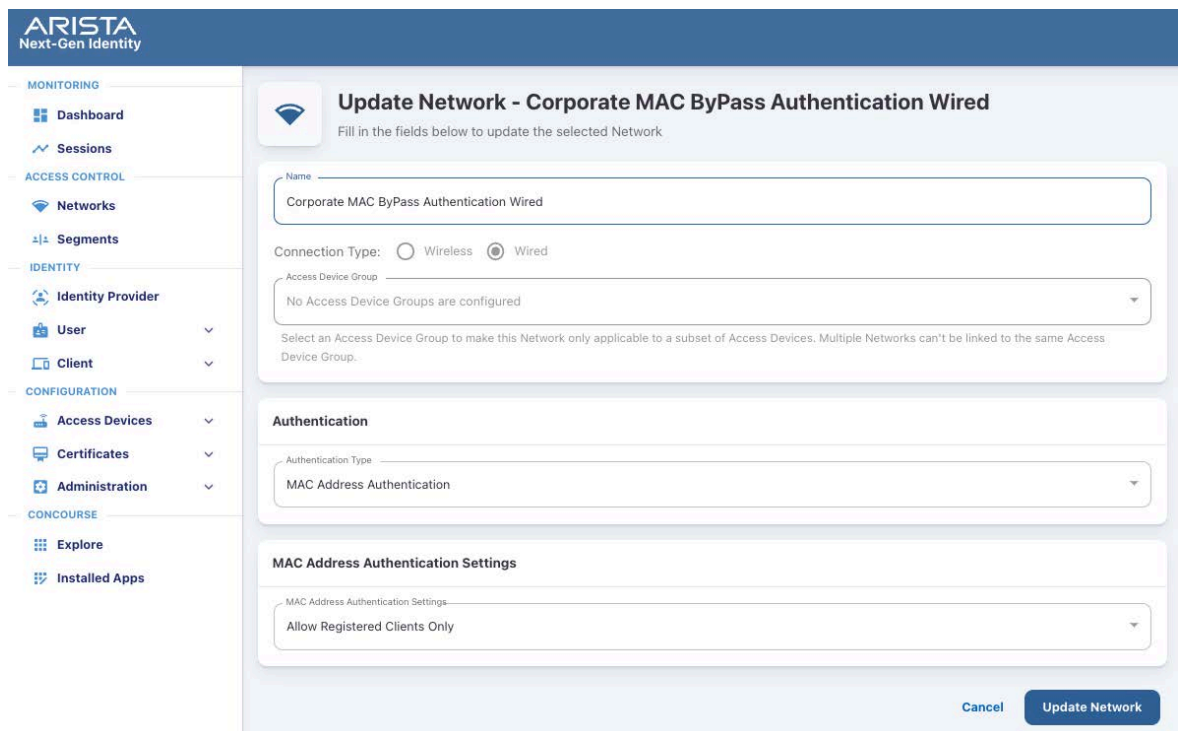
Selected Authorized OUIs

00052A 00052D

Add New Clients To Group

Figure: Add Network (Authorized OUIs)

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



ARISTA
Next-Gen Identity

Update Network - Corporate MAC ByPass Authentication Wired
Fill in the fields below to update the selected Network

Name
Corporate MAC ByPass Authentication Wired

Connection Type: ☐ Wireless ☒ Wired

Access Device Group
No Access Device Groups are configured

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

Authentication

Authentication Type
MAC Address Authentication

MAC Address Authentication Settings

MAC Address Authentication Settings
Allow Registered Clients Only

Cancel Update Network

Figure: MAC ByPass Authentication Configuration

Configuring Wired Captive Portal Network

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 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.

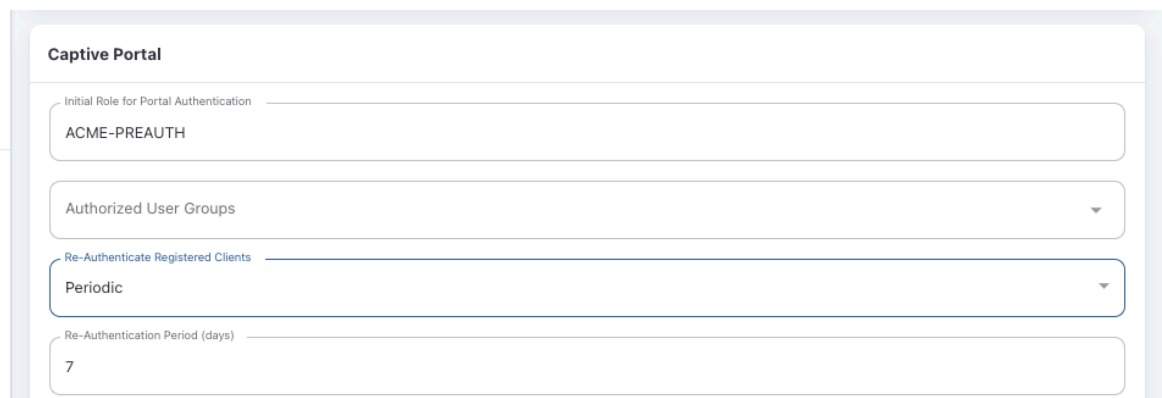
Configuration Steps

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.



The screenshot shows the 'Captive Portal' configuration page. It includes a text input for 'Initial ACL For Portal Authentication' with the value 'guest-acl' and a 'Show Domains' button. Below is a dropdown for 'Re-Authenticate Clients' set to 'Always'. A light blue informational box states: 'Configure the following URL as captive portal in the initial role, to allow users sign in.' Below this is a text input containing the URL 'https://qa.agnieng.net/guestPortal/Eba61d189-e361-4837-a116-182575420cfb/network/136' and a 'Copy' button.

Figure: Captive Portal



This screenshot shows the 'Captive Portal' configuration page with different settings. The 'Initial Role for Portal Authentication' is set to 'ACME-PREAUTH'. The 'Authorized User Groups' dropdown is empty. The 'Re-Authenticate Registered Clients' dropdown is set to 'Periodic'. The 'Re-Authentication Period (days)' is set to '7'.

Figure: Captive Portal (Re-authentication Option Periodic)

5. Click the **Add the network** button. The process generates a Captive Portal

URL, which should be specified in the switch ACL.



Figure: Captive Portal URL

Configuring Guest Portal Network

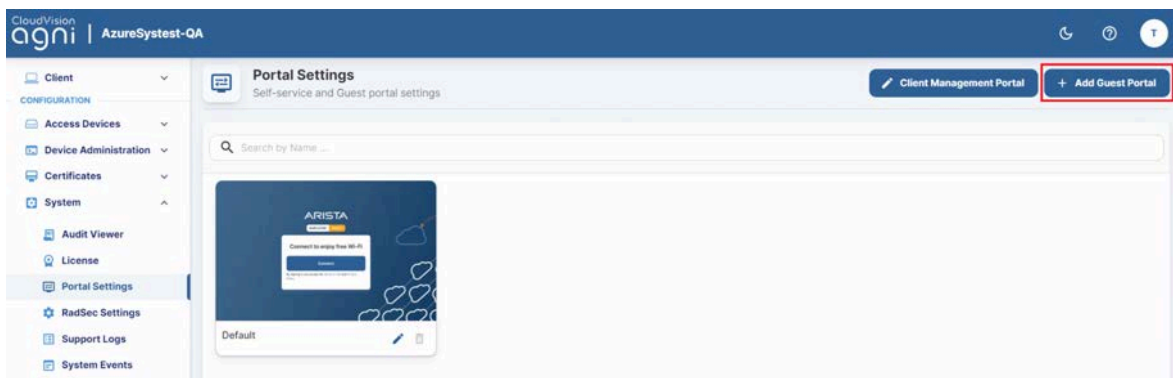
This section describes the steps to configure the guest portal using AGNI for wired clients. To configure the guest portal, you must configure AGNI and the switch.

Configuring AGNI

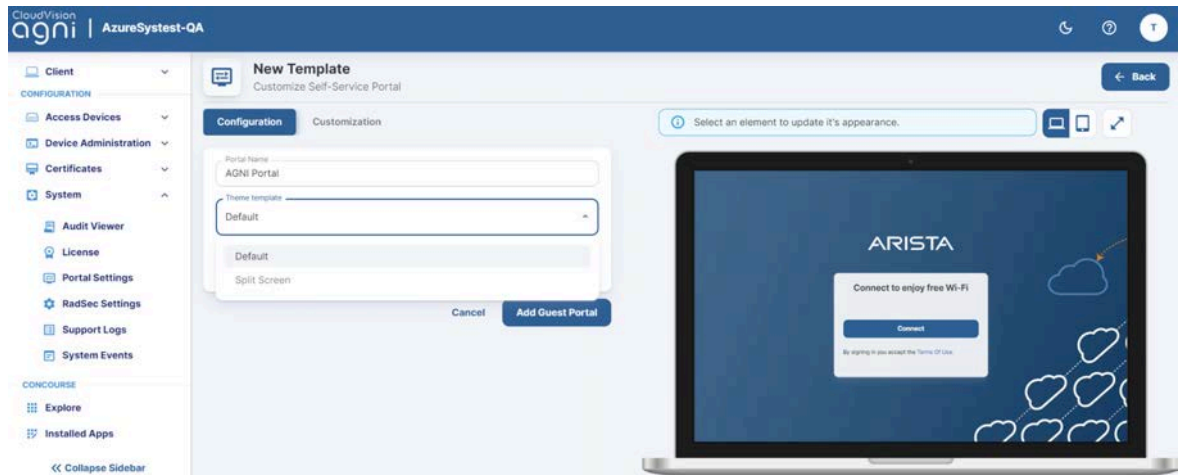
1. Log in to AGNI and navigate to **Identity > Guest > Portals**.



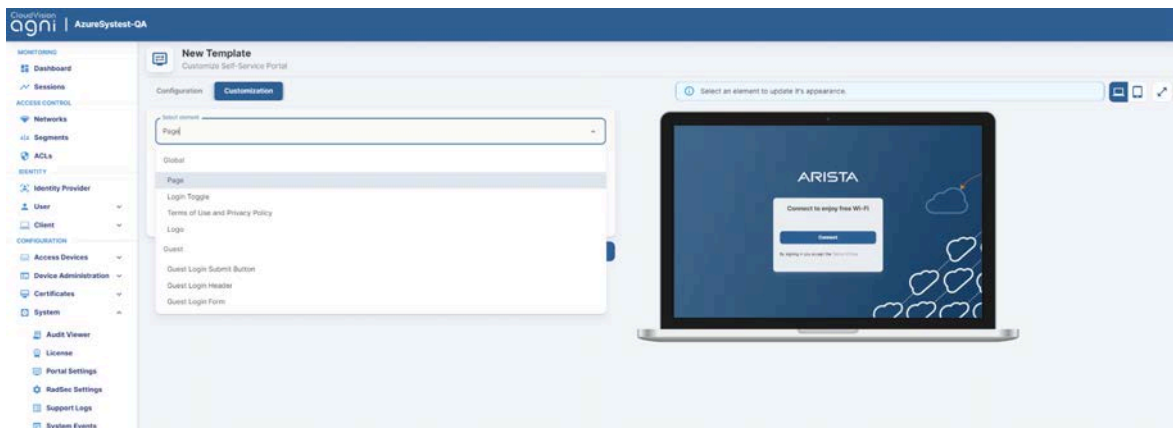
2. Click the **Add Guest Portal** button.



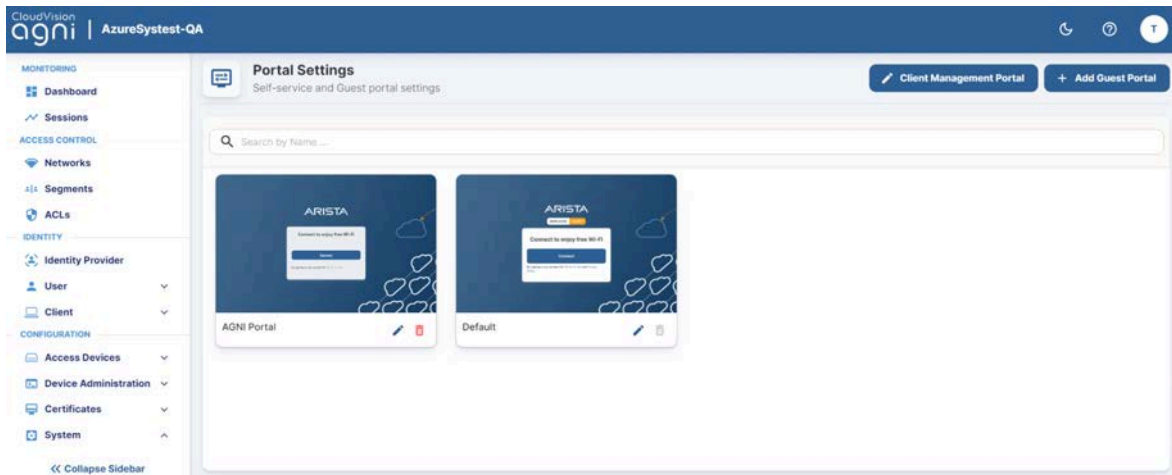
3. In the **Configuration** tab, provide the portal name and select the theme of the portal. The available theme options are Default or Split Screen.



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



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



Now,

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

ACME-wired-guest

Provide the following details to update the selected Network

← Back

Name: ACME-wired-guest

Connection Type: ☐ Wireless ☒ Wired

Access Device Group: Guest Switch


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

Status: Enabled

Authentication

Authentication Type: Captive Portal

Captive portal type: ☒ Internal ☐ External


ACME-wired-guest
Provide the following details to update the selected Network
← Back
⋮

Captive portal type: ☒ Internal ☐ External
Select internal portal: Default ▼ Preview

Captive Portal

Initial ACL For Portal Authentication: guest-acl Show Domains

Authorized User Groups: ▼
Applicable for organizational users only

Re-Authenticate Clients: Periodic ▼

Re-Authentication Period (days): 1

9. Click **Add Network**.

10. Edit the added network and copy the portal URL.

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

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

Configuring Segmentation Policies

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 **Add Segment** button to save the segment.

Sample Segments

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

Name
ACME Corp Employee Access

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

Status: Enabled 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:

The screenshot shows the configuration interface for an IOT Access Segment Policy. At the top, there are fields for 'Name' (ACME Corp IOT Access) and 'Description' (This is the segmentation policy for IoT devices in ACME Corp). Below these is a 'Status' section with a green 'Enabled' button and red 'Disable' and 'Monitor' buttons. The main configuration area is divided into two sections: 'Conditions' and 'Actions'. The 'Conditions' section, titled 'MATCHES ALL', contains two conditions: 'Network: Name is ACME-IOT' and 'Client: Group is IOT Devices'. The 'Actions' section contains one action: 'Assign VLAN' with a description 'Assign VLAN through RADIUS response'. This action is configured to assign 'VLAN' with the value 'ACME-IOT-Access'. Both sections have an 'Add Condition' or 'Add Action' button at the bottom right.

Figure: IOT Access Segment Policy

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 Integrating with Concourse Applications section (above).

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 Meraki
- 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 interface. The form is titled 'Add or Import Access Devices' with 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 showing 'Arista WiFi'), Serial Number (text input), IP Address (text input), Access Device Group (dropdown menu with a plus icon), and Location (text input with a location pin icon). Below the Location field is a note: 'Optional, example: Global/America/California/Site-1'. At the bottom right of the form are 'Cancel' and 'Add Device' buttons. 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, Devices, Device Groups, Cloud Gateways, Device Administration, Certificates, System), and CONCURSE (Explore, Installed Apps).

Figure: Adding a Device

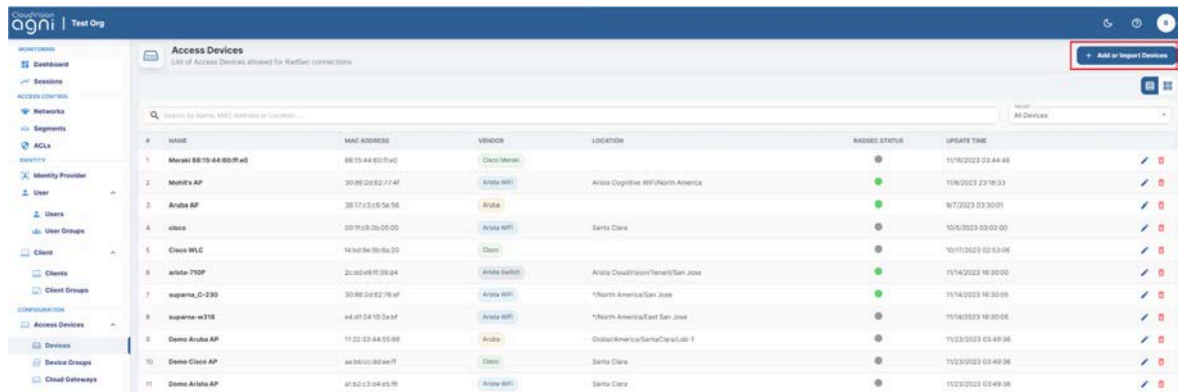
Importing Devices in Bulk to AGNI

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 an administrator and access the dashboard to import NAD devices in bulk.

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	ADDRESS STATUS	UPDATE TIME	
1	Meraki 8815-44-60-R-v0	8815-44-60-R-v0	Cisco Meraki			11/16/2023 03:44:48	
2	Meraki AP	30:85:28:62:77:47	Arista WPI	Arista Cognitive WPI/North America		11/16/2023 23:18:33	
3	Arista AP	38:17:c3:d5:5e:56	Arista			8/7/2023 03:30:01	
4	cisco	00:1f:09:2b:05:00	Arista WPI	Santa Clara		10/16/2023 03:00:00	
5	Cisco WLC	14:3d:5e:39:6a:20	Cisco			10/17/2023 02:53:06	
6	arista-710P	2c:30:a9:07:39:44	Arista Switch	Arista CloudVision/Tenant/San Jose		11/14/2023 16:30:00	
7	suparna_O-230	30:85:28:62:78:47	Arista WPI	*North America/San Jose		11/14/2023 16:30:05	
8	suparna-w31B	e4:4f:24:10:2a:3f	Arista WPI	*North America/East San Jose		11/14/2023 16:30:05	
9	Demo Arista AP	11:22:33:44:55:66	Arista	GlobalAmerica/Santa Clara/lab-1		11/23/2023 03:49:36	
10	Demo Cisco AP	aa:33:cc:dd:ee:ff	Cisco	Santa Clara		11/23/2023 03:49:36	
11	Demo Arista AP	af:52:c3:04:45:05	Arista WPI	Santa Clara		11/23/2023 03:49:36	

Figure: Importing Devices

2. Select the **Import** option to import devices using the .csv file format.
Note: Serial Number is a mandatory field for adding Cisco-Meraki devices using .csv file format.

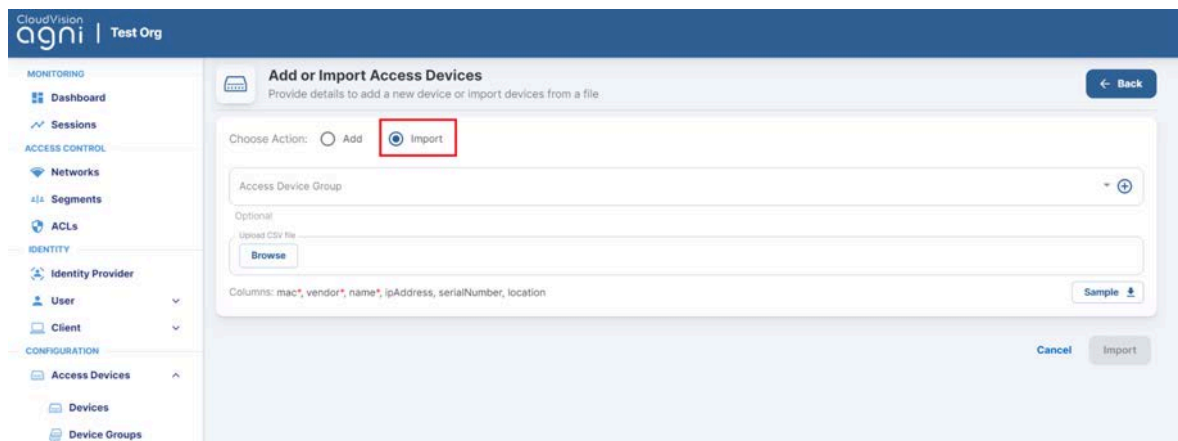


Figure: Add or Import Devices

As an 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).

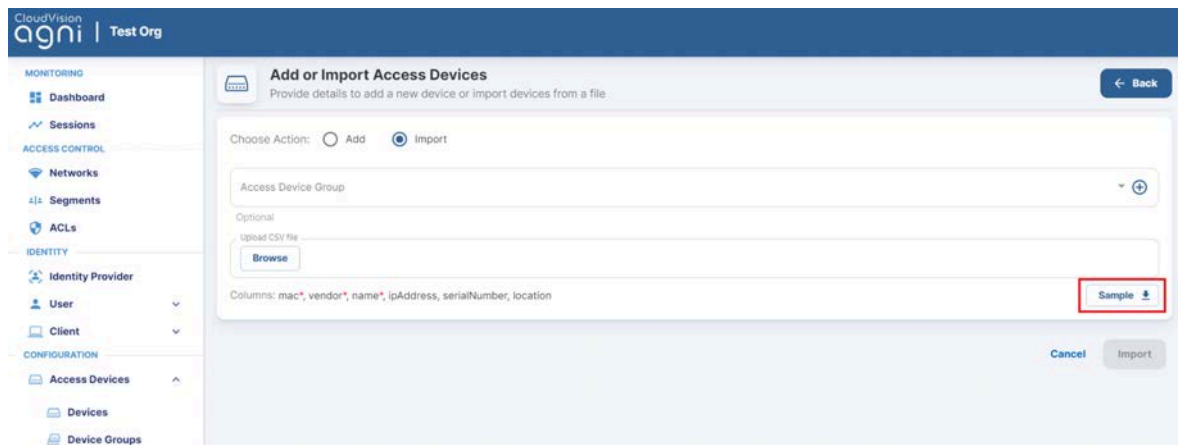


Figure: Add or Import Devices-2

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).

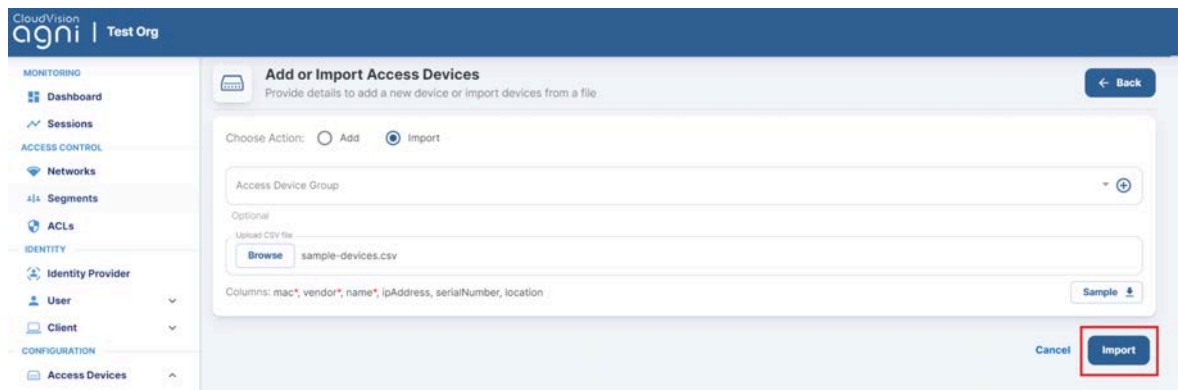


Figure: Add or Import Devices-3

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 88-15-44-60-F-v0	88-15-44-60-F-v0	Cisco Meraki		●	11/16/2023 03:44:48
2	Mobility AP	30-86-2d-63-77-a1	Arista WFI	Arista Cognitive WFI/North America	●	11/6/2023 23:18:53
3	Aruba AP	38-17-3-0b-5e-56	Aruba		●	9/1/2023 09:30:01
4	cisco	00-11-c9-26-06-00	Arista WFI	Santa Clara	●	10/5/2023 03:02:00
5	Cisco WLC	16-3d-3e-36-5a-20	Cisco		●	10/11/2023 02:53:06
6	arista-710P	2c-0b-69-07-39-64	Arista Switch	Arista CloudVision/Tenant/San Jose	●	11/14/2023 16:30:00
7	suparna_C-230	30-86-2d-63-76-a1	Arista WFI	*North America/San Jose	●	11/14/2023 16:30:05
8	suparna-w21B	e4-07-24-10-2a-0f	Arista WFI	*North America/East San Jose	●	11/14/2023 16:30:05
9	Demo Aruba AP	11-22-33-44-55-66	Aruba	GlobalAmerica/Santa Clara/Lab-1	●	11/23/2023 03:49:36
10	Cisco AP	aa-33-cc-00-aa-11	Cisco	Santa Clara	●	11/24/2023 15:29:33
11	Arista AP	a7-92-13-04-a5-06	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	a8-35-c4-c3-a2-01	Demo	San Jose	●	11/23/2023 03:49:36
14	Demo Cisco Meraki	a8-35-c4-c3-a2-02	Cisco Meraki	Mountain View	●	11/23/2023 03:49:36
15	Arista C-75	00-11-14-0f-00-0f	Arista WFI	GlobalAmerica/Santa Clara/Lab-1	●	11/24/2023 15:31:10

Figure: Access Devices

User Configurations

Users

All Users

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

External Users

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

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

Figure: External Users

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

The screenshot shows the 'Update User' page for 'Steve Kratt' in the AGNI interface. The left sidebar contains navigation menus for 'MONITORING' (Dashboard, Sessions), 'ACCESS CONTROL' (Networks, Segments, ACLs), 'IDENTITY' (Identity Provider, User, Users, User Groups), 'Client' (Clients, Client Groups), and 'CONFIGURATION' (Access Devices, Certificates, System). The main content area has a header 'Steve Kratt' with a 'Back' button and a description 'View user details and update the selected user.' Below this are input fields for 'Name' (Steve Kratt), 'User Id' (steve.kratt), and 'Passphrase' (masked with dots and a 'Copy' button). A 'Status' toggle is set to 'Enabled'. At the bottom right are 'Cancel' and 'Update User' buttons. Below the user details is a 'User clients' section with a search bar and a table. The table has columns for '#', 'MAC ADDRESS', 'DESCRIPTION', and 'STATUS'. One entry is shown: #1, MAC 70:1a:b8:82:10:31, Description 'Steve Kratt's Windows', and Status 'Enabled'.

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

Figure: External User Updation

Local User

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

The screenshot shows the 'Add Local User' page in the AGNI interface. The left sidebar is identical to the previous screenshot. The main content area has a header 'Add Local User' with a 'Back' button and a description 'Fill in the fields below to add a new local User'. Below this are input fields for 'User Id' (test@myorg1.com), 'Name' (Test User), and 'Password' (masked with dots and an eye icon). A 'Status' toggle is set to 'Enabled'. Below the status is a toggle for 'User should change password at next login', which is also 'Enabled'. At the bottom is a 'Login Invitation Email' section with a 'Disabled' toggle and a text box containing the instruction 'Enable to send notification with account details to user via email.' At the bottom right are 'Cancel' and 'Add User' buttons.

Figure: Local Users Addition

However, if the user is added to a Read-only user group, then that user do not have the permission to add, update, or delete clients using the AGNI portal or APIs (see image).




#	MAC ADDRESS	DESCRIPTION	OWNER (USER)	STATUS	UPDATE TIME
1		Karth's Mac OS X	Karth	Enabled	02/07/2024 11:53:01
2	88-aa-cc-dd-ee-ff	Karth's Mac OS X	Karth	Enabled	05/07/2024 22:30:35
3	aa-55-33-19-2b-4f	Karth's Android	Karth	Enabled	21/06/2024 16:10:08

Figure: Local User with Read-only Access (part of Restricted User Group)

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.



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

Figure: External User Groups

Local User Groups

Local User Groups provide the ability for administrators to manage the users within local group membership. With this, you can map local users with the configured local user group. As this is managed locally in the system, the administrators can add, modify, and delete these entities.

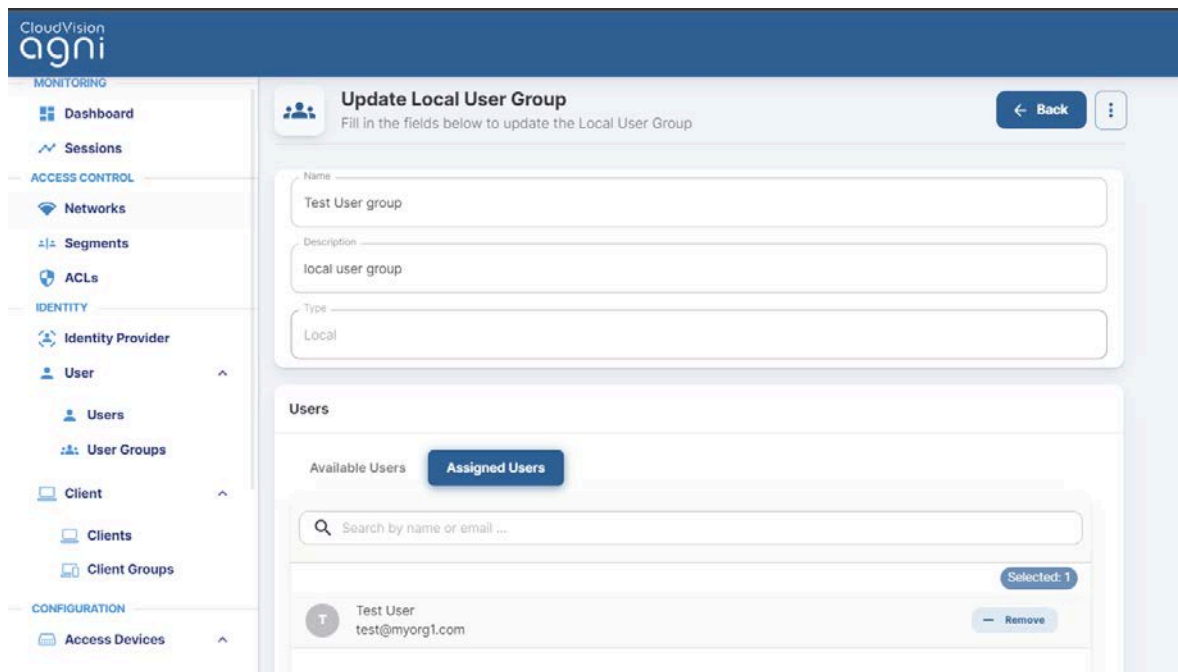


Figure: Local User Groups

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.
- **User Association** - The Client Group can either be Not User associated or associated to Onboarding User
 - **Not User Associated** - This is meant for IOT clients. If mac bypass authentication is enabled in the Network configuration then IOT clients authenticate and dynamically get added to the client group that is typically Not User Associated. If the client group is Not Associated then the Group UPSK and Delegated Management options are provided to the admin.
 - **Onboarding User** - Client which belongs to a client group with User Association Type as Onboarding User can do client certificate based onboarding
- **Group UPSK** - Client Groups can be defined with a Group UPSK, which can be used to onboard the desired client devices in that specific group.

The screenshot shows the AGNI CloudVision interface. On the left is a navigation menu with categories: MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Users, User Groups), Client, and Clients. The main content area is titled 'Test Client Group' and contains the following fields:

- Name:** Test Client Group
- Description:** The client mapped to this group are test clients
- User Association:** Not user associated (dropdown menu)
- Group U-PSK:** Enabled (toggle switch)
- Passphrase:** A field with masked characters and a 'Copy' button.

Buttons at the top right include 'Add or Import Clients', 'Back', and a menu icon.

Figure: Client Group UPSK

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

The screenshot shows the 'Add Client Group' interface in the CloudVision AGNI dashboard. The left sidebar contains navigation links for Monitoring, Access Control, and Identity. The main form area is titled 'Add Client Group' and includes a 'Back' button. The form fields are: Name (Test Client Group), Description, User Association (Not user associated), Group U-PSK (disabled), and Allowed Networks (PUNE-WPA2). The 'Allowed Networks' field has a red 'x' icon and a 'Select Networks...' link.

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.

The screenshot shows the 'Test Client Group' interface in the CloudVision AGNI dashboard. The left sidebar contains navigation links for Monitoring, Access Control, and Identity. The main form area is titled 'Test Client Group' and includes buttons for 'Add or Import Clients', 'Back', and a menu icon. The form fields are: User Association (Not user associated), Group U-PSK (disabled), Allowed Networks (PUNE-WPA2), and Delegated Management (enabled). The 'Delegated Management' field has a green 'Enabled' toggle and a 'Select user groups...' link.

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 shows the 'Add or Import Clients' form in the CloudVision agni interface. The left sidebar contains navigation menus for MONITORING (Dashboard, Sessions), ACCESS CONTROL (Networks, Segments, ACLs), IDENTITY (Identity Provider, User, Users, User Groups, Client, Clients, Client Groups), and CONFIGURATION (Access Devices, Certificates). The main form area has a title 'Add or Import Clients' and a subtitle 'Fill in the fields below to add a new Client or upload a file to import Clients'. A 'Back' button is in the top right. The 'Client Group' dropdown is set to 'Test Client Group'. Under 'Choose action:', the 'Add' radio button is selected. The 'MAC Address' field contains '00:11:74:12:ed:4f' and the 'Description' field contains 'Test Client'. At the bottom right are 'Cancel' and 'Add Client' buttons.

Figure: Client Addition

The screenshot shows the 'Add or Import Clients' form with the 'Import' radio button selected under 'Choose action:'. The 'Client Group' dropdown remains 'Test Client Group'. The 'Upload CSV File' section includes a 'Browse' button, the text 'Columns: mac*, description', and a 'Sample' button with a download icon. At the bottom right are 'Cancel' and 'Import' buttons. Below the form, there is a section titled 'Clients in this group' with a 'Show Clients' button.

Figure: Client Import

Client Details

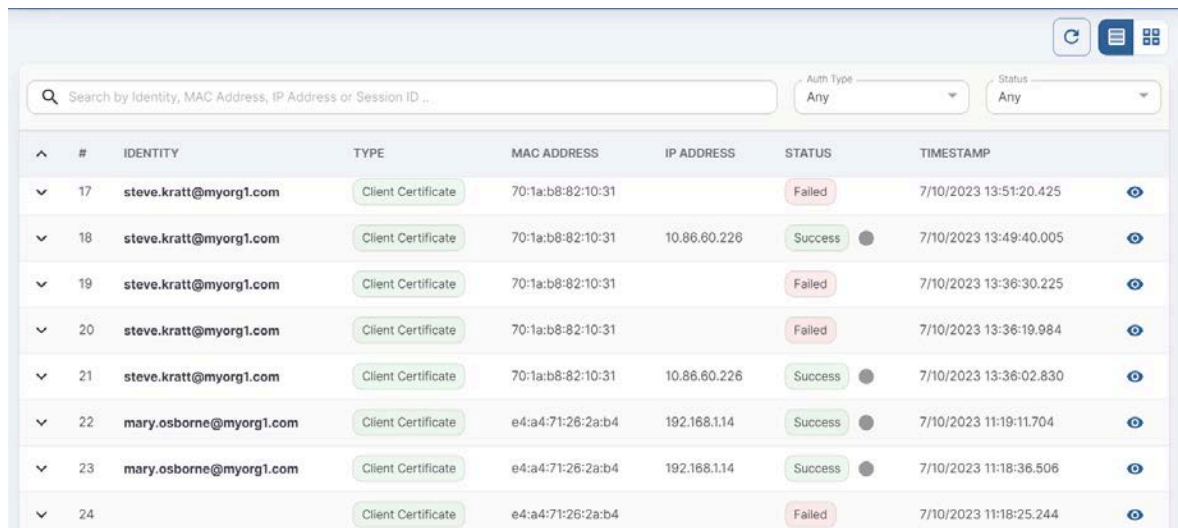
Click on the clients to display the client details:

- **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 computer 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

The screenshot displays the 'Steve Kratt's Windows' client details page. The interface includes a header with the client name and a 'Back' button. The main content area is divided into several sections:

- Client Information:** Shows the MAC address (78:1a:68:02:10:31), description (Steve Kratt's Windows), status (Enabled), and buttons for 'Cancel' and 'Update Client'.
- Client Details:** A table showing device type (Computer/Windows), machine authentication (No), added at (7/10/2023 13:49:20), and updated at (7/10/2023 13:49:36).
- Client Fingerprint:** A table showing DHCP Option 55 (1,3,6,16,31,33,43,44,48,47,18,121,249,252), DHCP Options (55), MAC Vendor (Intel Corporate), HTTP User Agent (Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like ...), and HTTP User Agent (Microsoft/NET).
- Last Session Details:** A table showing IP Address (10.88.60.126), Location (-), Signpost (Default), and Authentication Status (Success).
- Client Certificate (EAP-TLS):** A table showing Subject DN (CN=steve.kratt, O=myorg), Issuer DN (CN=ADN, Issuer CA, O=TyOw-Bute (E/TyP35c-nd5-4wd3-95c7-c76c4872b4a3)), and Expiry Date (7/9/2024 13:49:36).

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	192.168.1.14	Success	7/10/2023 11:19:11.704
23	mary.osborne@myorg1.com	Client Certificate	e4:a4:71:26:2a:b4	192.168.1.14	Success	7/10/2023 11:18:36.506
24		Client Certificate	e4:a4:71:26:2a:b4		Failed	7/10/2023 11:18:25.244

Figure: Client Sessions

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 an administrator to AGNI to create client certificates. You can generate the client certificate only for available clients in AGNI.

Before this release, the 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/Linux devices using the client application.

The admins can:

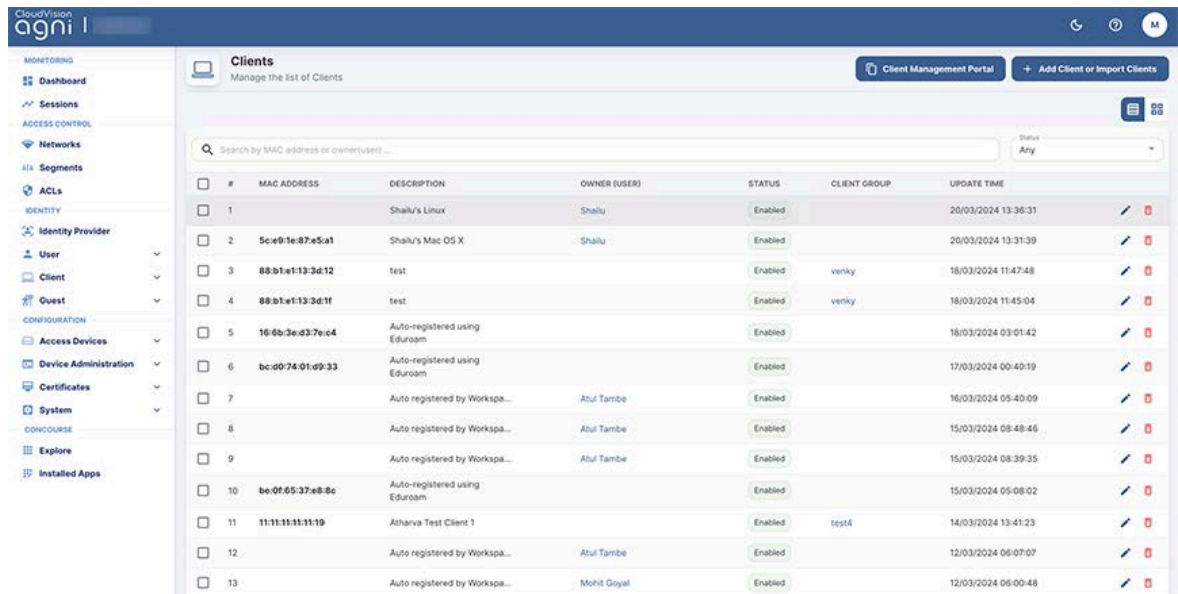
- Manually generate client certificates for each of the client/user devices in AGNI.
- Download the client certificate as a .pem file.
- Download the PFX (.p12) file containing the certificate and private key (if they have not used a CSR). This p12 file is encrypted by providing a password.

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

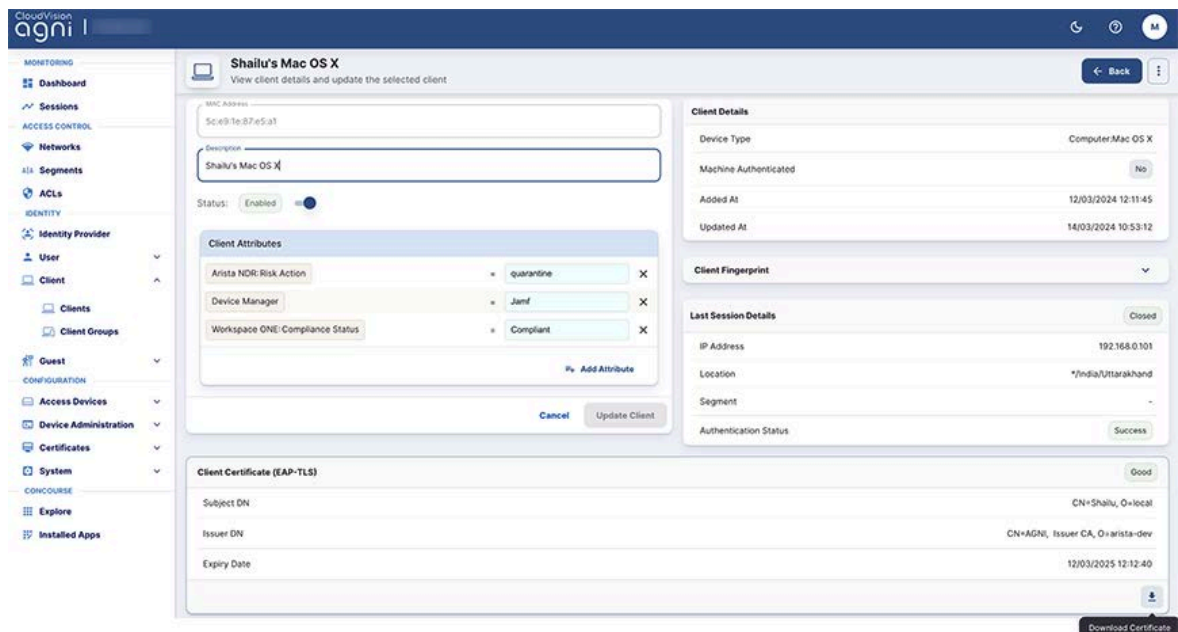
Note: This client certificate is different from the RadSec client certificate, which is used in access devices such as switches, routers, servers, and so on.

To generate the Client certificate:

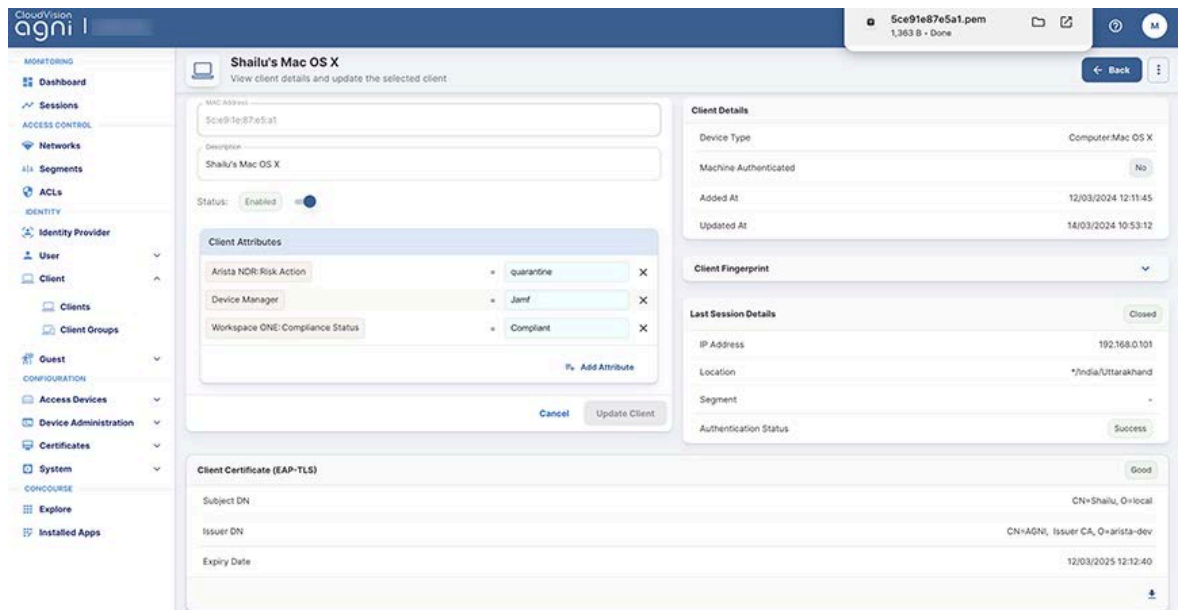
- Navigate to **Client > Clients** on AGNI portal (see image below).



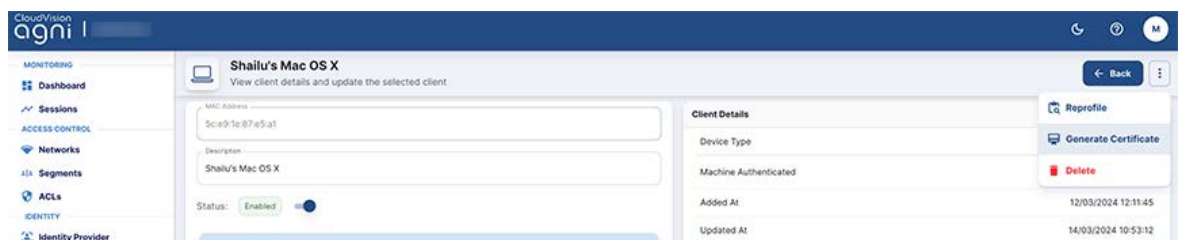
- Select a client to open the client details page (see image below). This page displays the client certificates of the selected client.
Note: If the client is not present in the client details table, the admin should add the client before generating the client certificate.



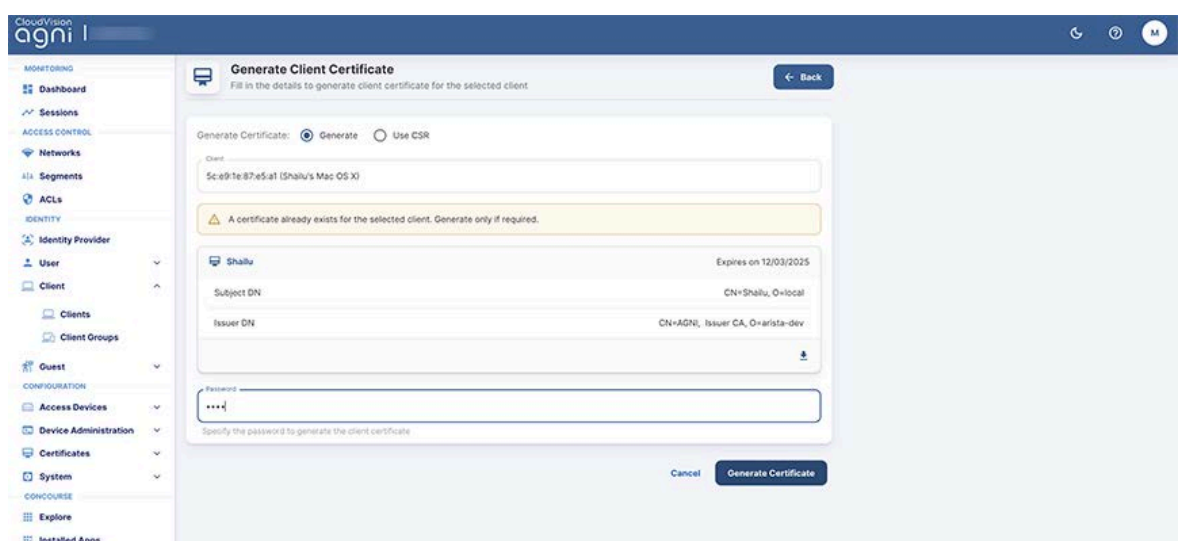
- Download the certificate by clicking the download button (arrow). The X509 certificate (.pem file) is saved to the download folder. You can open the file to verify the details.



- 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.

The screenshot shows the 'Generate Client Certificate' page in the AGNI interface. The left sidebar contains navigation menus for MONITORING, ACCESS CONTROL, IDENTITY, CONFIGURATION, and CONFORMANCE. The main content area has a title 'Generate Client Certificate' and a subtitle 'Fill in the details to generate client certificate for the selected client'. Below this, there are two radio buttons: 'Generate' (selected) and 'Use CSR'. A text box for 'Client' contains '1c:4d:70:b3:b9:97 (Shailu's Linux)'. Below this is a table with columns for 'Client', 'Expires on', 'Subject DN', and 'Issuer DN'. The table shows a client named 'Shailu' with an expiry date of '21/03/2025', a subject DN of 'CN=Shailu, O=local', and an issuer DN of 'CN=AGNI, Issuer CA, O=arista-dev'. At the bottom, there is a 'Password' field with a note 'Specify the password to generate the client certificate'. The page has 'Cancel' and 'Generate Certificate' buttons.

- 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.

The screenshot shows the 'Generate Client Certificate' page in the AGNI interface, with the 'Use CSR' radio button selected. The 'Client' text box still contains '1c:4d:70:b3:b9:97 (Shailu's Linux)'. A yellow warning box with a triangle icon and the text 'A certificate already exists for the selected client. Generate only if required.' is displayed. Below the warning box is a table with columns for 'Client', 'Expires on', 'Subject DN', and 'Issuer DN'. The table shows a client named 'Shailu' with an expiry date of '27/03/2025', a subject DN of 'CN=Shailu, O=local', and an issuer DN of 'CN=AGNI, Issuer CA, O=arista-dev'. Below the table, there are two radio buttons for 'Select Action': 'Upload CSR File' and 'Paste CSR' (selected). A large text box for 'Paste CSR' contains the text 'Sample CSR text'. The page has 'Cancel' and 'Generate Certificate' buttons.

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

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 \(Wireless\)](#)
- [Configuring Guest Portal in AGNI for Wired Clients](#)
- [Configuring Guest Portal Using Guestbook \(Wired\)](#)
- [Configuring Guest Portal Using Guestbook-Host Approval \(Wired\)](#)
- [Configuring Guest Portal Using Self-Registration \(Wired\)](#)

Guest Onboarding Using AGNI

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

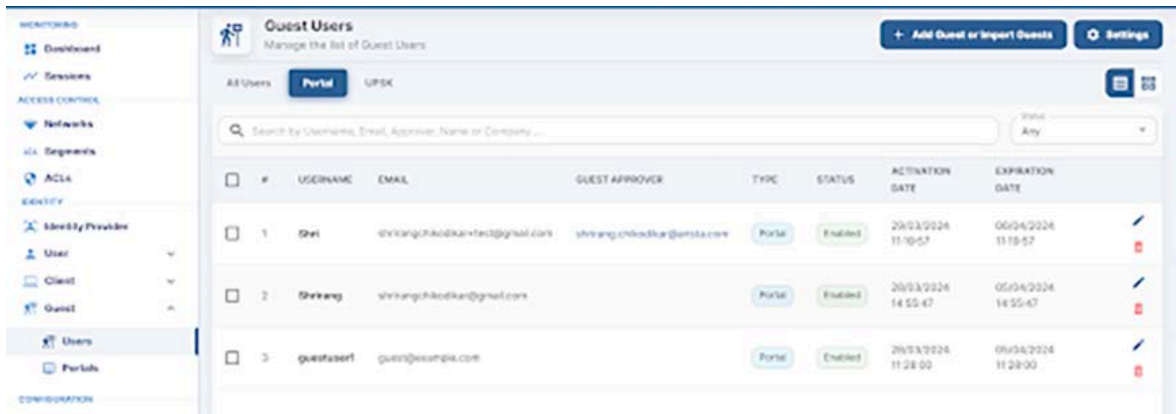
Guest User in AGNI

AGNI supports the following user categories to provide the guest onboarding experience:

- 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.

Choose Action: ☒ Add ☐ Import

Username: guestuser1

Email: guest@example.com

Portal: Org users

Valid From: 02/04/2024 08:52 PM

Valid To: 10/04/2024 08:52 PM

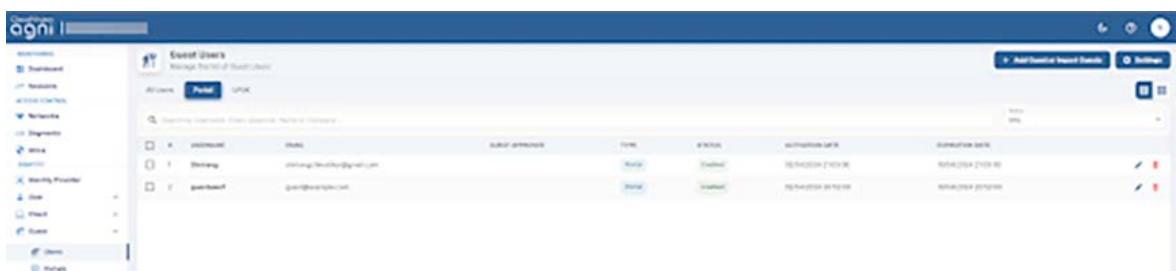
Validity: 8 Days

Device Limit: 4

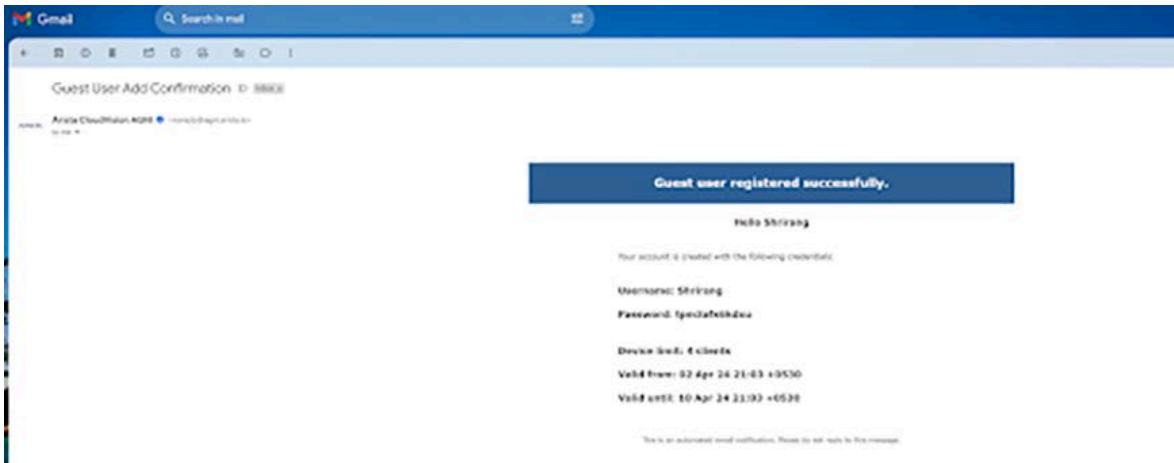
Additional guest user information

Buttons: Cancel, Add, Add and Email

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 USERNAME	TYPE	STATUS	ACTIVATION DATE	EXPIRATION DATE
1	user1	username1@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
2	user2	username2@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
3	user3	username3@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
4	user4	username4@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
5	user5	username5@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
6	user6	username6@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
7	Shrirang	shrirang@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00
8	guestuser1	guest@example.com		Portal	Enabled	02/04/2024 21:43:00	10/04/2024 21:43:00

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.

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

Choose Action: ☐ Add portal user ☒ Add UPSK user ☐ Import

Email: shirangchikodkar+upsk@gmail.com

Validity: 8 Hours

Device Limit: 4

Additional guest user information

Name: TestUser

Company: Example LLC

Phone:

Address:

Notes: Test account

Cancel Add 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.

Update Guest User
New guest user details will update the selected guest user.


Email:

Username:

Password:

Device Limit:

Valid From: Valid Until:

Network QR code for this user: 

Additional guest user information:

First Name:

Last Name:

Phone:

Address:

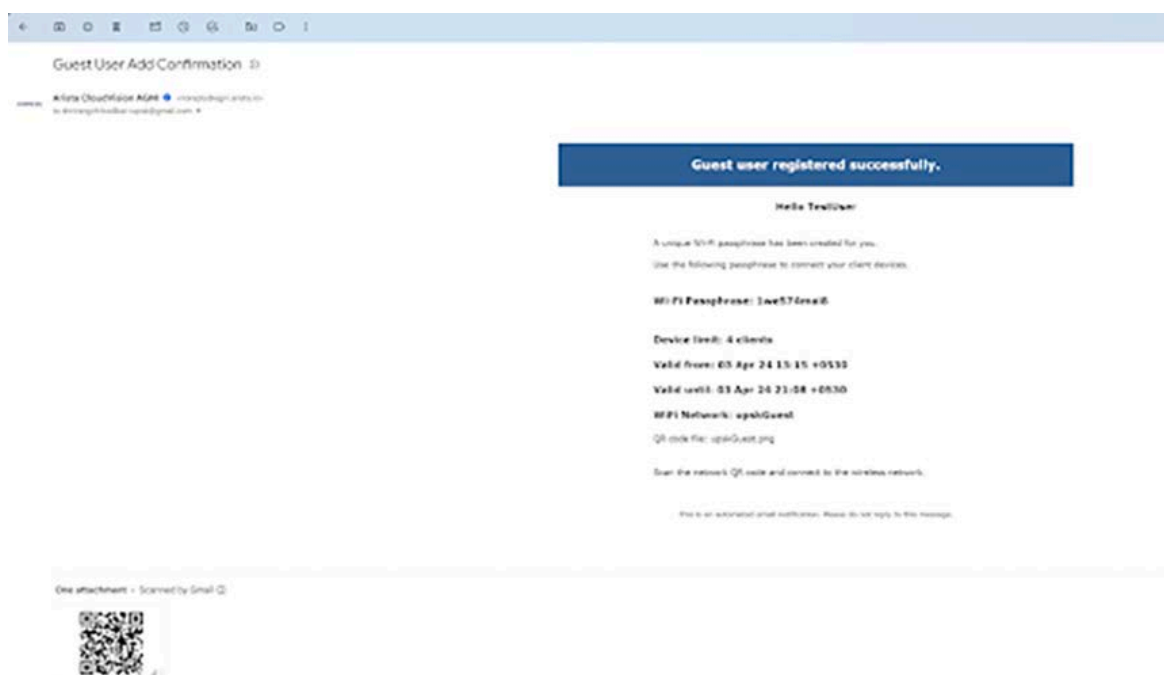
City:

State:

Postal Code:

Buttons:

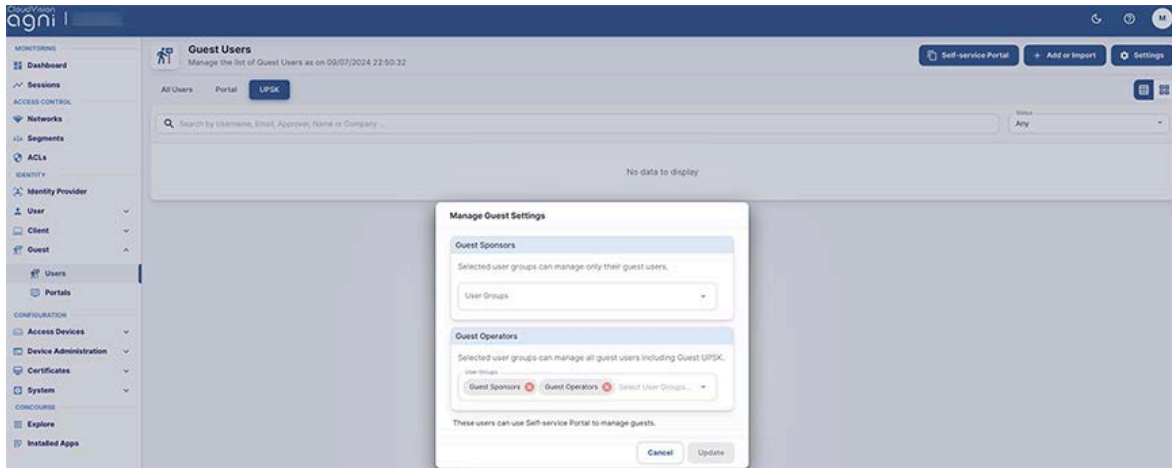
- Click the **Add and Email** button. An email is sent to the configured email address with the following details: UPSK user name, passphrase, user validity, device limit, and QR code of the network.
- The UPSK Guest user can onboard the devices to the network by scanning the QR code or by using a system-generated 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.

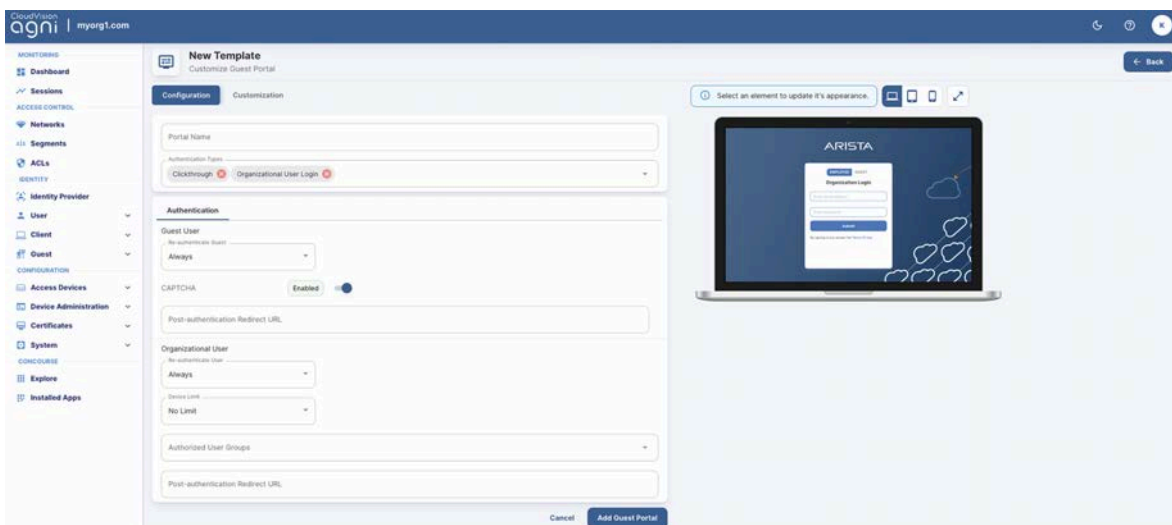
The AGNI admin can add a portal with multiple customization options and modify every field on it. The portal-based authentication method uses the following client onboarding methods:

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.

AGNI supports **captcha** in guest portals and captcha can be enabled for Guest Clickthrough and Guestbook users. To enable Captcha:

- Navigate to **Identity**→**Guest**→**Portals**.
- Choose the **Authentication Type** as either *Clickthrough* or *Guestbook*.
- Enable the captcha Knob.
- Preview the captcha, which is displayed on the right side.
- Click the **Add Guest Portal** button to save the configuration.



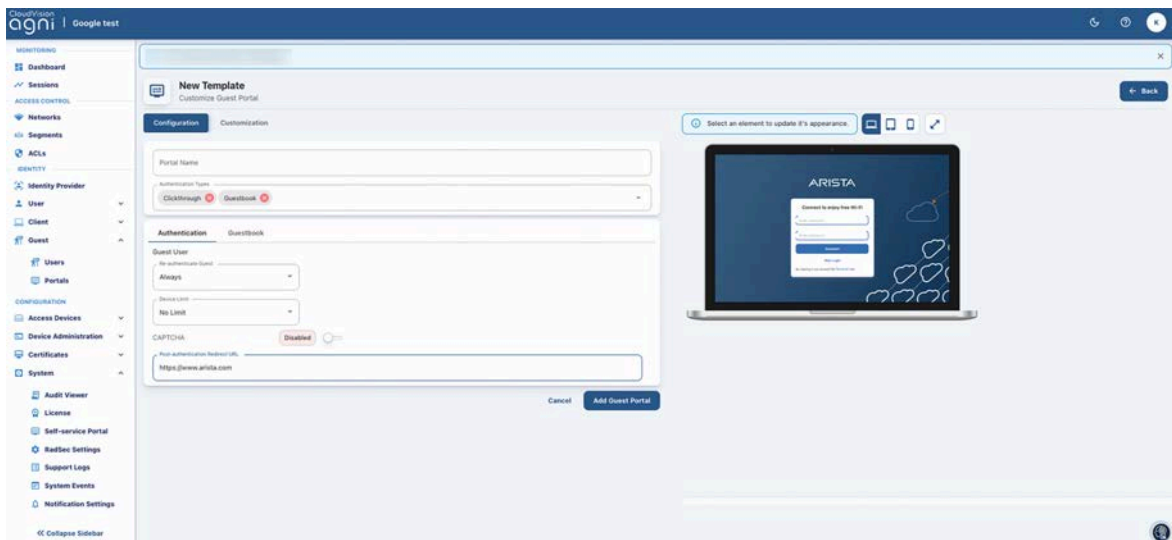
Support for Redirect URL in Guest Portal

AGNI portal provides support for redirection of URL as part of guest portal authentications. Upon successful authentication, the clients are redirected to the redirectURL, if configured in the guest portal. The guest portal redirection of URL is available for all authentication types in guest portal such as Clickthrough users, GuestBook users, and Organizational Users (IDP and Local). To configure redirect URL:

- Navigate to **Identity**→**Guest**→**Portals**.
- Select the Guest Portal for which you want to configure the redirect URL.
- Enter the URL in the **Post-authentication Redirect URL** field.
- Click the Update button to save the configuration (see image).

The redirect URL feature is applicable and visible to all the client platforms that AGNI supports.

Note: For Android platforms, the redirectURL may or may not be visible after successful portal authentication because the Android CNA transitions to connected state very quickly.



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

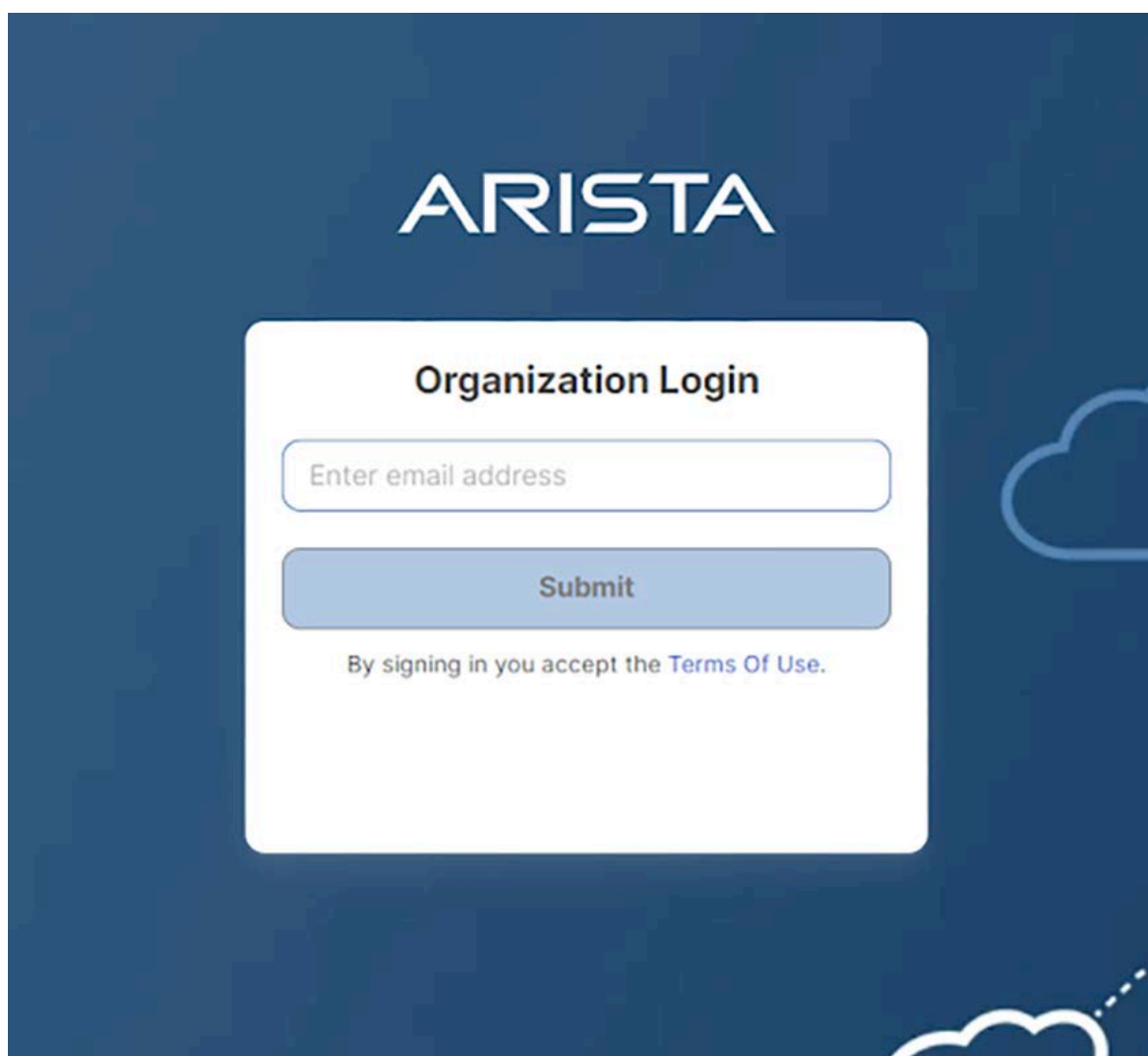
Re-Authentication Period
12 Hours

Device Limit
4

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

Cancel Add Guest Portal

See the sample portal below:



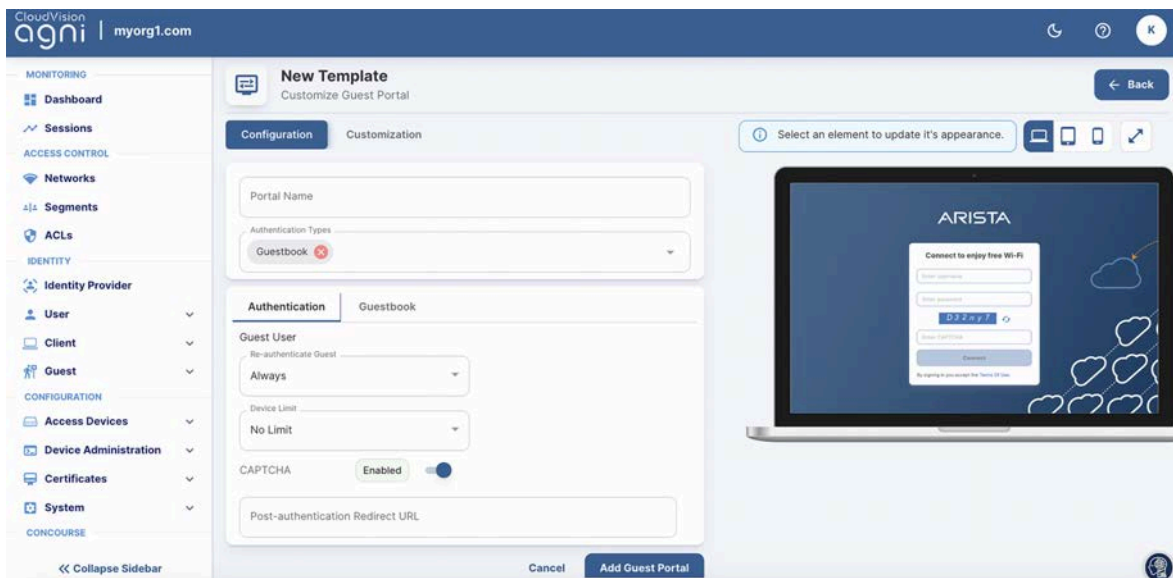
Guestbook Based Onboarding

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.

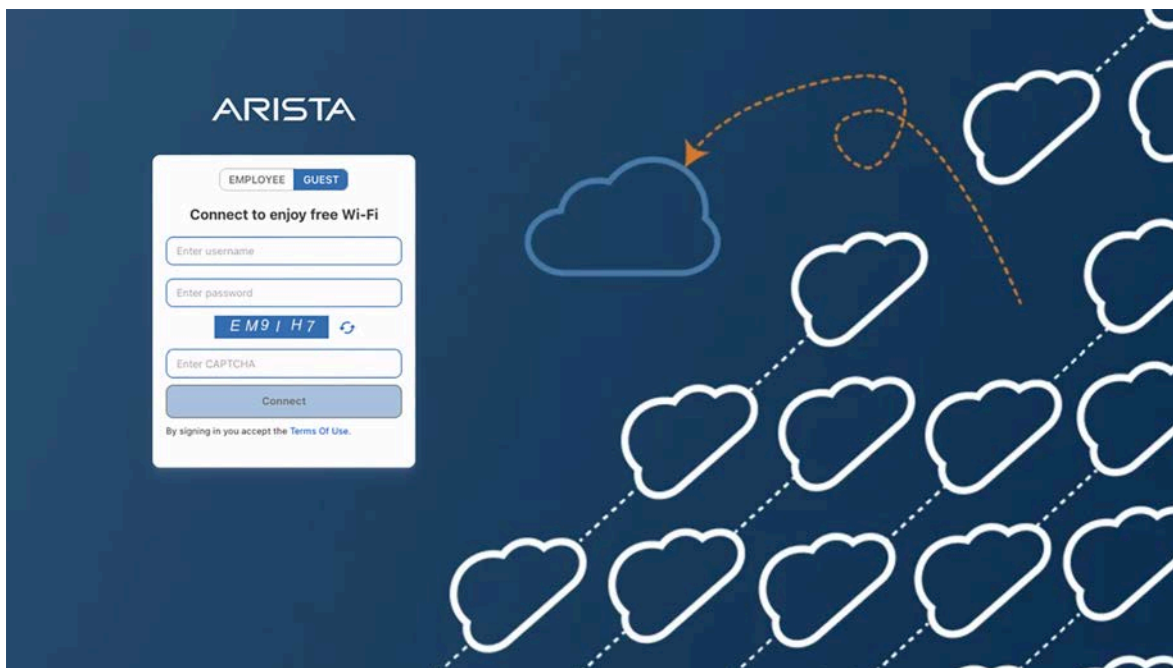
Guestbook Method

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 sample portal is as follows:



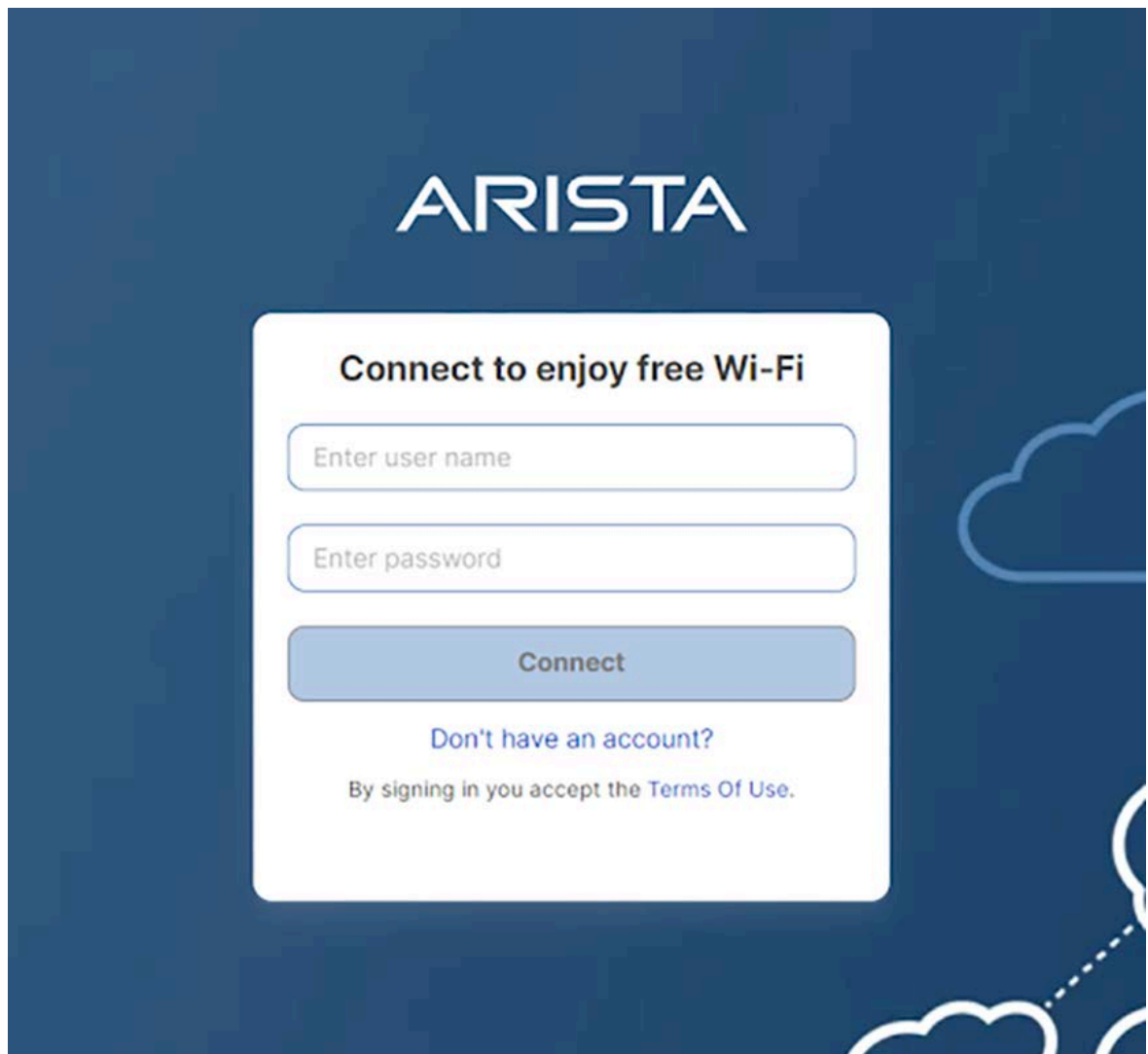
Self-Registration

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:

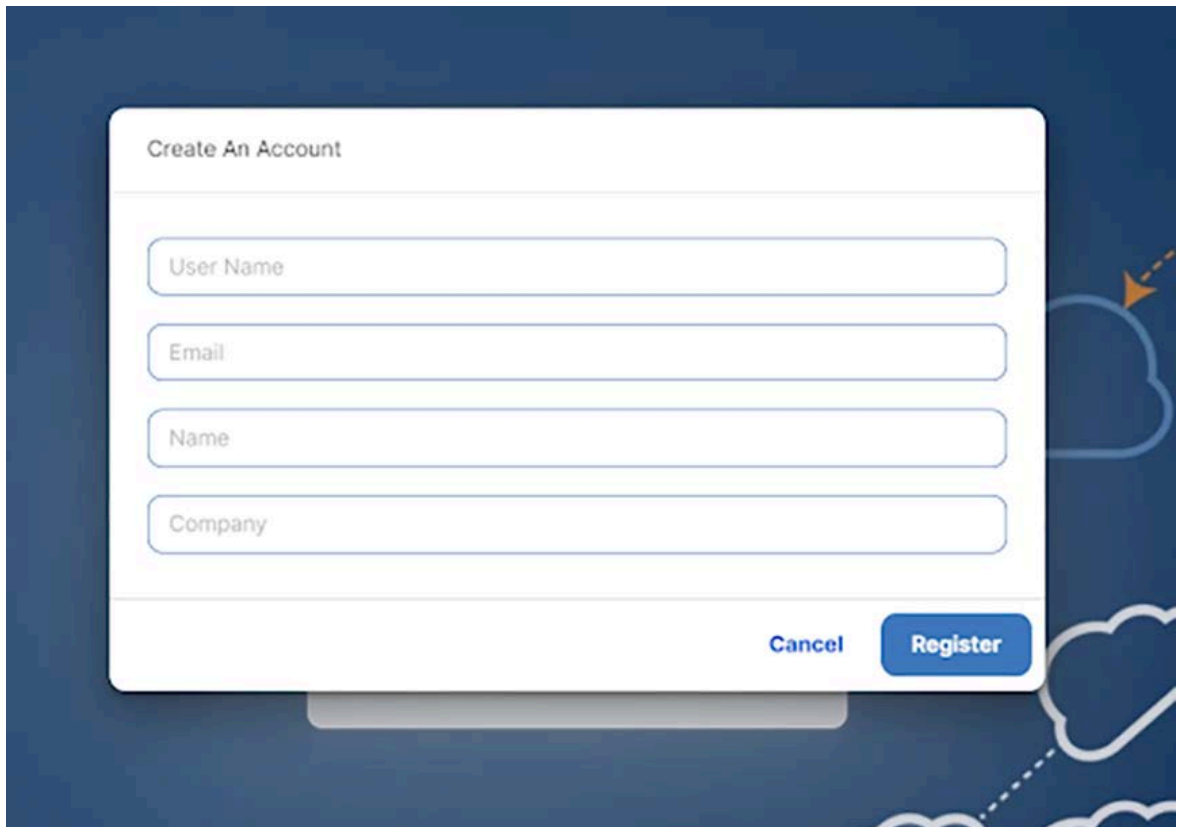
The screenshot displays the 'AGNI Guestbook' configuration interface. At the top, there's a header with the AGNI logo and the title 'AGNI Guestbook' with a subtitle 'Customize Guest Portal'. Below this, there are two tabs: 'Configuration' (active) and 'Customization'. The 'Configuration' tab contains several settings:

- Portal Name:** A text field containing 'AGNI Guestbook'.
- Authentication Types:** A dropdown menu with 'Guestbook' selected and a red 'X' icon next to it.
- Authentication / Guestbook Section:**
 - Default Validity:** A text field with '8' and a unit dropdown set to 'Hours'.
 - Allow Self Registration:** A toggle switch that is currently 'Enabled' (blue).
 - Approval required for guest access:** A toggle switch that is currently 'Disabled' (grey).
 - Customize Guest User Fields:** A button with a downward arrow.

Below is a sample portal:

The image shows a login interface for Arista's free Wi-Fi. At the top, the word "ARISTA" is displayed in a large, white, sans-serif font against a dark blue background. Below the logo, the heading "Connect to enjoy free Wi-Fi" is centered in a smaller white font. The login form consists of three main elements: a text input field labeled "Enter user name", a text input field labeled "Enter password", and a blue "Connect" button. Below the button, there is a link that says "Don't have an account?" and a line of text stating "By signing in you accept the Terms Of Use." The background features faint white cloud outlines on the right side.

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:

A screenshot of a 'Create An Account' form. The form is white with rounded corners and is set against a dark blue background with cloud graphics. It contains four input fields: 'User Name', 'Email', 'Name', and 'Company'. At the bottom right, there are two buttons: a blue 'Cancel' button and a blue 'Register' button. The title 'Create An Account' is at the top left of 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

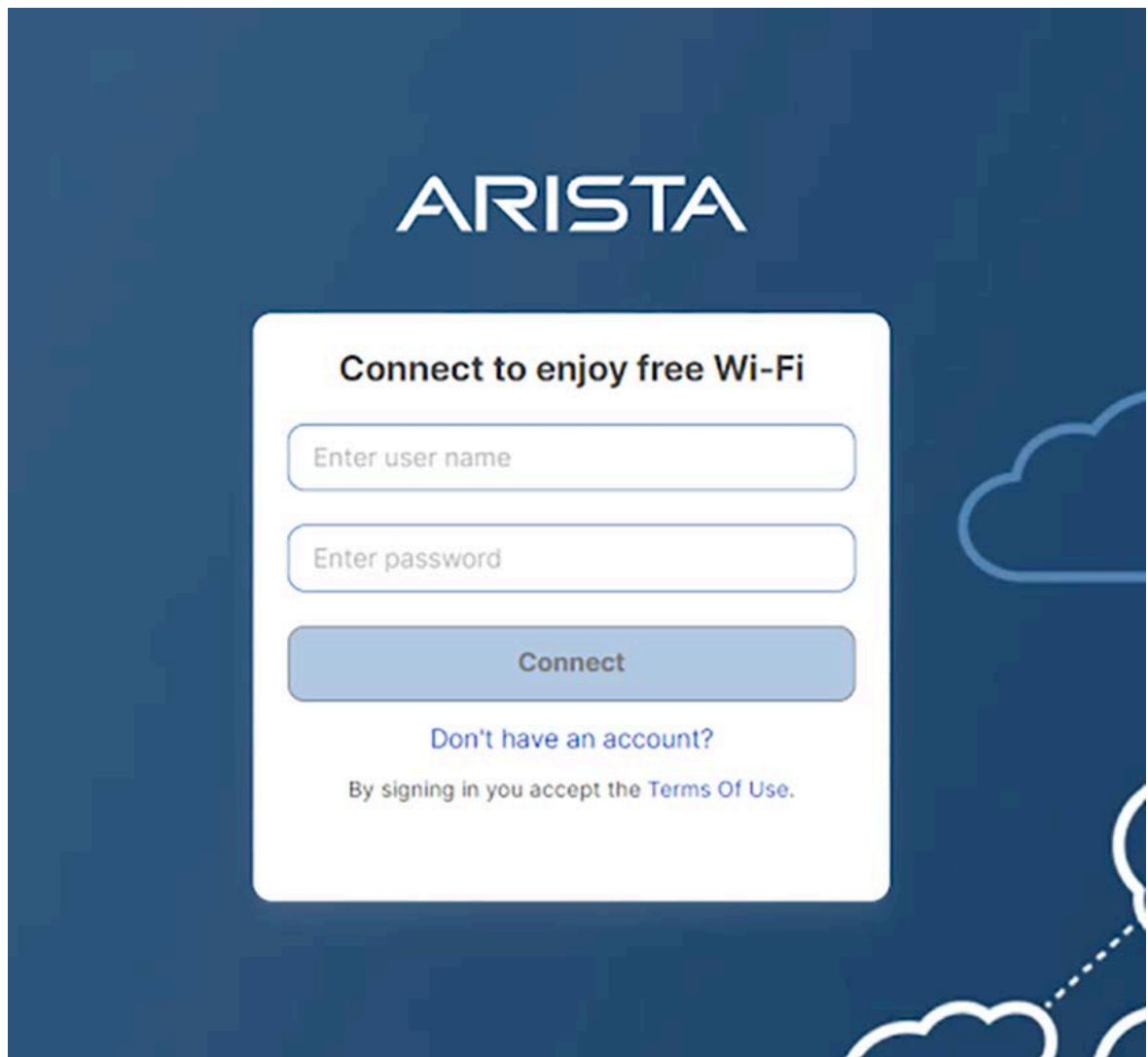
Engineering 

approver 

Select Authorized User Groups...

Customize Guest User Fields

Below is a sample portal:



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:

Create An Account

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:

Guest User Registration Approval External Block

Arista CloudVision AGNI monopy@agni.arista.io to me

Guest User approval request

A guest account is created with the following details:

Name: Shrirang
Username: Shri
Email: shrirangchikodiker+test@gmail.com
Company: shrirangchikodiker@gmail.com
Notes: shrirangchikodiker@gmail.com
Device limit: 4 clients
Valid from: 29 Mar 24 05:49 UTC
Valid until: 06 Apr 24 05:49 UTC

To approve the guest account, click the following button:

Approve Guest

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 section 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 for both WPA2+ PSK and WPA3+PSK modes. 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.

The screenshot shows the 'Add Network' configuration page in the CloudVision Agni interface. The left sidebar contains navigation menus for MONITORING, ACCESS CONTROL, IDENTITY, and CONCOURSE. The main content area is titled 'Add Network' and includes a 'Back' button. The form fields are as follows:

- Name:** A text input field containing 'UPSK for Guest'.
- Connection Type:** Radio buttons for 'Wireless' (selected) and 'Wired'.
- SSID:** A text input field containing 'upskGuest'.
- Status:** A toggle switch set to 'Enabled'.
- Authentication:**
 - Authentication Type:** A dropdown menu set to 'Unique PSK (UPSK)'.
 - Allowed Users:** Radio buttons for 'Organizational users only' and 'Guest users only' (selected).
 - Message:** A light blue informational box stating: 'The wireless SSID type must be configured as WPA2 only for guest access. Applicable for Arista Wi-Fi only.'
- User Private Networks:** A toggle switch set to 'Enabled'.
- Shared Clients:** A toggle switch set to 'Disabled'.
- Message:** A light blue informational box stating: 'Enable to make a set of clients accessible to all users.'

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

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 **Guests > 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.

The screenshot shows the 'Add or Import Guests' page in the CloudVision Agni Self Service Portal. The left sidebar contains navigation menus for Manage Clients, Register Client, Wi-Fi Passphrase, GUESTS, and Users. The main content area is titled 'Add or Import Guests' and includes a 'Back' button. The form fields are as follows:

- Choose Action:** Radio buttons for 'Add portal user', 'Add UPSK user' (selected), and 'Import'.
- Email:** A text input field.
- Validity:** A text input field containing '8' and a 'Hours' label.
- Device Limit:** A dropdown menu set to 'No Limit'.
- Additional guest user information:** A collapsed section indicated by a downward arrow.

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

8. Add the user's email address and click the **Add and Email** option.
9. The guest user 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.

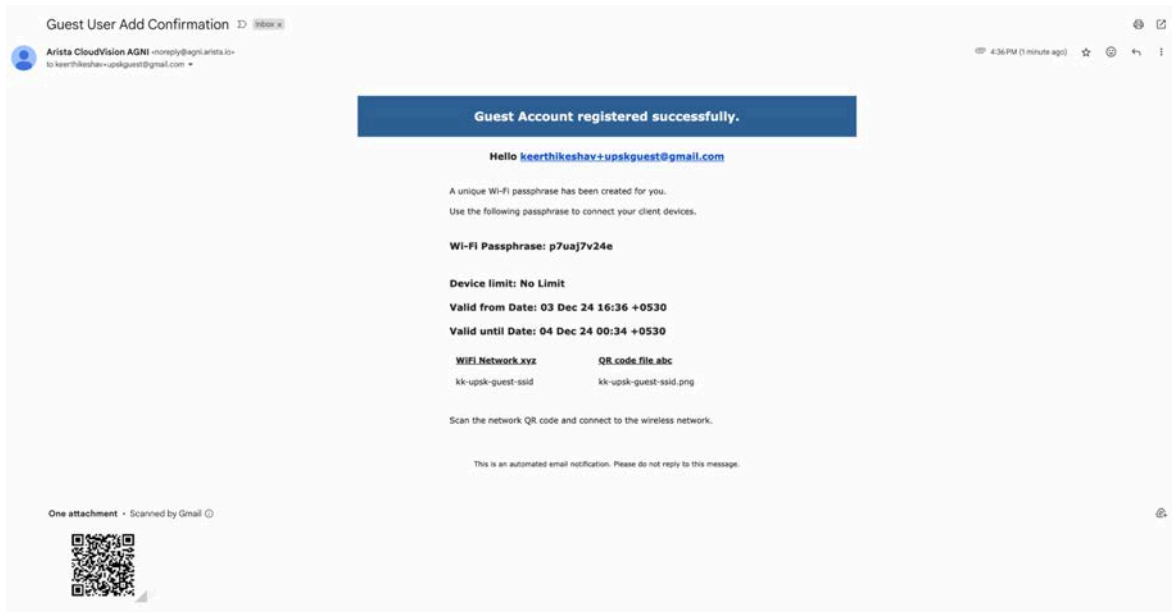
The screenshot shows the 'Update Guest User' interface in the CloudVision agni Self Service Portal. The left sidebar contains navigation links: Manage Clients, Register Client, Wi-Fi Passphrase, GUESTS, and Users. The main content area is titled 'Update Guest User' with a subtitle 'View guest user details and update the selected guest user'. It includes a 'Back' button and a menu icon. The form contains the following fields and controls:

- Email:** A text input field containing 'keerthikeshav+upskguest@gmail.com'.
- Username:** A text input field containing 'kk-guest-operator-101'.
- Notification:** A blue box with an information icon and the text 'This is a UPSK based guest user.'
- Password:** A password input field with a toggle for visibility and a 'Copy' button.
- Created At:** A date and time field showing '12/3/2024 04:36 PM' with a calendar icon.
- Validity:** A field showing '8' hours, with a 'Valid until' date of '12/4/2024 12:34 AM'.
- Device Limit:** A dropdown menu currently set to 'No Limit'.
- Status:** A toggle switch labeled 'Enabled'.
- Additional guest user information:** A collapsed section.
- Buttons:** 'Cancel', 'Update', and 'Update and Notify' at the bottom of the form.

On the right side, there is a section titled 'Network QR code for this user' showing the 'Wireless Network' as 'kk-upsk-guest-ssid' and a QR code.

At the bottom, there is a 'Guest User Clients' section with a 'Show Clients' button.

Below is an example of the email received:



General Behavioral Guidelines:

For WPA2 + UPSK client registrations:

- **Unregistered Clients:** Client or user machine can connect directly to UPSK SSID by using the UPSK keys. However, you must first enable *UPSK Identity Lookup* on the access point for the same UPSK SSID. This ensures AGNI to Identify and automatically register the client.
- **Registered Clients (UPSK Onboarding and Self Service Portal):** *UPSK Identity Lookup* is not mandatory in this case as AGNI is aware of the client that is previously onboarded, either through UPSK onboarding URL or Self Service Portal.

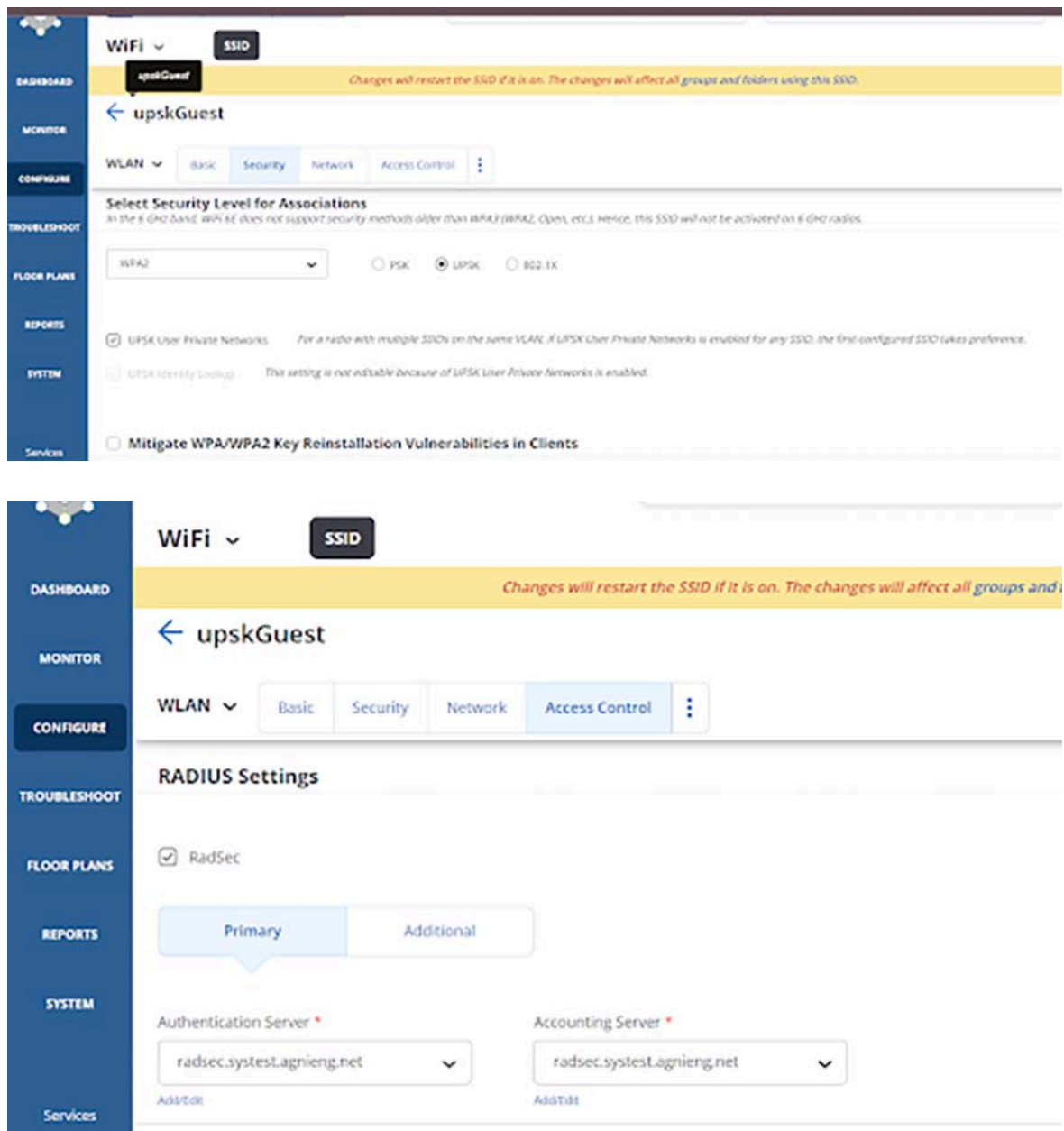
For WPA3 + UPSK client registrations:

- **Unregistered Clients:** WPA3 Enhanced key management does not support cracking or Identity Lookup. Users should register the device through UPSK onboarding flow before connecting to the network.
- **Registered Clients (UPSK Onboarding and Self Service Portal):** AGNI is aware of the client that is previously onboarded through UPSK onboarding. Hence clients can connect to the UPSK network after successful UPSK onboarding through the Onboarding URL. Subsequently, clients that are registered through the self service portal gets connected to the UPSK networks.

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

The screenshot displays the CV-CUE web interface for configuring a WiFi profile. On the left is a blue sidebar with navigation links: DASHBOARD, MONITOR, CONFIGURE (highlighted), TROUBLESHOOT, FLOOR PLANS, REPORTS, SYSTEM, and Services. The main content area has a top bar with 'WiFi' and a 'SSID' button. Below this is a yellow warning banner: 'Changes will restart the SSID if it is on. The changes will aff...'. The page title is '← upskGuest'. Under the 'WLAN' dropdown, there are tabs for 'Basic' (selected), 'Security', 'Network', and 'Access Control'. The 'Name' section contains two required fields: 'SSID Name' and 'Profile Name', both containing the text 'upskGuest'. At the bottom, there is a 'Select SSID Type' section.



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:

- The guest user scans the UPSK QR code and onboard to the AGNI network.
OR
- 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)

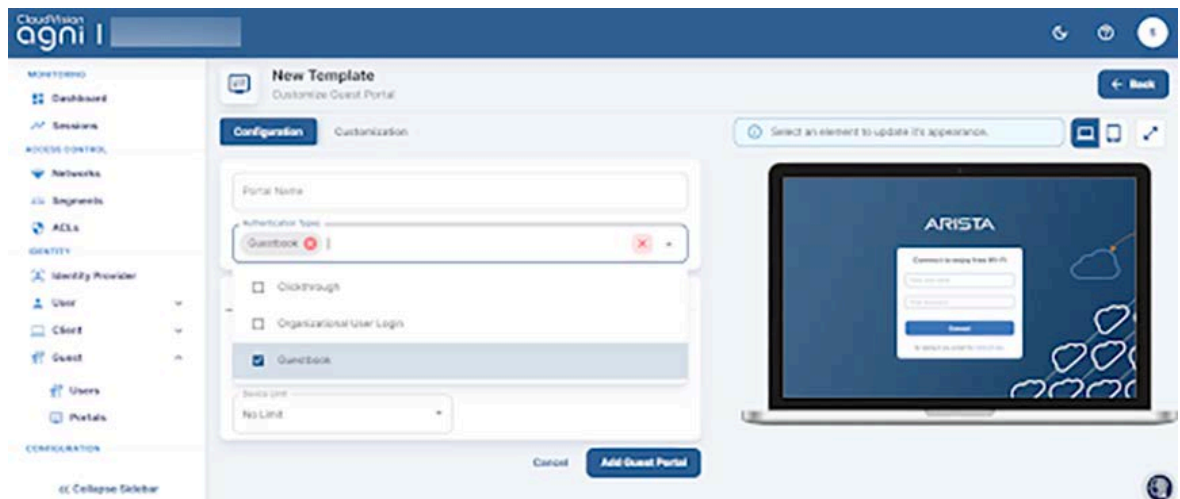
This section describes the steps to configure the guest portal with the Guest Book authentication method for wireless clients. You must configure both AGNI and CV-CUE to configure the guest portal.

Configuring the Portal on AGNI

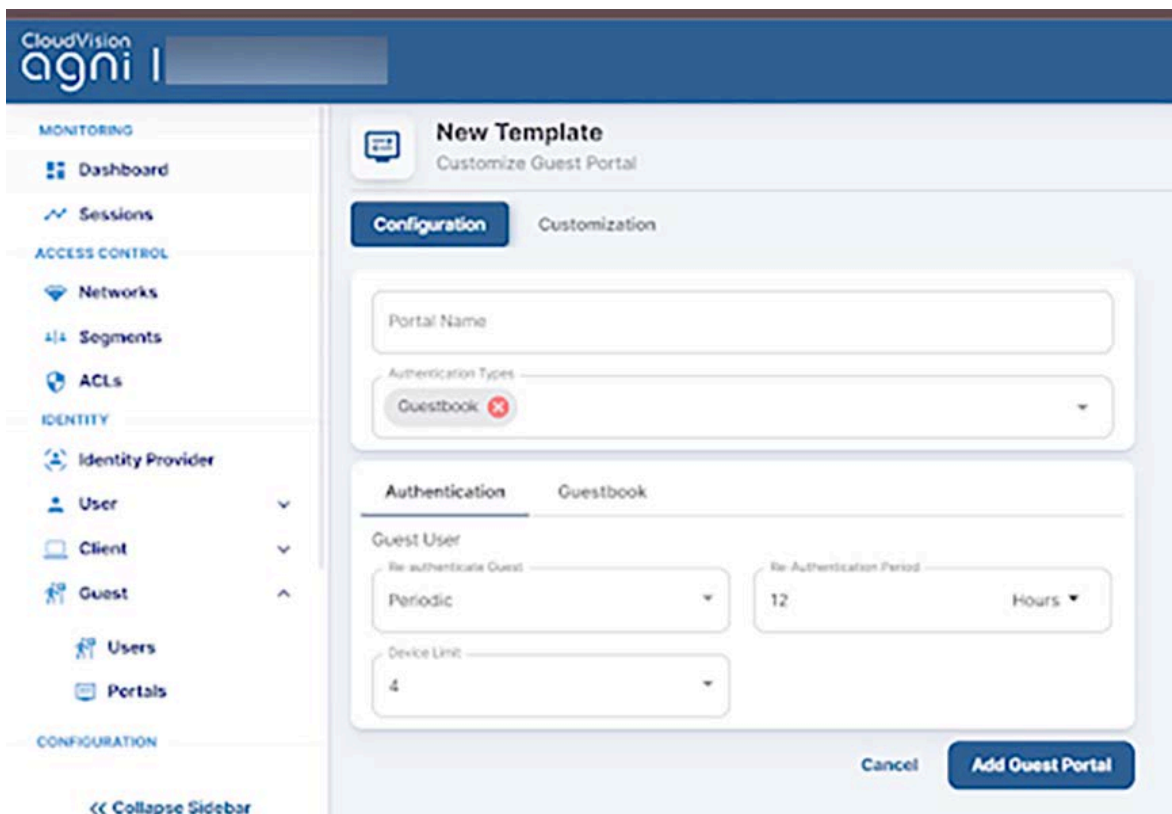
1. Log in to AGNI and navigate to **Identity > Guest > Portals**
Note: The **Default** portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.



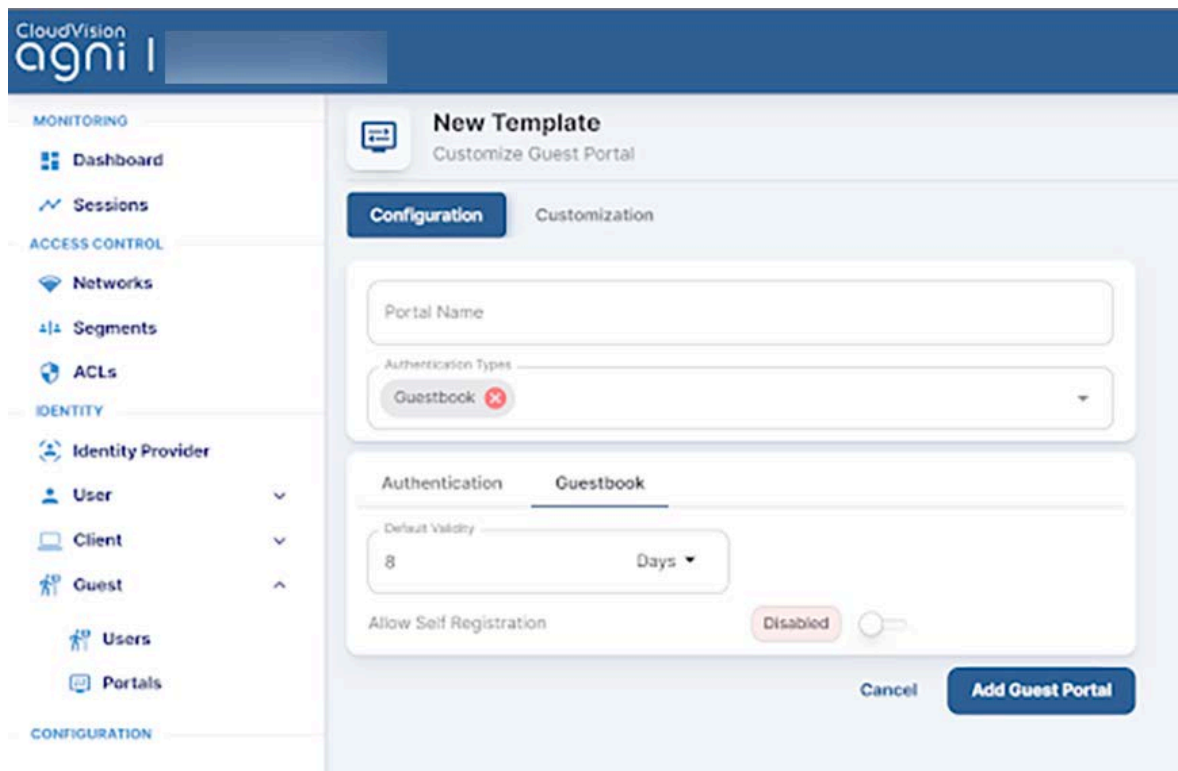
2. Click the **+Add Guest Portal** button.
3. In the **Configuration** tab, provide the portal name and select the Authentication Types. The available Authentication types are **Default**, **Organizational User Login**, and **Guestbook**. Select **Guestbook** as the Authentication Type.



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

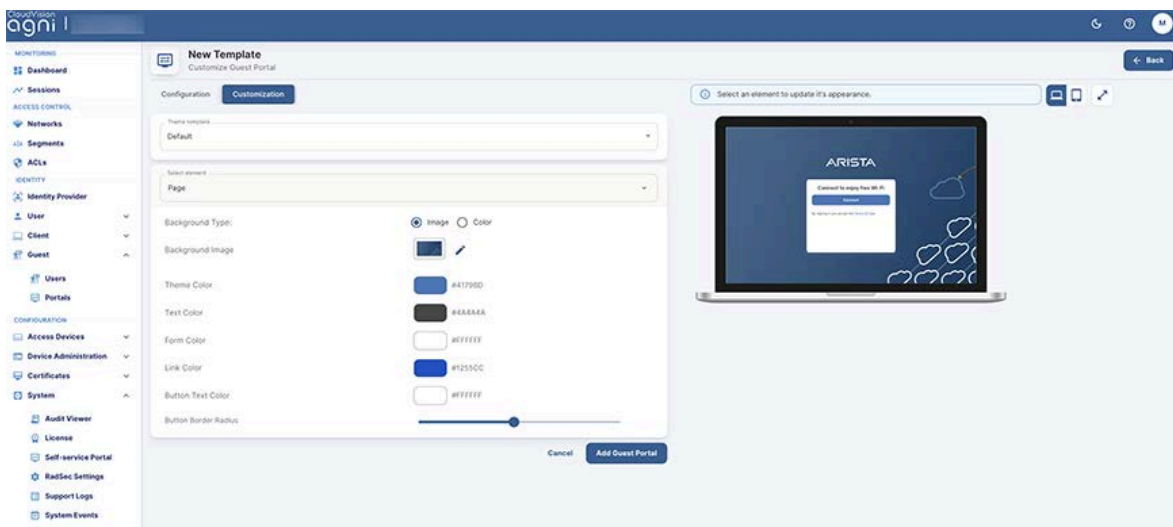
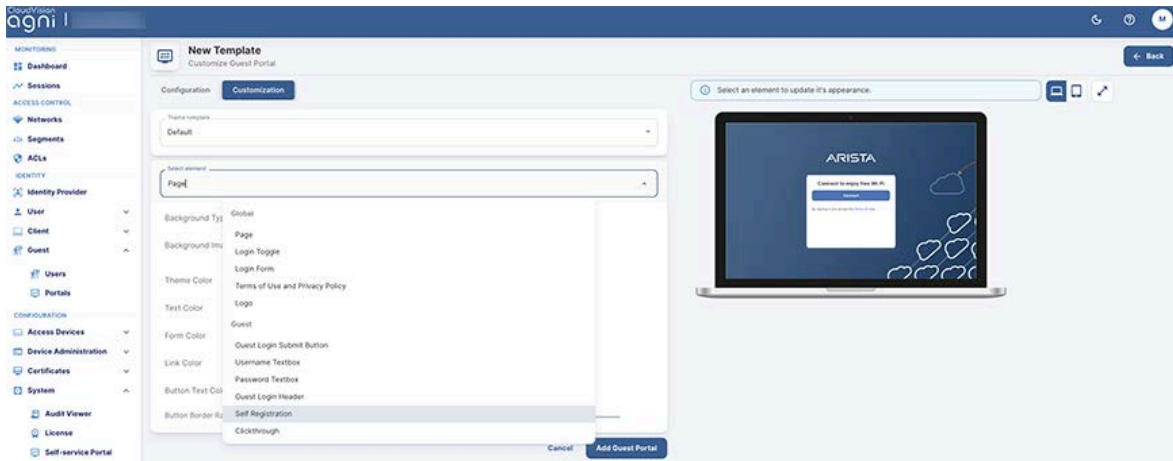


5. Navigate to Guestbook settings and configure the Device Validity to 8 Days. Keep **Allow Self Registration** Disabled.

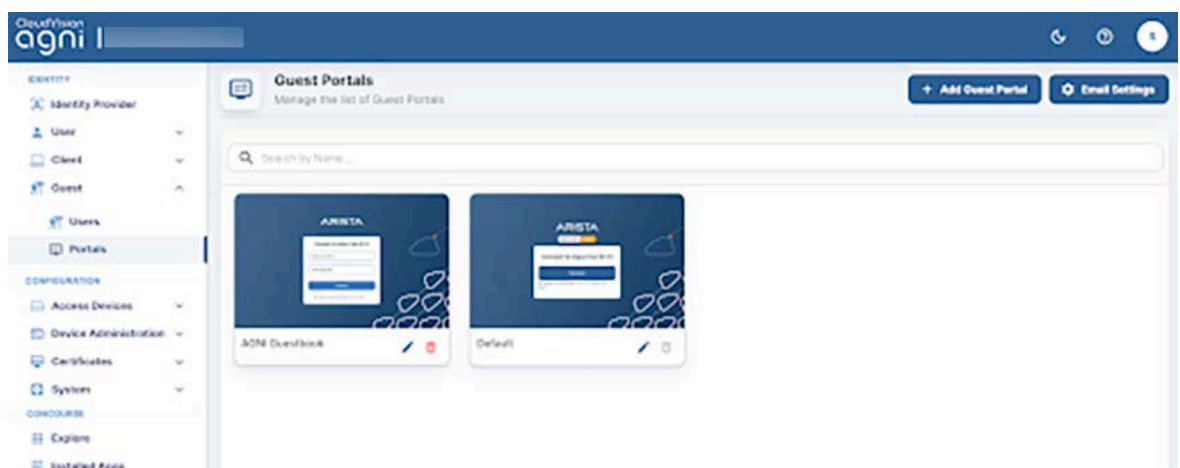


Note: Device validity should always be greater than the re-authentication period. The default value for Device Validity is 8 Hours.

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

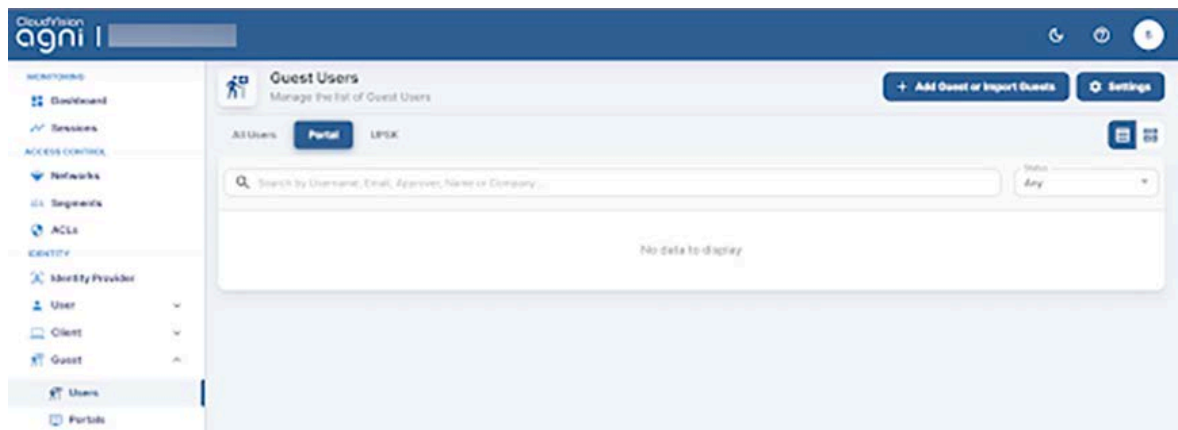


7. When done, click **Add Guest Portal**. The portal gets listed in the portal listing.



8. Navigate to **Identity > Guest > Users**

9. Click on the **Add Guest or Import Guests** option to add portal users.

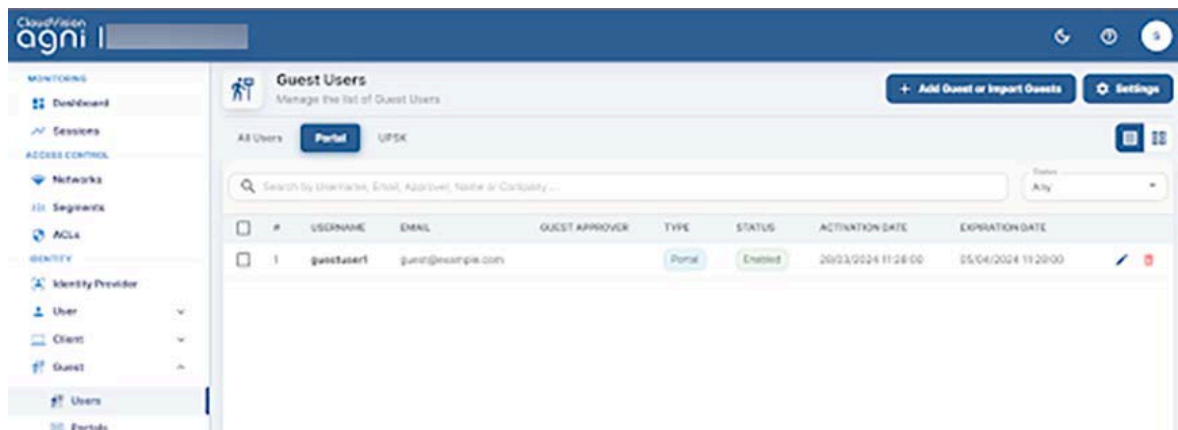


10. Add a Guest user with the following settings:

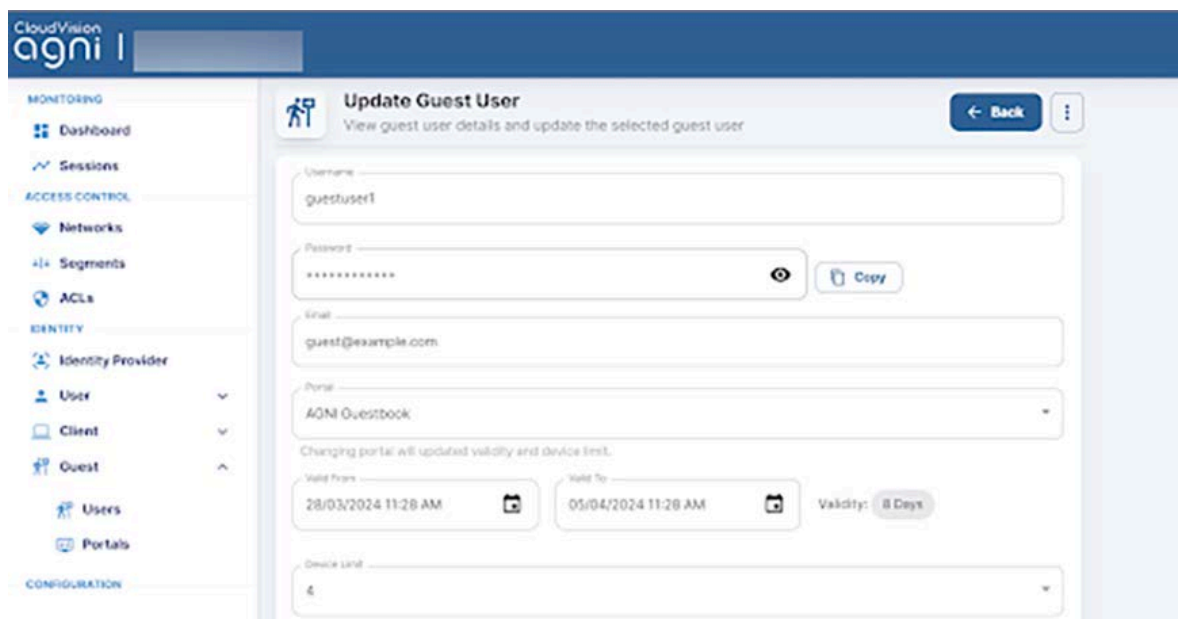
- Username - guestuser1
- Email - guest@example.com
- Portal - AGNI Guestbook
- Validity - 8 Days
- Device Limit - 4

Note: The Validity & Device Limit changes automatically as per the portal selected

11. 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.
12. The guest user is listed in the Portal User listing.



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

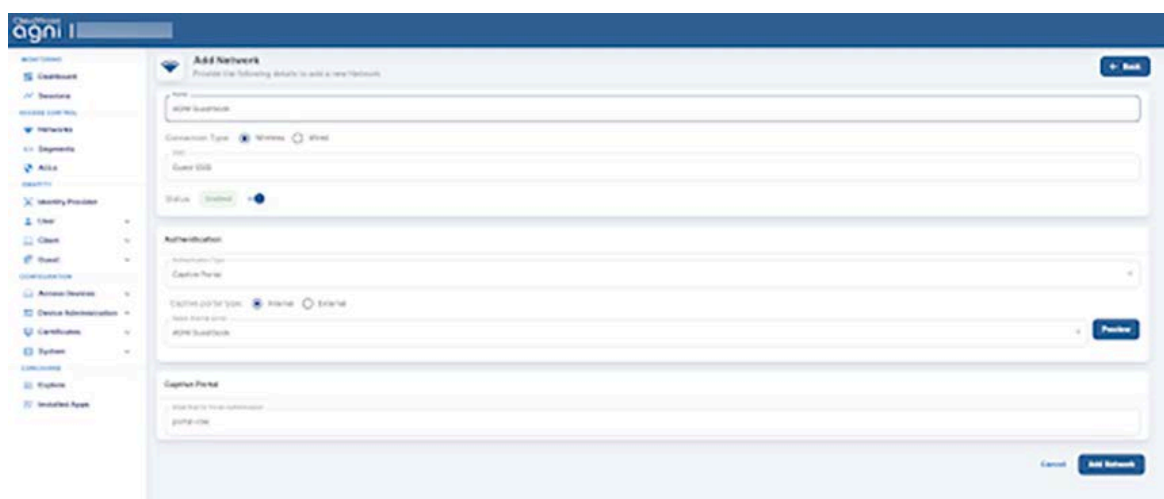


14. Select the guest user from the portal user listing and use the **Export** option to export user details (including password) into a CSV file.



Configuring the Network

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

The screenshot shows the 'Add Network' configuration page in the AGNI web interface. The left sidebar contains a navigation menu with options like Dashboard, Settings, Networks, Elements, and more. The main content area is titled 'Add Network' and includes a 'Name' field with 'AGNI Guestbook', a 'Connection Type' dropdown set to 'Wireless', an 'SSID' field with 'Guest SSID', and a 'Status' dropdown set to 'Enabled'. Below these are 'Authentication' settings: 'Authentication Type' set to 'Captive Portal', 'Captive Portal Type' set to 'Internal', and a 'Select internal portal' dropdown set to 'AGNI Guestbook'. At the bottom, there is a 'Captive Portal' section with a 'Select role for portal authentication' dropdown set to 'portal-role'. 'Add' and 'Cancel' buttons are at the bottom right.

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.

Network Profiles
Role Profile

portal-role

Profile Name
portal role

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
addn.microsoft.net:80,443
addn.microsoft.net:80,443
login.live.com:80,443
syntest.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** 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 *
radius.system.agning.net ▾
Available

Accounting Server
radius.system.agning.net ▾
Available

☒ 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:
 - a. Rule Type — 802.1X Default VSA
 - b. Operand — Match
 - c. 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 *

802.1X Default VSA ▼

Operand *

Match ▼

Assign Role *

portal-role [portal 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)

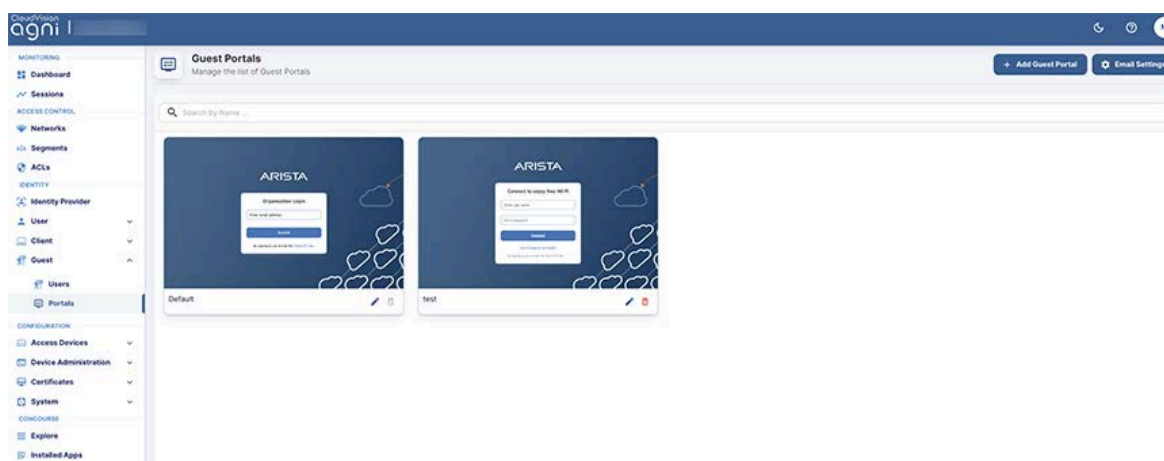
This section describes the steps to configure the guest portal using the Guest Book authentication method for wireless clients. You must configure both AGNI and CV-CUE to configure the guest portal.

Configurations on AGNI

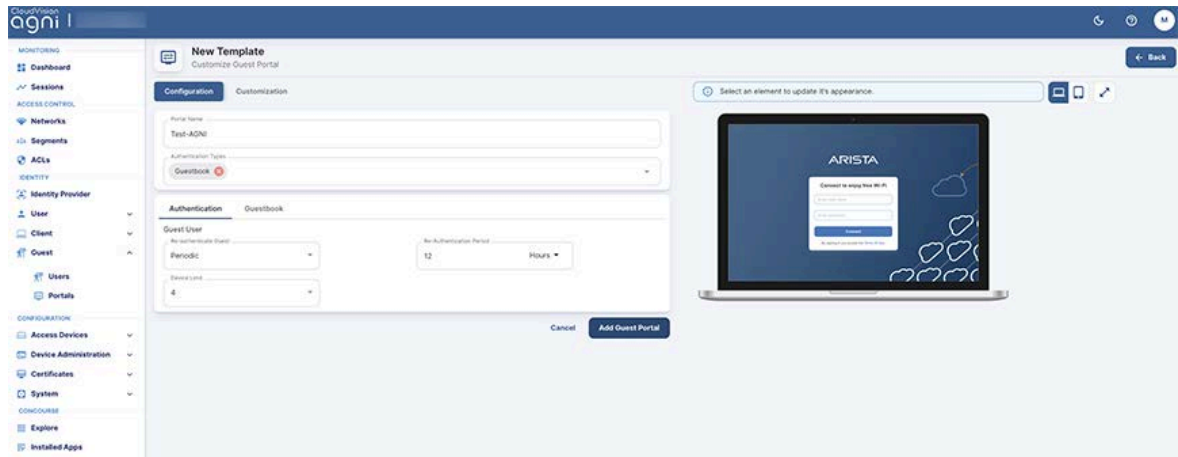
To configure AGNI for Guestbook authentication:

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

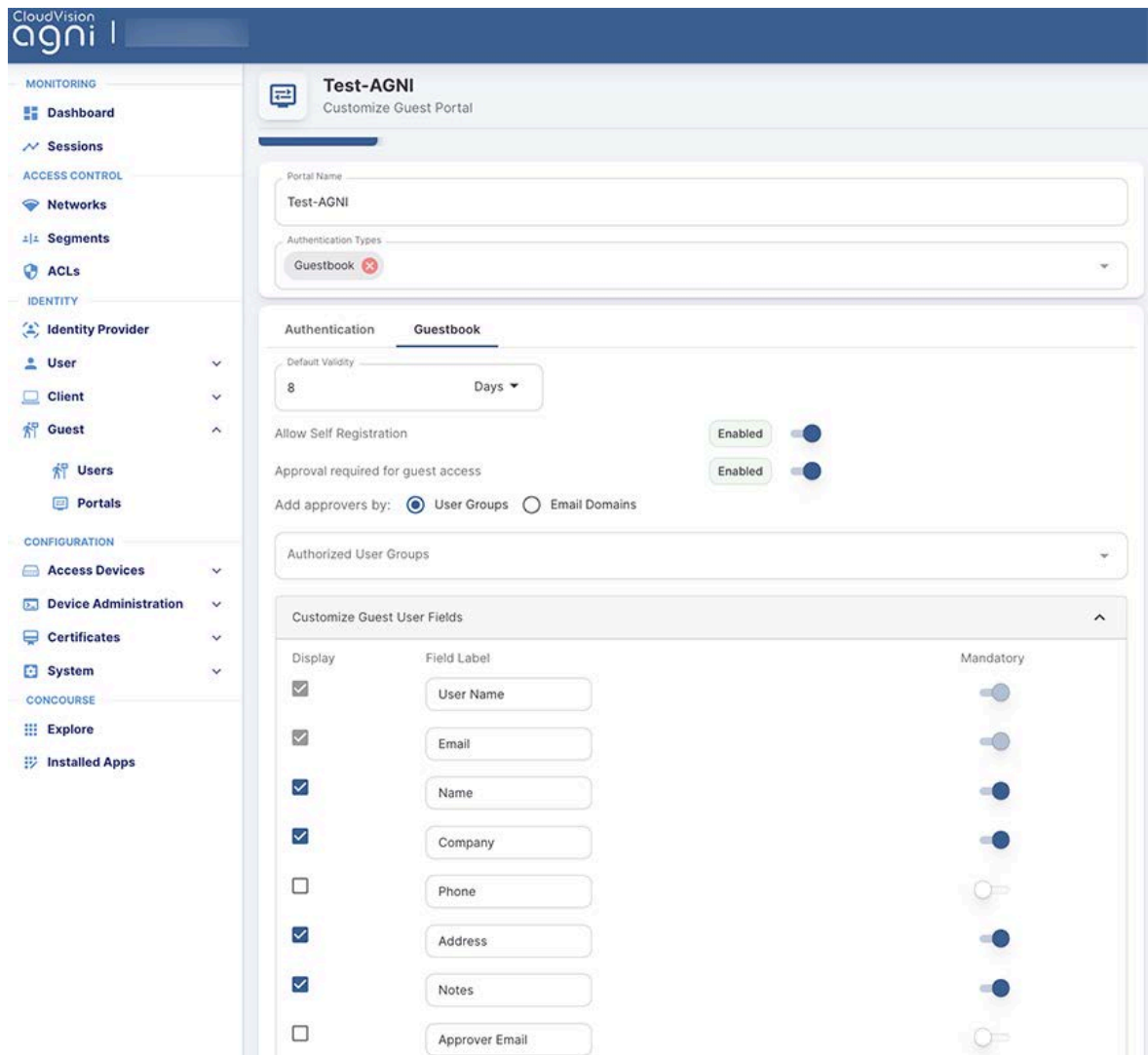
Note: The Default portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.



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:
 - a. Re-authenticate Guest - Periodic
 - b. Re-authentication Period - 12 Hours
 - c. 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.
 - a. User Name
 - b. Email
 - c. Name
 - d. Company
 - e. Address
 - f. Notes
6. Click the **Update** button.



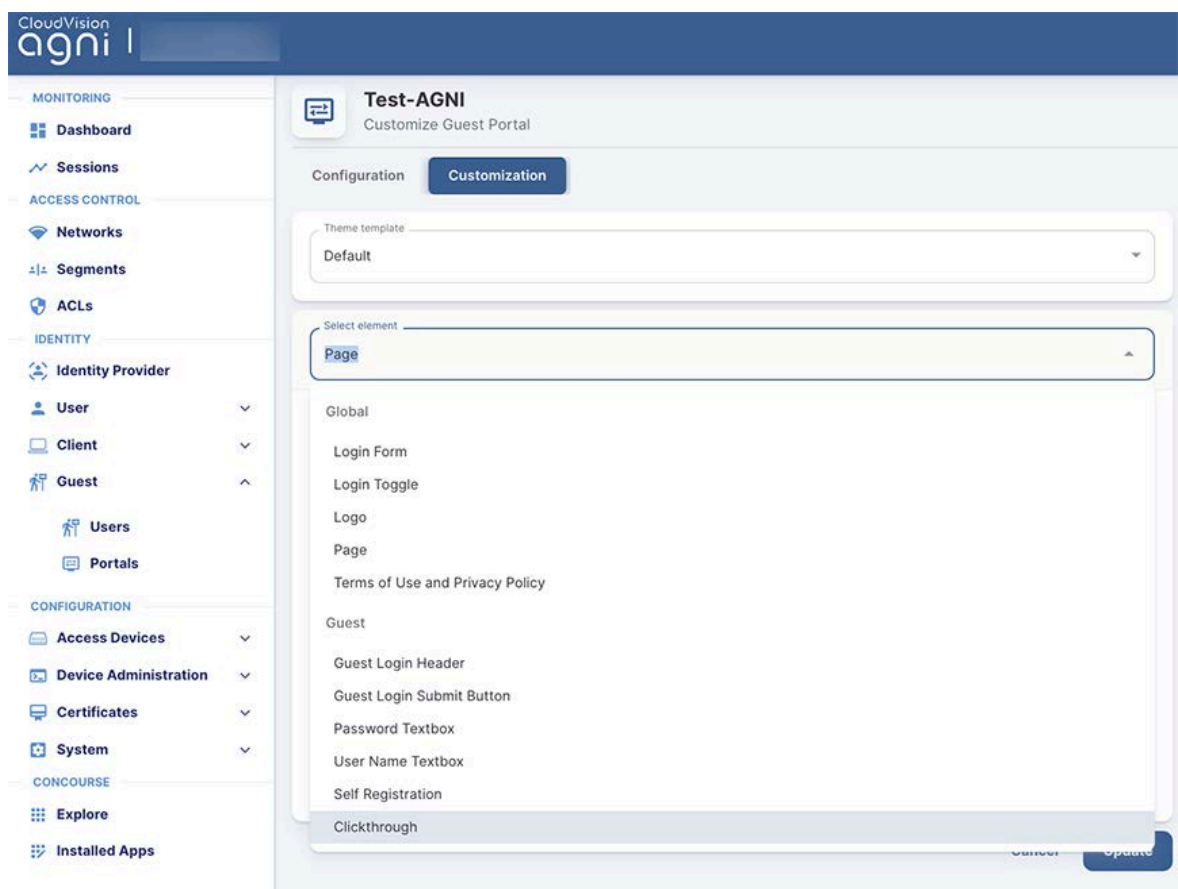
Two options are available to approve guest accounts that are created using self-registration:

- **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.
- **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".

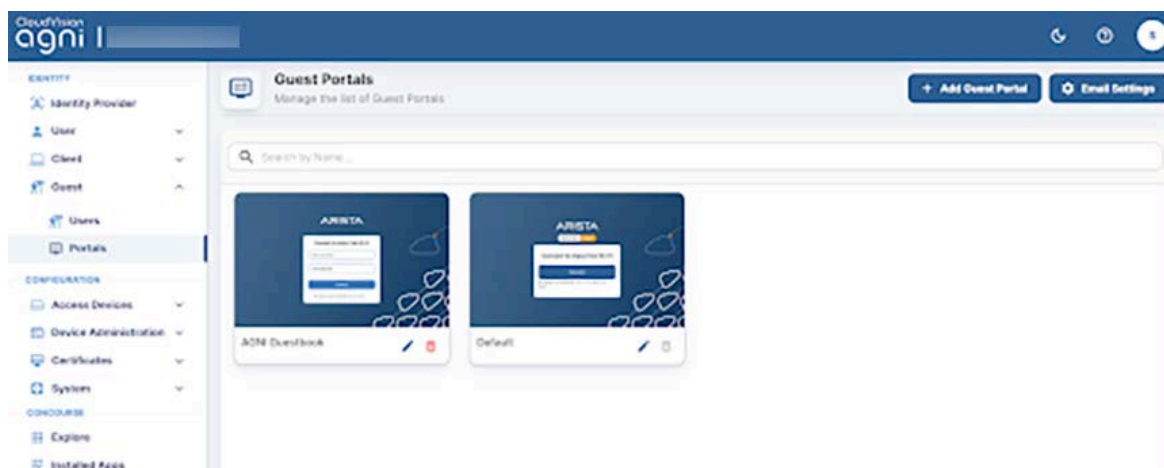
Note: Device validity should always be greater than the re-authentication period. The default value for Device Validity is 8 Hours.

7. Click the **Customization** tab to customize the portal settings, including:
 - a. Theme template
 - i. Default
 - ii. Split Screen

- b. Select element
 - i. Global
 - ii. Page
 - iii. Login Toggle
 - iv. Terms of Use and Privacy Policy
 - v. Logo
- c. Guest
 - i. Guest Login Submit Button
 - ii. User Name Textbox
 - iii. Password Textbox
 - iv. Guest Login Header
 - v. Guest Login Form
 - vi. Self Registration
 - vii. Clickthrough



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



Configuring the Network

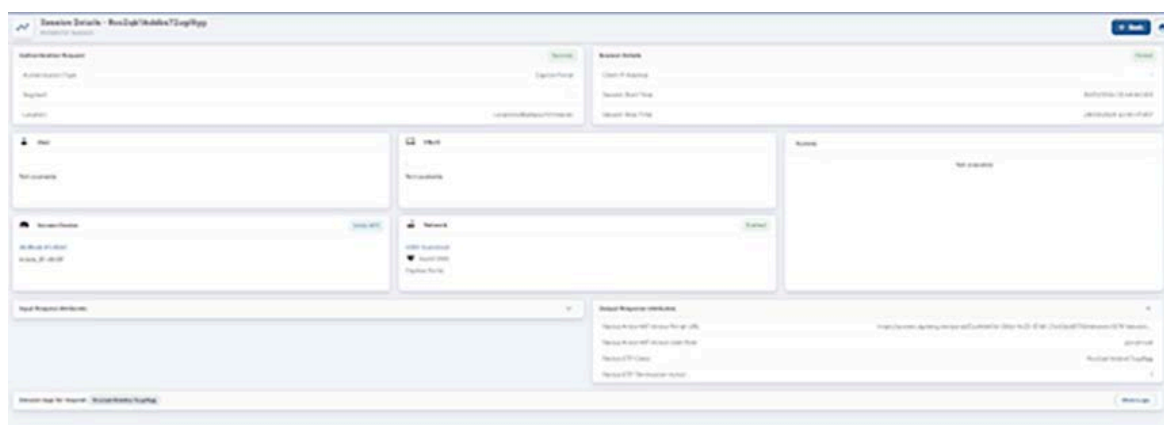
For details, see the [Configuring the Network](#) section above.

Configuring CV-CUE

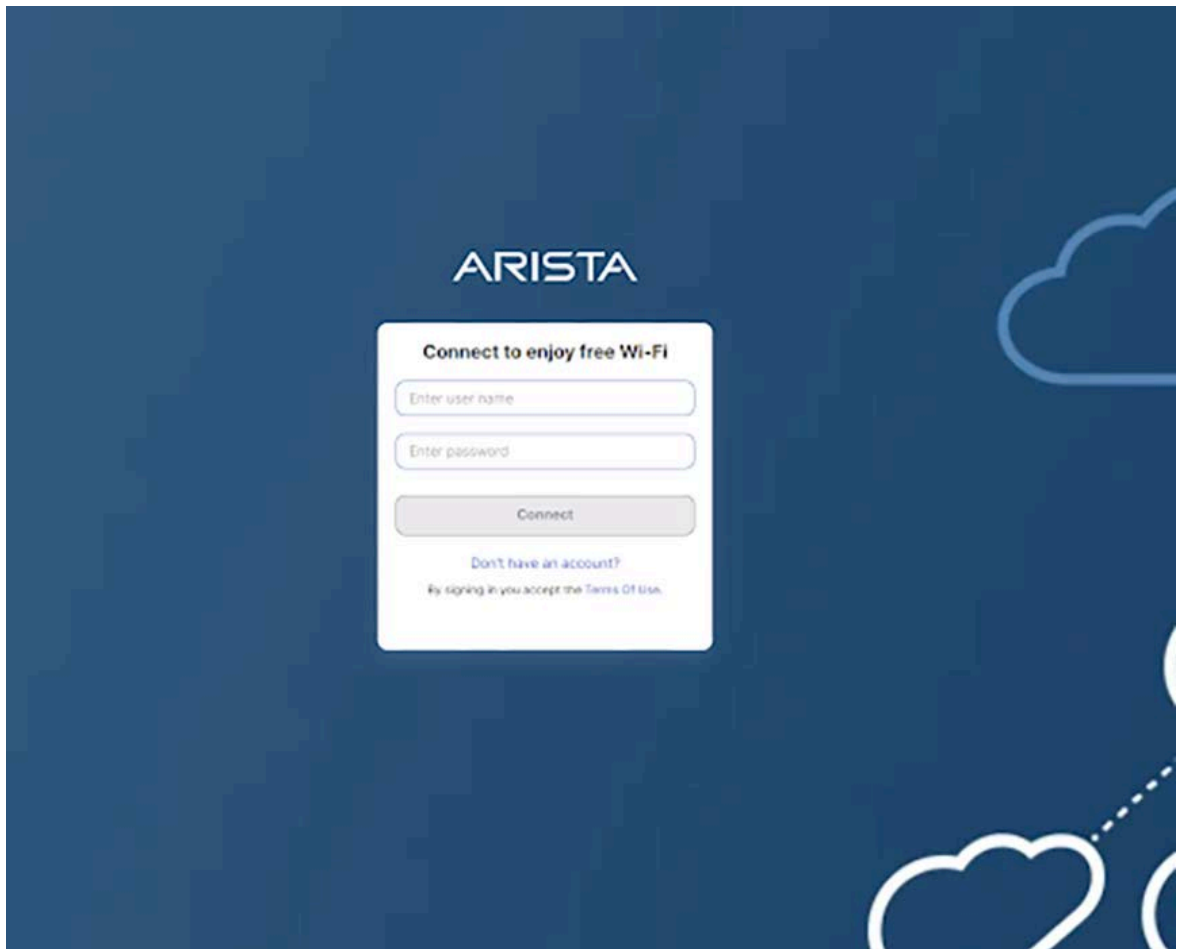
For details, see the [Configuring CV-CUE](#) section above.

User Onboarding

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.



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

A screenshot of a 'Create An Account' form. The form is white with rounded corners and is set against a dark blue background. It contains several input fields: 'User Name', 'Email', 'Name', 'Company', 'Address', 'Notes', and 'Approver Email'. The 'Notes' field is preceded by the word 'Optional'. At the bottom right of the form are two buttons: 'Cancel' and 'Register'.

Create An Account

User Name

Email

Name

Company

Address

Optional

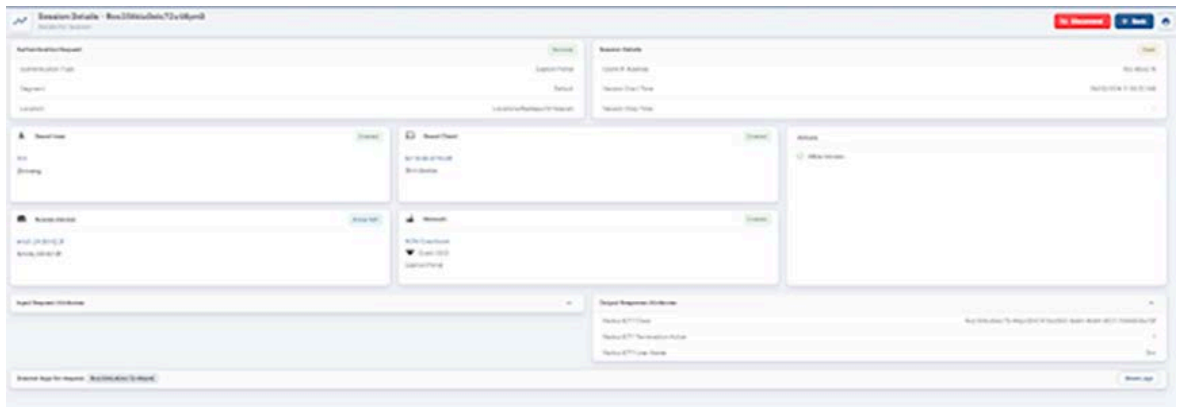
Notes

Optional

Approver Email

Cancel Register

- On clicking the **Register** button, the guest users receive an email with the following details:
 - Username
 - Password
 - Device limit
 - Valid From time in UTC
 - Valid until time in UTC
- 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)

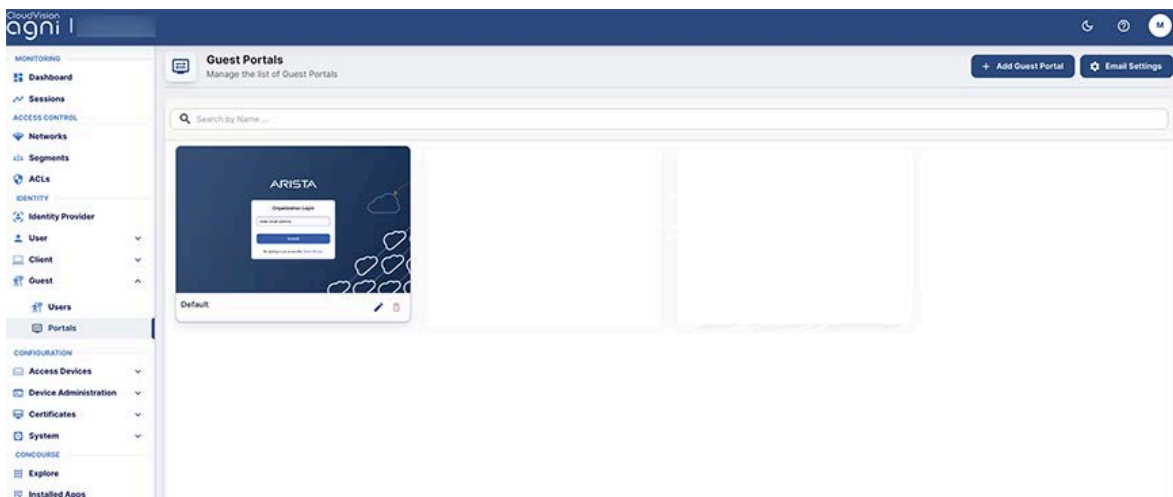
Guest management in AGNI is enabled using the Guestbook authentication type in Guest Portals. In earlier releases, AGNI supported only the Clickthrough authentication type, which allowed anonymous guest access.

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.

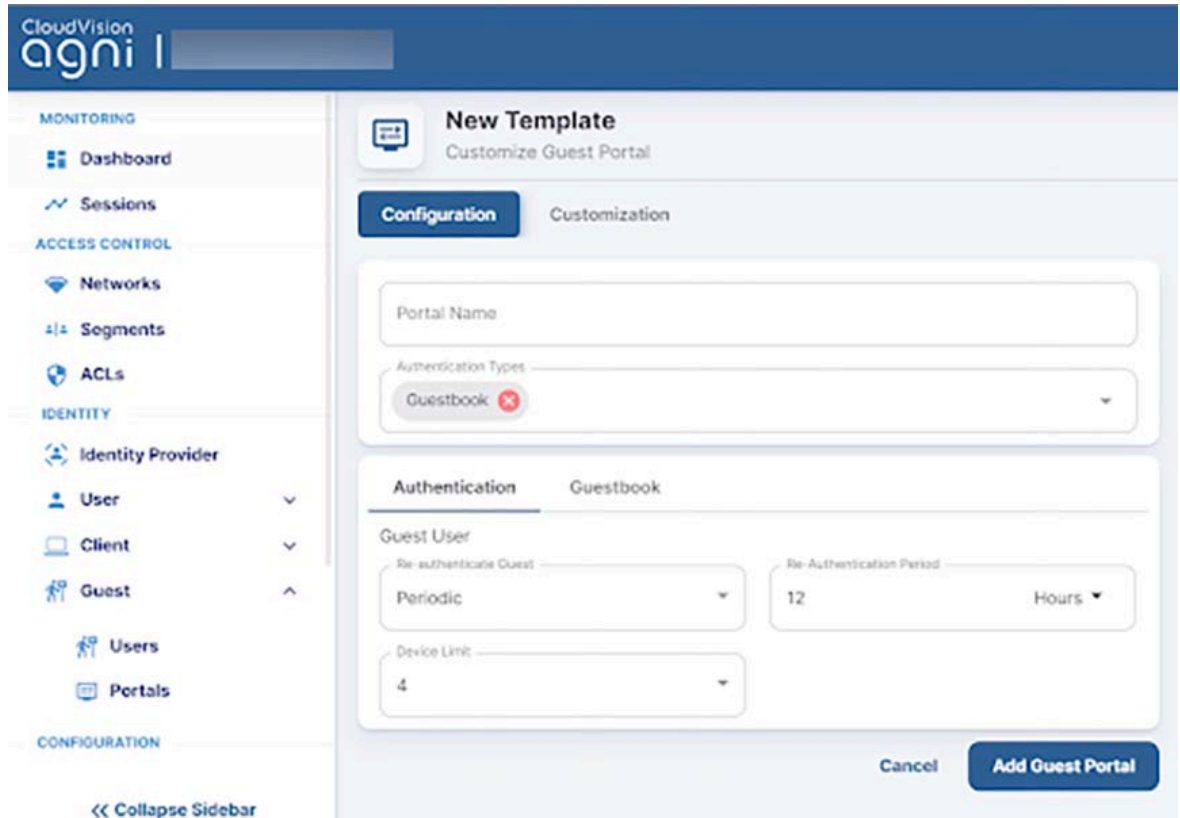
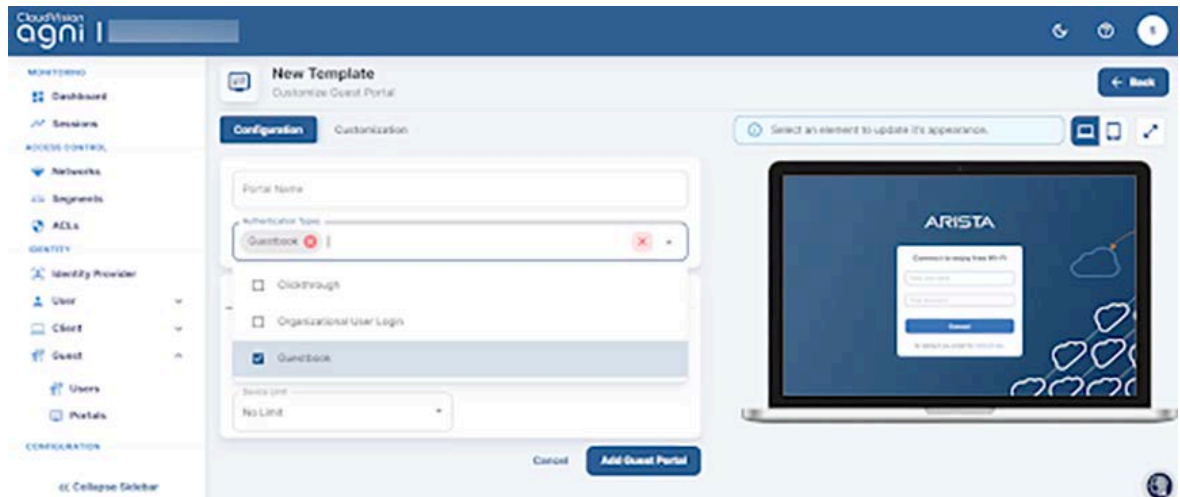
Configuring the Portal on AGNI

To configure the portal:

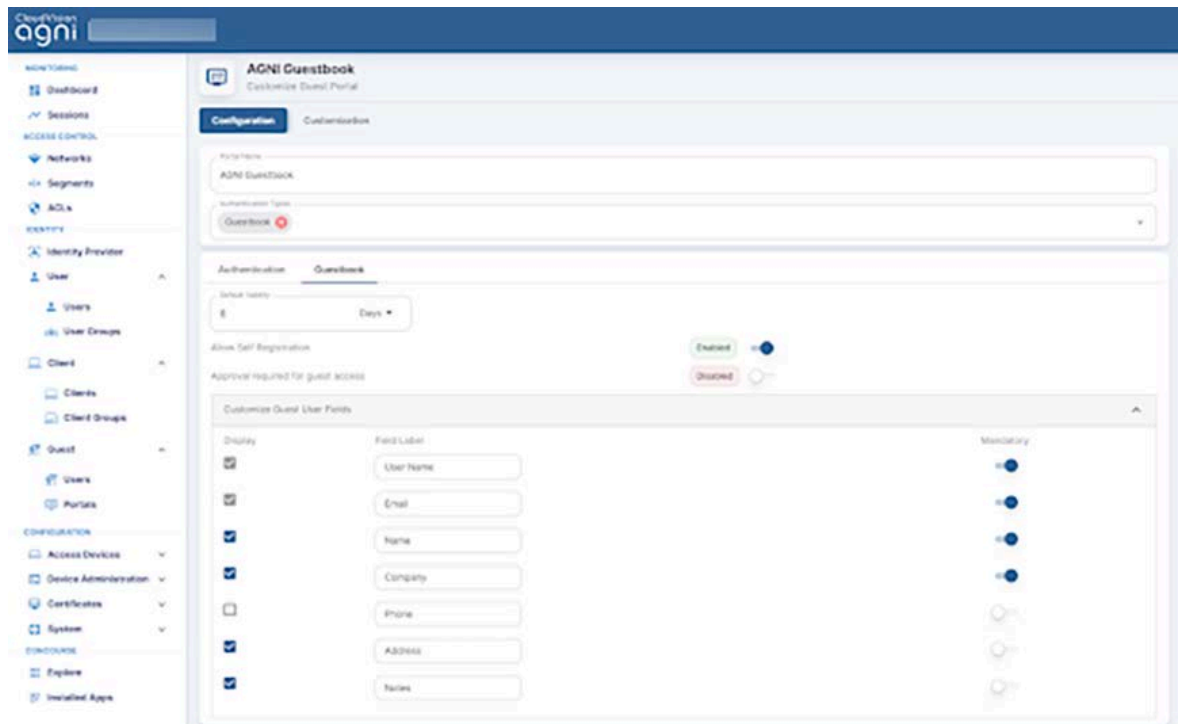
1. Log in to AGNI and navigate to **Identity > Guest > Portals**
Note: The Default portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.



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:
 - a. Re-authenticate Guest - Periodic
 - b. Re-authentication Period - 12 Hours
 - c. Device Limit - 4

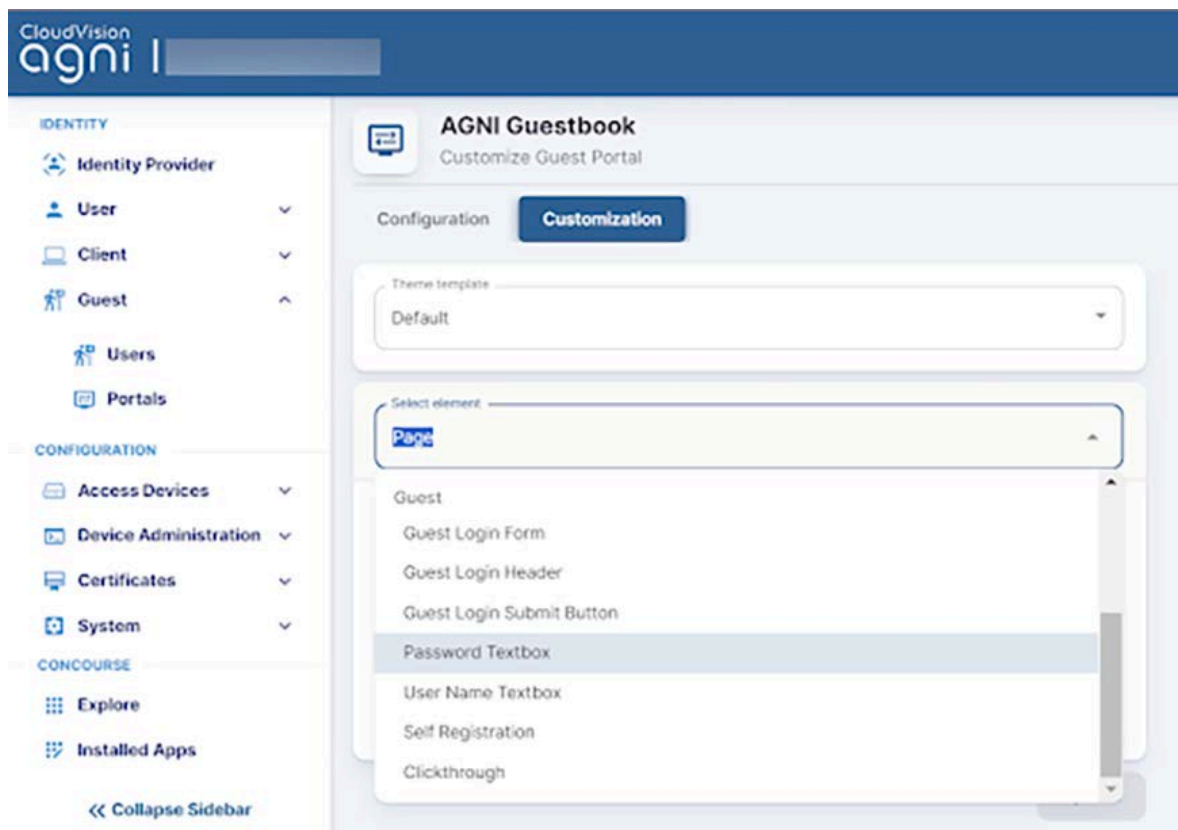
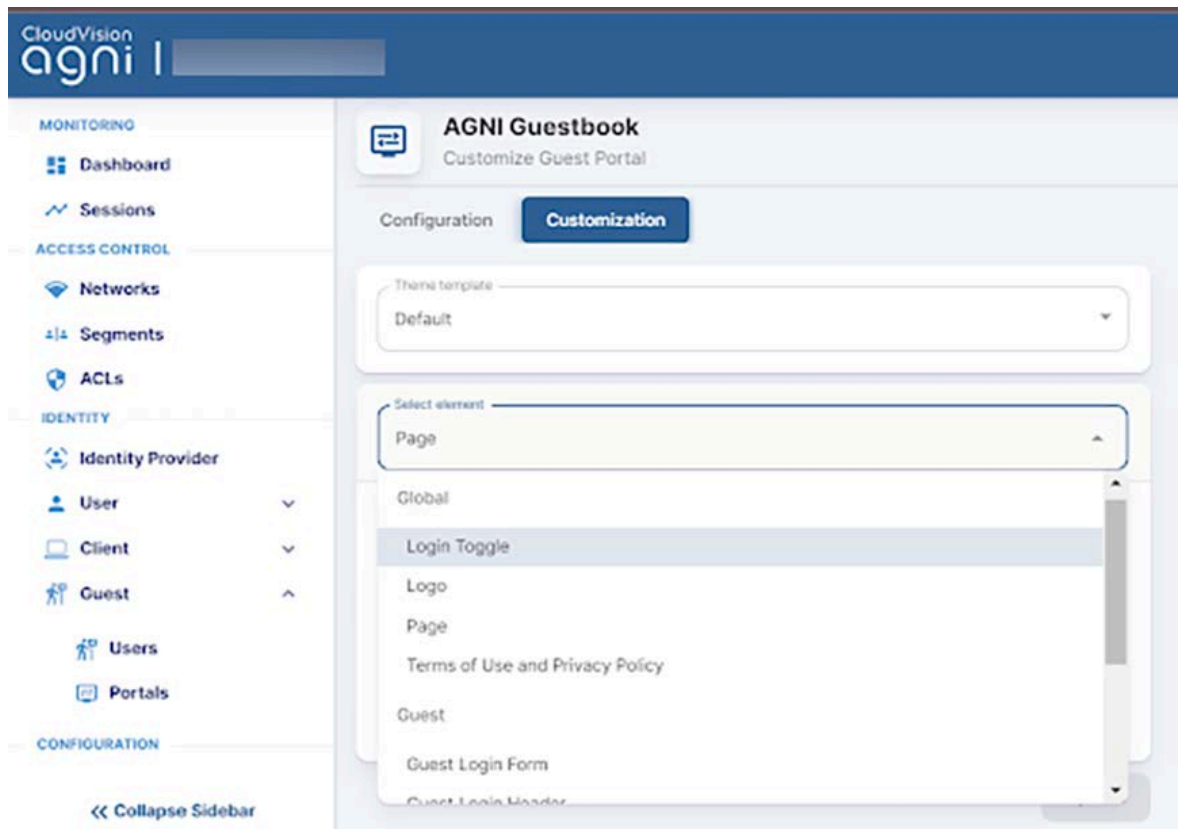


5. Navigate to Guestbook settings and configure the Device Validity for 8 Days. Keep Allow Self Registration Enabled add the following user fields:
 - a. User Name
 - b. Email
 - c. Name
 - d. Company
 - e. Address
 - f. Notes

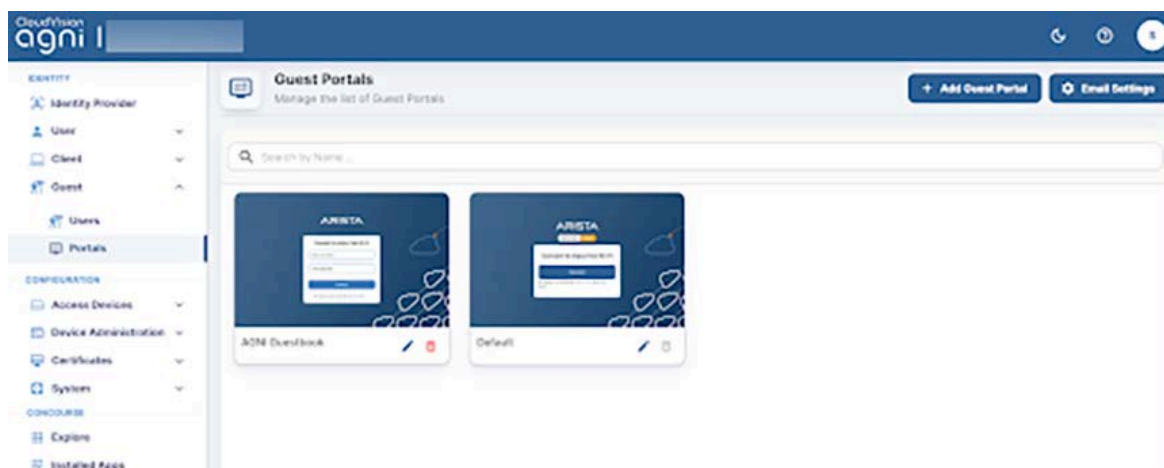


Note: Device validity should always be greater than the re-authentication period. The default value for Device Validity is 8 Hours.

6. Click the Customization tab to customize the portal settings:
 - a. Theme template
 - i. Default
 - ii. Split Screen
 - b. Select element
 - i. Global
 1. Page
 2. Login Toggle
 3. Terms of Use and Privacy Policy
 4. Logo
 - ii. 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



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



Configuring the Network

For details, see the [Configuring the Network](#) section above.

Configuring CV-CUE

For details, see the [Configuring CV-CUE](#) section above.

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

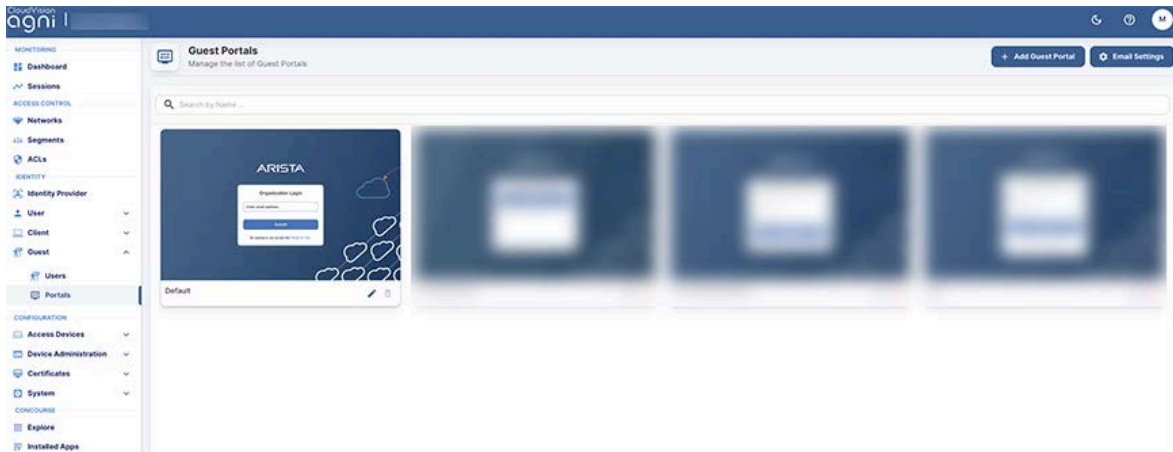
For details, see the [User Onboarding](#) section above.

Configuring Guest Portal in AGNI for Wired Clients

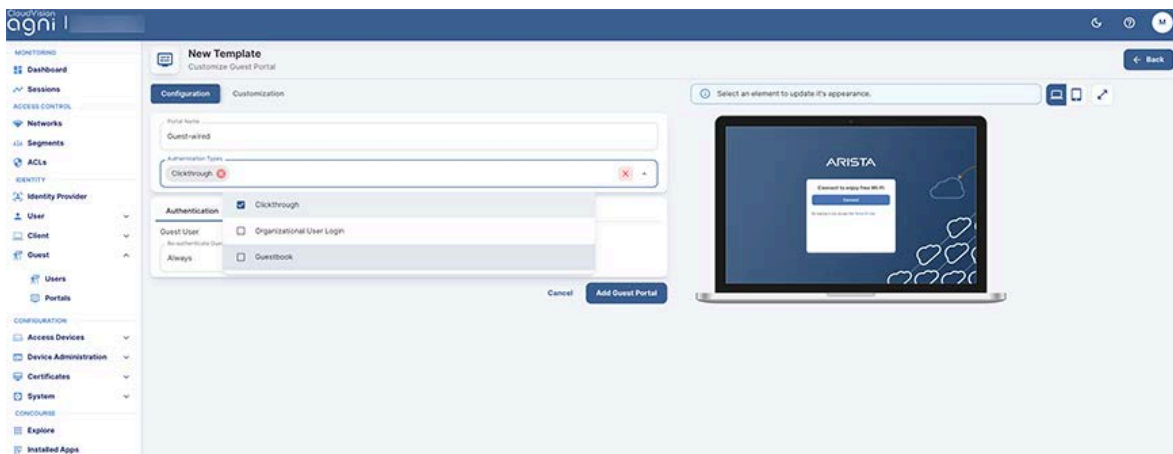
This section describes the steps to configure the guest portal using AGNI for wired clients. To configure the guest portal, you must configure AGNI and the switch.

Configuring AGNI

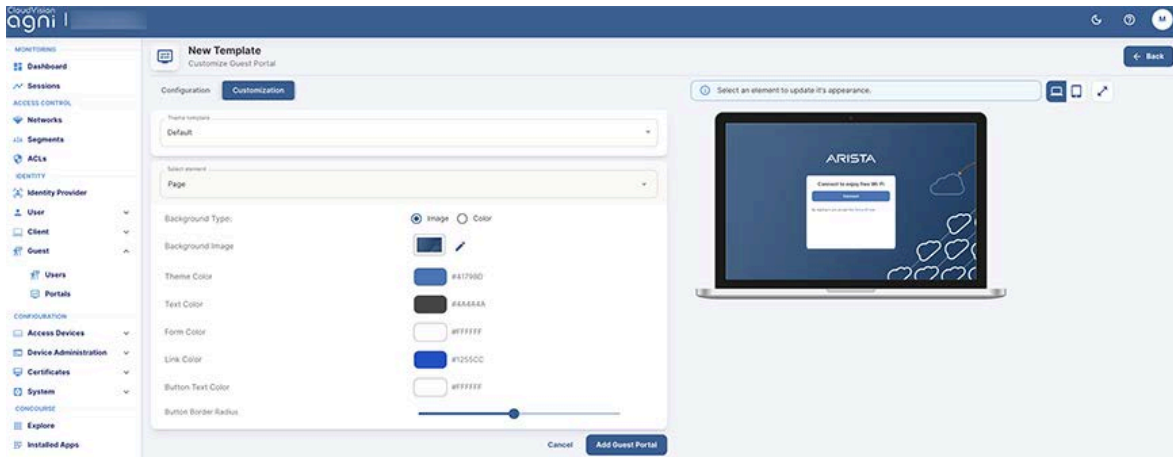
- Log in to AGNI and navigate to **Identity > Guest > Portals**.



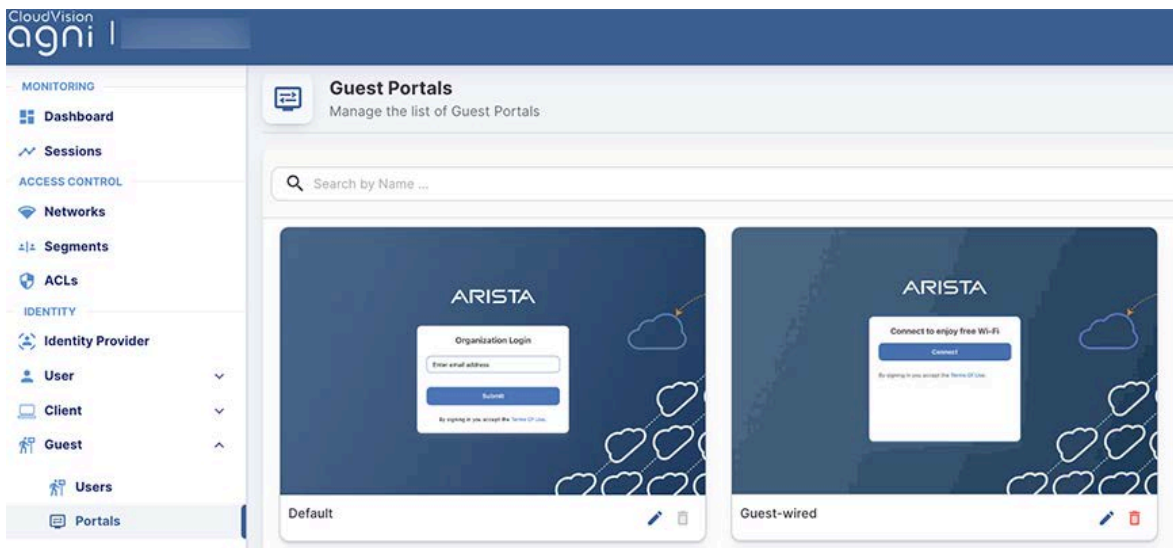
- Click the **Add Guest Portal** button.
- In the **Configuration** tab, provide the portal name and select the theme of the portal. The available theme options are Default or Split Screen.



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



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



- Navigate to the **Access Control > Network**. Click **Add Network** button.
- Add a new network with the 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
- Click **Add Network**.
- Edit the added network and copy the portal URL.

CloudVision agni

MONITORING

- Dashboard
- Sessions

ACCESS CONTROL

- Networks
- Segments
- ACLs

IDENTITY

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

CONFIGURATION

- Access Devices
- Device Administration
- Certificates
- System

CONCOURSE

- Explore
- Installed Apps

Guest-wired
Provide the following details to update the selected Network

← Back

Name: Guest-wired

Connection Type: ☐ Wireless ☒ Wired

Access Device Group: [dropdown]

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

Status: Enabled

Authentication

Authentication Type: Captive Portal

Captive portal type: ☒ Internal ☐ External

Select internal portal: Test-AGNI-Docs [Preview]

Captive Portal

Initial ACL For Portal Authentication: guest-acl [Show Domains]

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

https://qa.agnienet.net/portal/Ea613f9d9-2a76-44d3-ba16-2e27e944e045/network/810 [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
!
```

Configuring Guest Portal Using Guestbook (Wired)

This section describes configuring the guest portal with the Guest Book authentication method for wired clients. You must configure both AGNI and the Arista Switch to configure the guest portal.

For details, see the [document](#).

Configuring Guest Portal Using Guestbook-Host Approval (Wired)

This section describes configuring the guest portal with the Guest Book authentication method for wired clients in AGNI. You must configure both AGNI and CV-CUE to configure the guest portal.

For details, see the [document](#).

Configuring Guest Portal Using Self-Registration (Wired)

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 section describes configuring the guest portal with the Guestbook authentication type for wired clients. You must configure both AGNI and CV-CUE to configure the guest portal.

For details, see the [document](#).

Generating Client Certificates for RadSec

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).

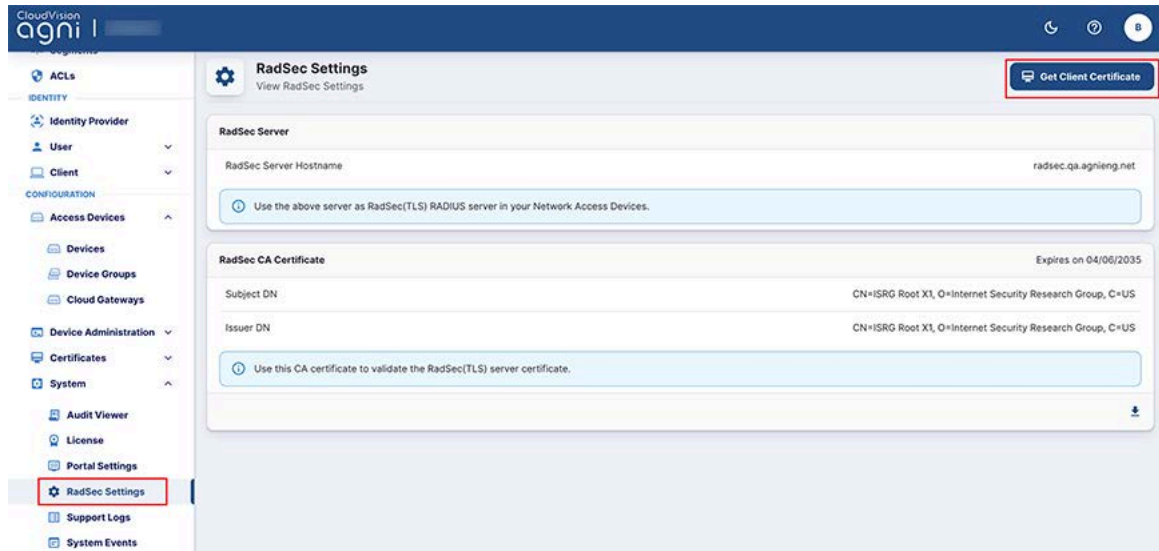


Figure: RadSec Settings Certificate Generate Page

OR

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

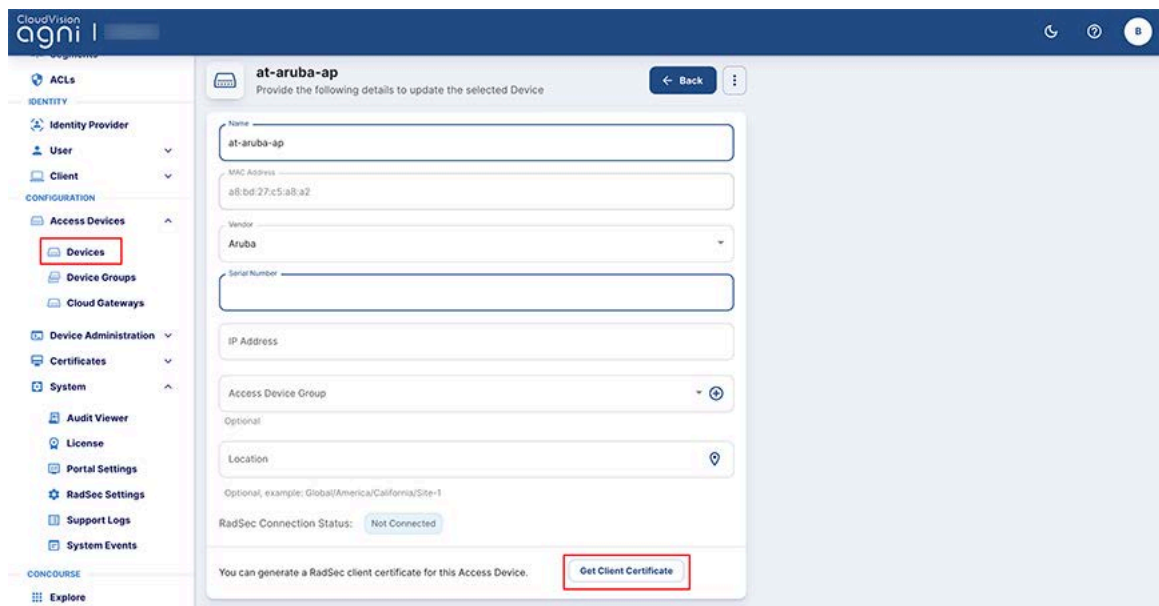


Figure: Device Settings Certificate Generate Page

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.

The screenshot shows the 'Generate RadSec Client Certificate' page in the CloudVision AGNI portal. The left sidebar contains a navigation menu with 'RadSec Settings' highlighted. The main content area has a title 'Generate RadSec Client Certificate' and a subtitle 'Fill in the details to generate RadSec client certificate for the Access Device'. There are three radio buttons for 'Generate Certificate': 'Generate' (selected), 'Use CSR (Single Device)', and 'Upload Zip with multiple CSRs'. Below these are input fields for 'Access Device', 'Password', and 'DNS Names'. A 'Generate Certificate' button is located at the bottom right of the form.

Figure: RadSec Client Certificate Generating Options

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

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

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.

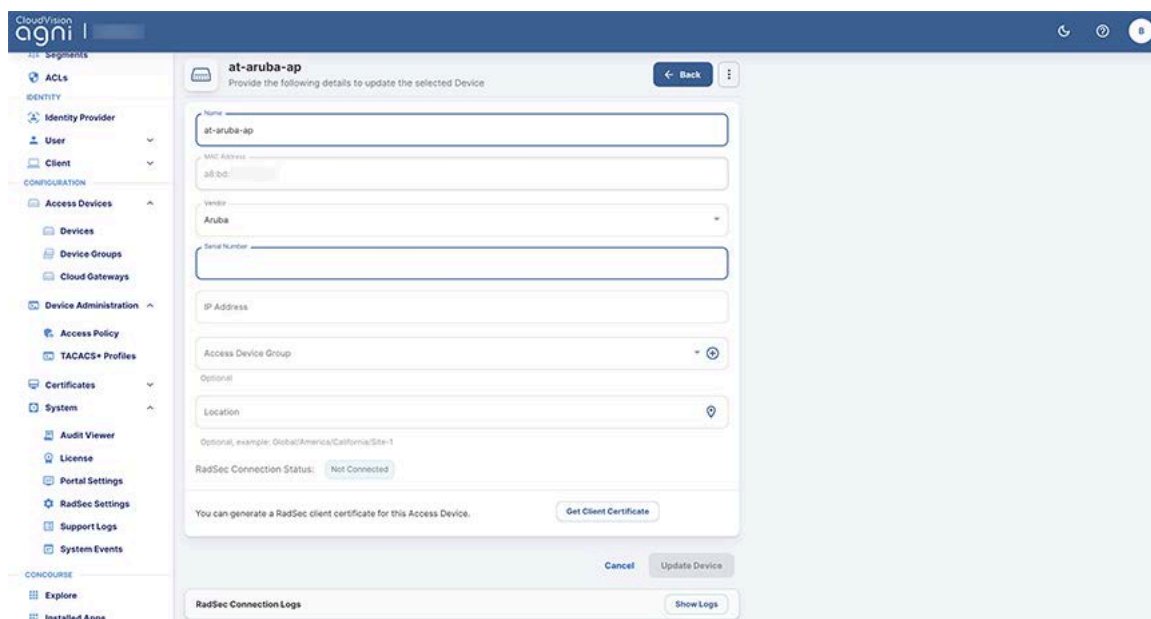


Figure: Device Details

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.

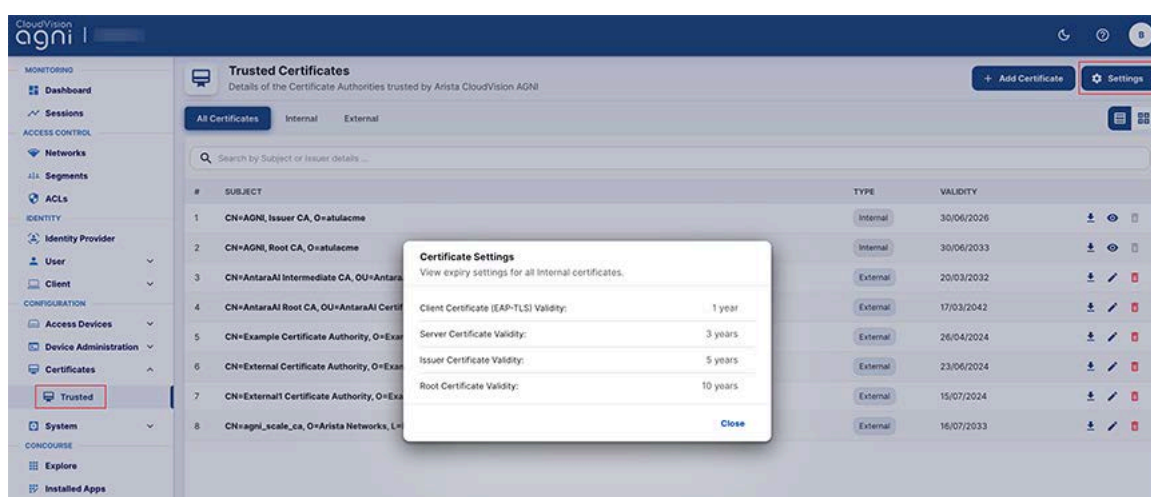


Figure: Trusted Certificates

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.

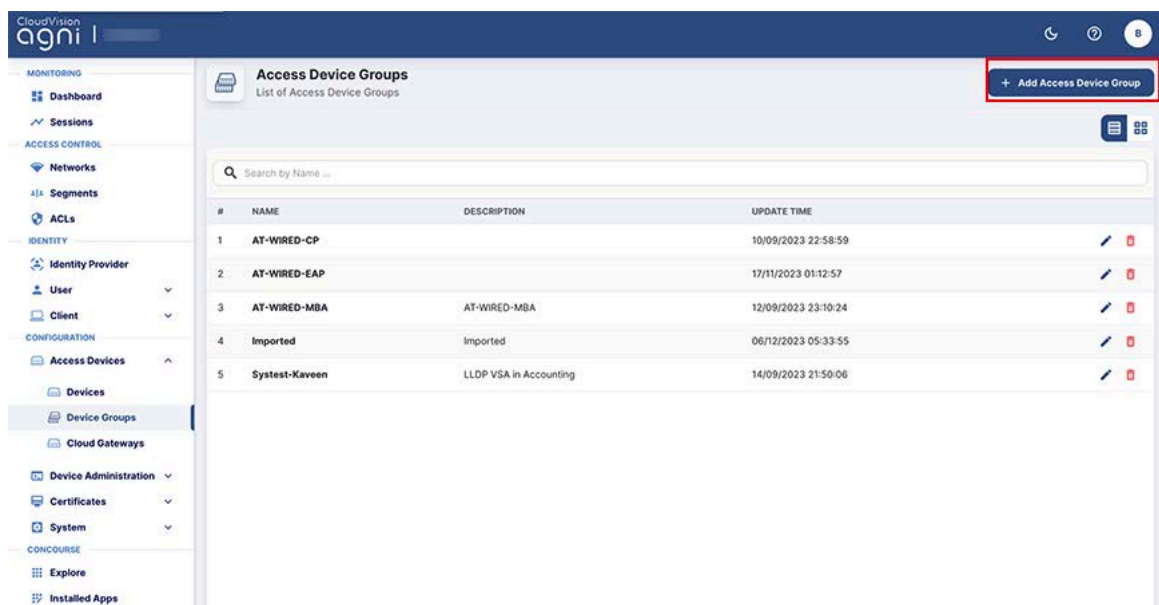
For external PKIs, the system supports certificate revocation checks either by querying the URL or statically checking against the revocation list.

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 wired Network Configuration and in the Segment conditions to enforce network access policies.

To add a Device Group:

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



- On the Add Access Device Group page, enter a device group name and click **Add Access Device Group** button. (see image below). You can add the devices from the Available Devices tab.

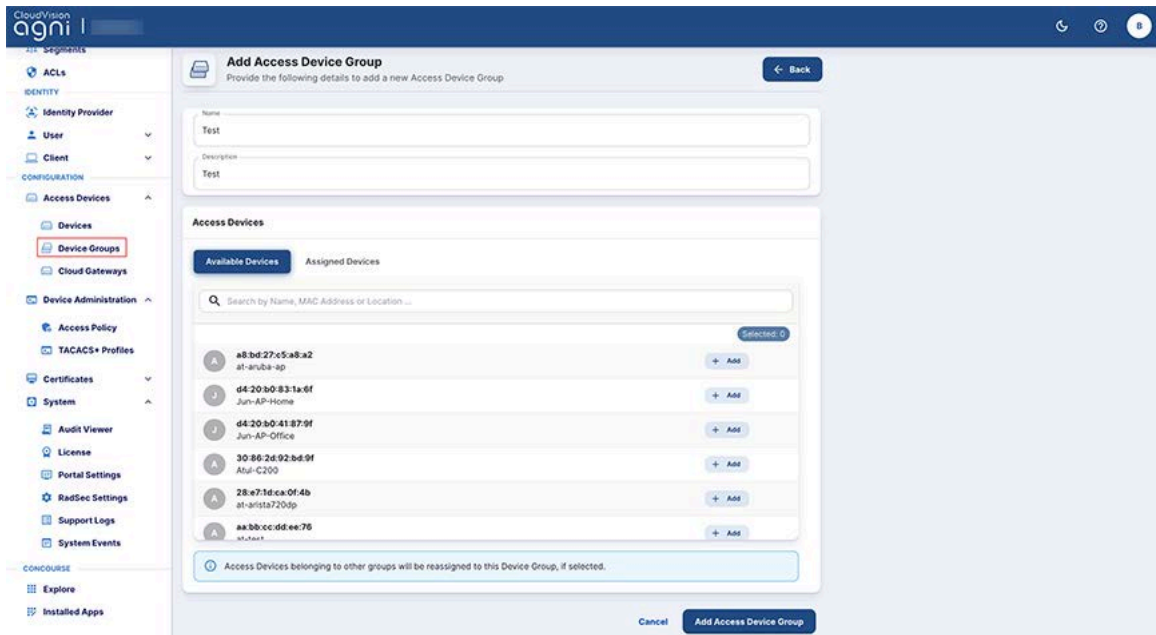


Figure: Adding Access Device Groups

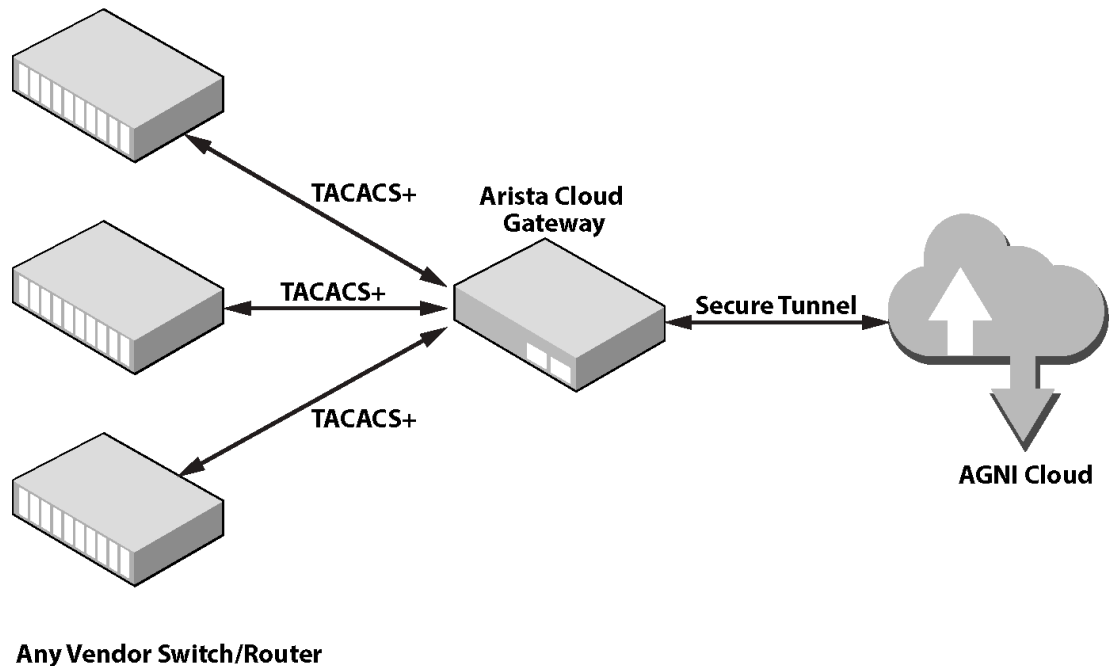
Configuring TACACS+ with AGNI

This section explains the process of configuring TACACS+ with AGNI. Before configuring TACACS+ with AGNI the 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.



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-centrall-docker.pkg.dev/agni-eng-common/agni-public/acc:
  1.3 &
```
4. Validate **Port 67** is running on the client machine where you have installed Docker.

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



```

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

```

Debugging Workflow

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

```

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

```

```

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

```

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

```


other than port 49), use the CLI command below:

```
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.agnienet.net/acg/connect
```

Figure: 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

[Add Secret](#)

[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

Cloud Gateway-1

Location

San Jose

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

Connection Status:

Not Connected

Copy the generated token into the Cloud Gateway.

Token

eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IklvYTYxZDE4OS11MzYxLTQ4MzctYTExNi0xODI1NzU0MjB

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
AristaSwitch

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

← Back

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

← Back

Name: Cloud Gateway-1

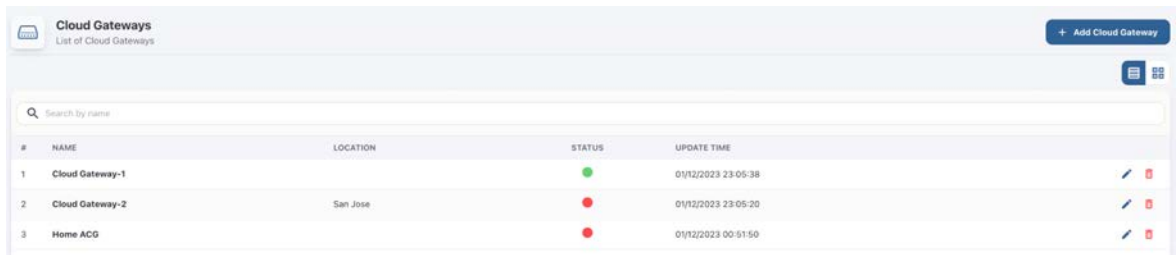
Location:

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



The screenshot shows a web interface titled "Cloud Gateways" with a sub-header "List of Cloud Gateways". There is a search bar and a table with the following data:

#	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
```

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
```

Note: The above command output displays that the Arista Cloud gateway is successfully connected with AGNI and is listening on TCP port 49 for TACACS+ requests. See output details in the images below (Figure: Command Output):


```
IN-MH04-PL-SW02(config)#show daemon AristaCloudGateway
Agent: AristaCloudGateway (running with PID 6987)
Uptime: 0:02:23 (Start time: Tue Dec 12 07:41:15 2023)
Configuration:
Option                               Value
-----
AGNI_API_TOKEN                       eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJvcmdJRCI6IkdVYTYxZDE4OS1mZyXLA\
TQ4MzctYTExNi0xODI1NzU0MjBjZmIiLCJ0b2t1bklEIjoIURURDTFmWU0JTSVFNvbkM3MlM\
1SkNOMCI6ImZyI6IkhFTkklLCJhdWQiOiJBQ00cgRGV2aWNNIiFRva2VuIiwiaXhwIjoIm\
jEzYmI0xMS0xOFQwNzozOToyNy41NTU3OTIxOTVaIiwiaWF0IjoImjAyMy0xMjU0MlQwNzoz\
zOToyNy41NTU3OTUxNDI1Iiwic2NvcGVzIjpbImkZM50aXR5LnNsaWVud3C5wcm9naWx1I\
iwiaWRIbnRpdHkuY2xpZW50LnByb2ZpbGUudXBkYXRlIiwiaWF0Ij0iImF0dHJzIjpbImF\
jz0RldmljZU1EIjoIzjc2MDk3NjItODIyMy00ZTEyLTgwZDktNWVud3C5wcm9naWx1I\
2xlc3Rlc2N1IiwiaWF0Ij0iImF0dHJzIiwiaWF0Ij0iImF0dHJzIiwiaWF0Ij0iImF0dHJz\
.JjtBvKrFnkg7lLuett1NF-Vnsm8PzipAzQymUL3fT_FqR7bcyt9as5BIO4FnkPJeBx8JE\
SrT7luFA5LyL_18Pw

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

IN-MH04-PL-SW02(config)#
```

```
IN-MH04-PL-SW02(config)#show extensions
Name                               Version/Release   Status   Extension
-----
AristaCloudGateway-1.0.0-1.swix   1.0.0/1           A, I     1

A: available | NA: not available | I: installed | F: forced | B: install at boot
S: valid signature | NS: invalid signature
The extensions are stored on internal flash (flash:)
IN-MH04-PL-SW02(config)#
```

Figure: Command Output

Enabling Device Administration on AGNI

For TACACS+ to function correctly, enable Device Administration on AGNI and specify the authorized user groups. Users belonging to the authorized user groups should log in to the Device Administration portal using their SSO and generate an SSH Password. Using this SSH password, administrators can log in to the managed devices using TACACS+.

You can add multiple user groups in the Authorized User Groups field. To enable Device Administration:

- Navigate to **Device Administration > Access Policy**.
- Select the Enable Device Administration **Enabled** button (see image below).
- Select user groups by selecting the Authorized User Groups.
- Select the SSH Passphrase Validity (in days)
- Click on the **Update** button.

Note: The administrator can set the validity period of the TACACS token for a period ranging from 1 to 365 days. This helps the administrator to login to devices periodically without logging in to the self-service portal.

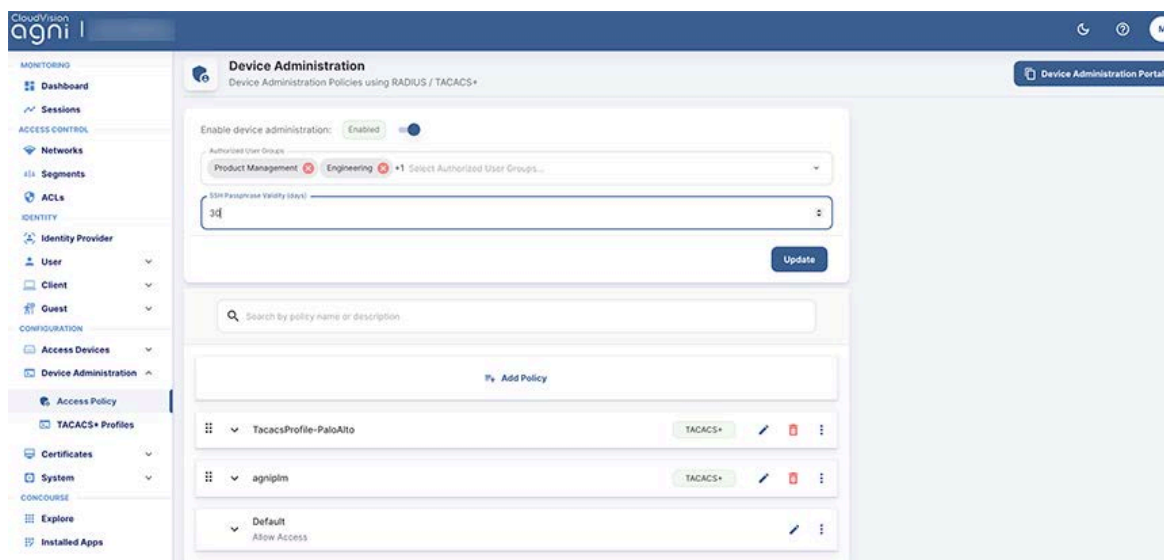


Figure: Device Administration Enabled and Passphrase Validity

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).

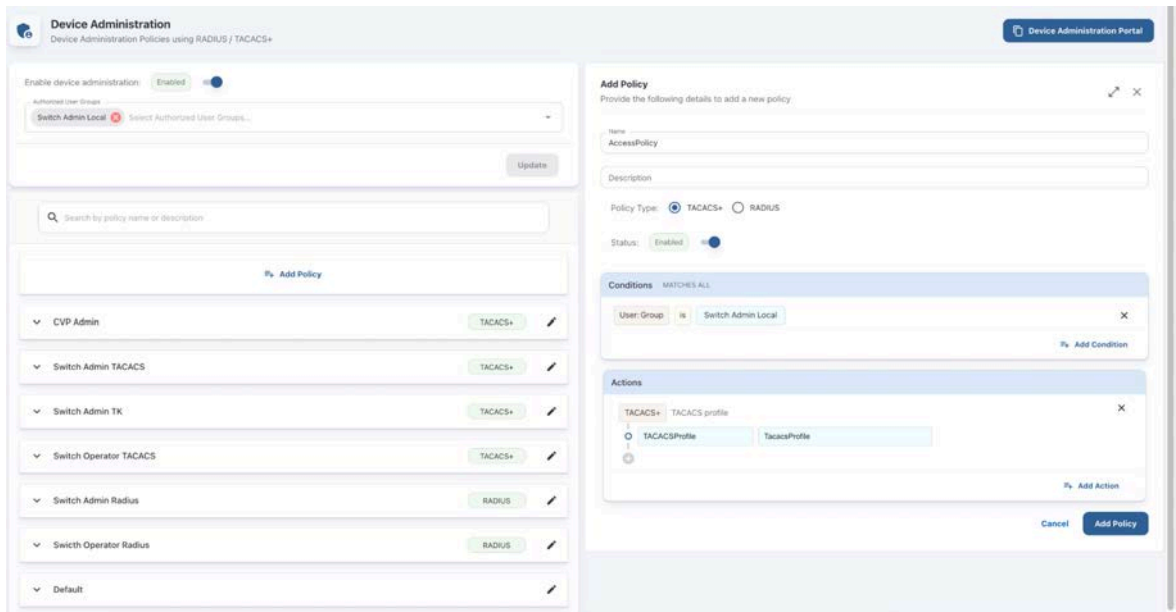


Figure: Creating TACACS+ Profiles

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

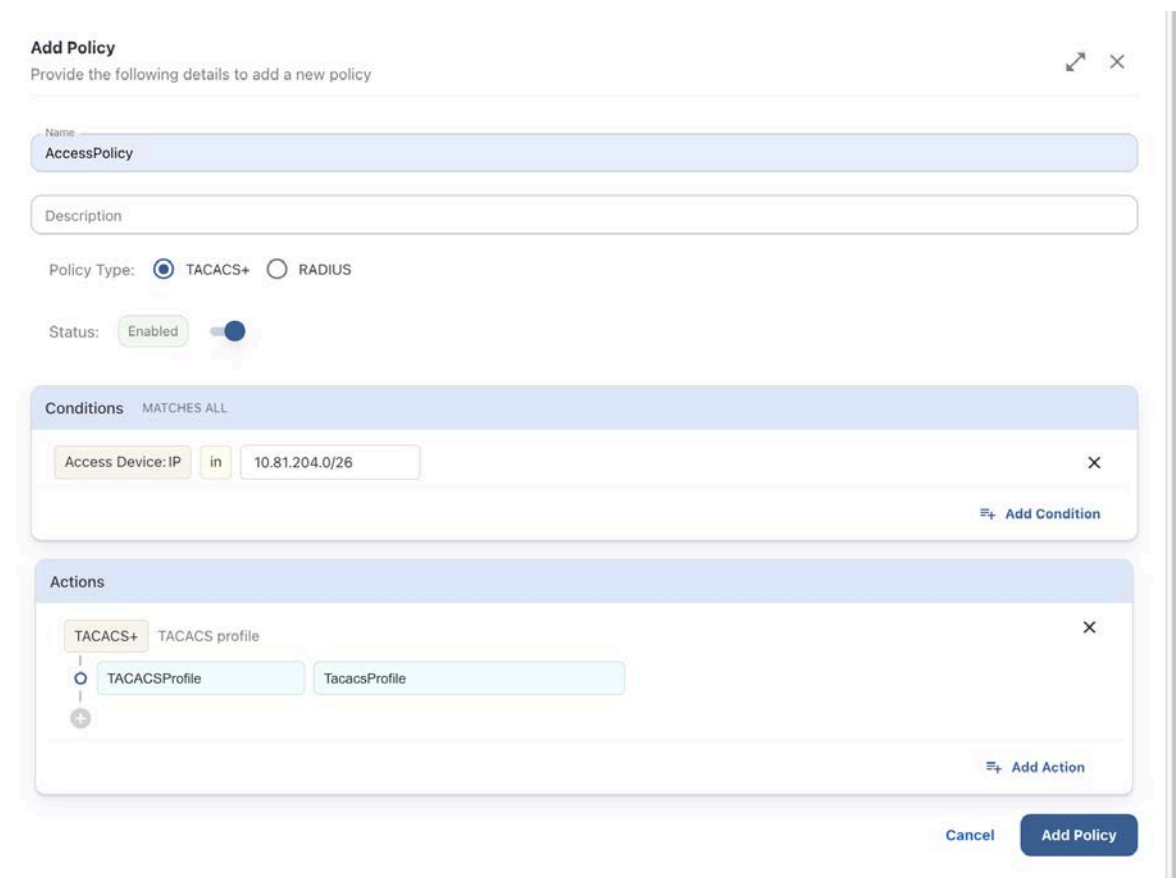


Figure: Creating TACACS+ Policy Details

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 → Device Administration → Show Details (eye icon):

Session Details - Tc1nm60c88nsc72qekc50
Details for Session
Back

Authentication Request
Success

Authentication Type
TACACS+

Policy
Switch Admin TACACS

Location
San Jose

Request Details

NAS IP Address
10.81.204.5

Request Time
05/12/2023 23:20:57.448

TACACS+ Profile Name
TacacsProfile

User
Enabled

Access Device
Not available

Cloud Gateway
Connected

Input Request Attributes

Output Response Attributes

TACACS+ Activity
Show Activity

Session logs for request: Tc1nm60c88nsc72qekc50
Show Logs

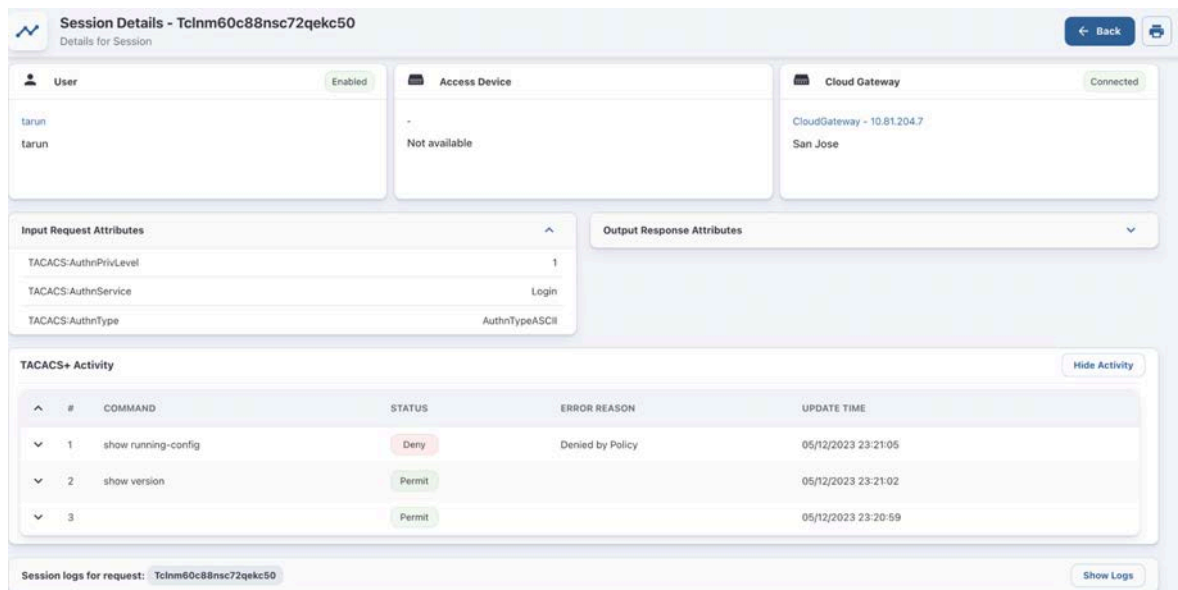
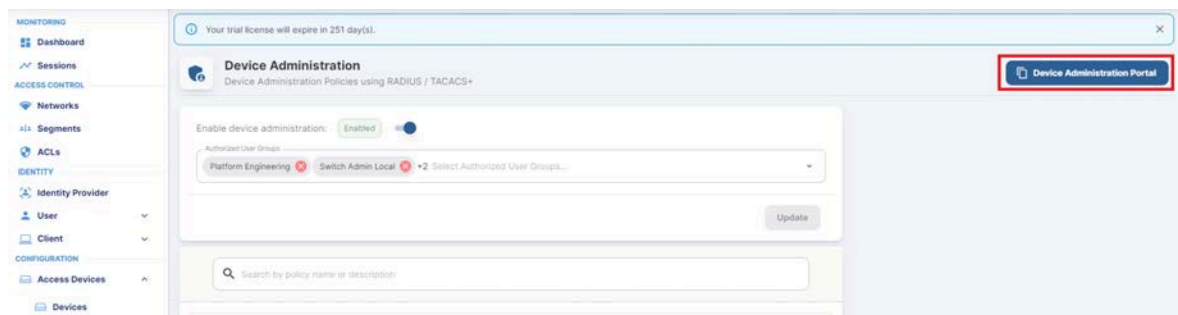


Figure: TACACS+ Session Details

Accessing Self Service Portal on AGNI

To access the Self-Service Portal, the 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.

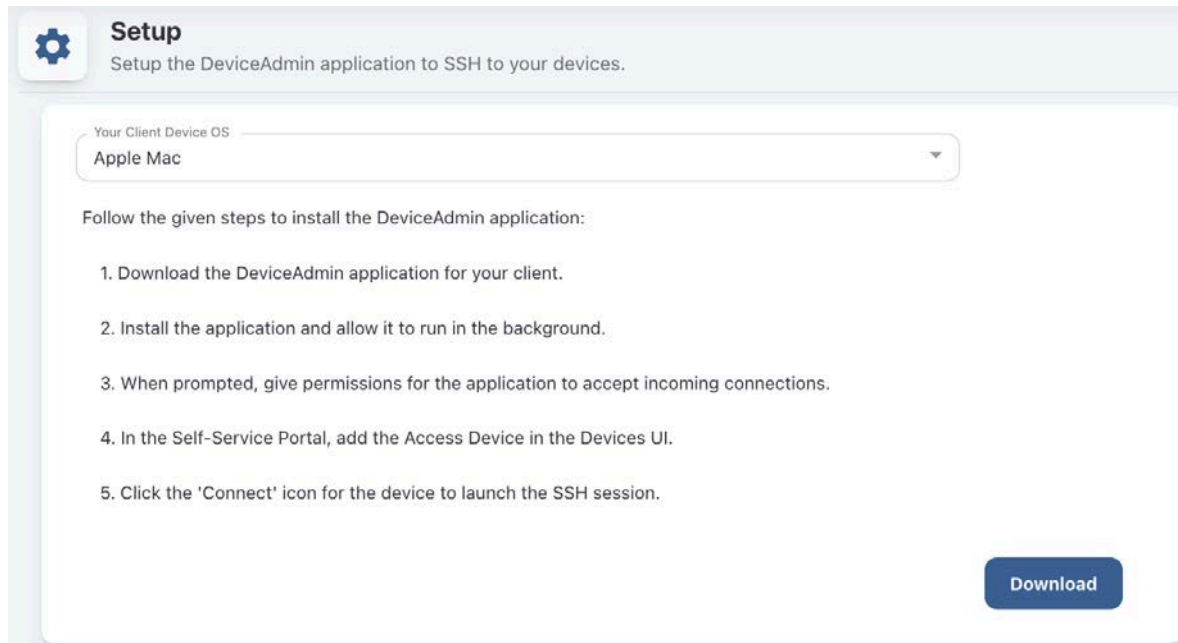


Figure: Self-Service Portal for Mac OS

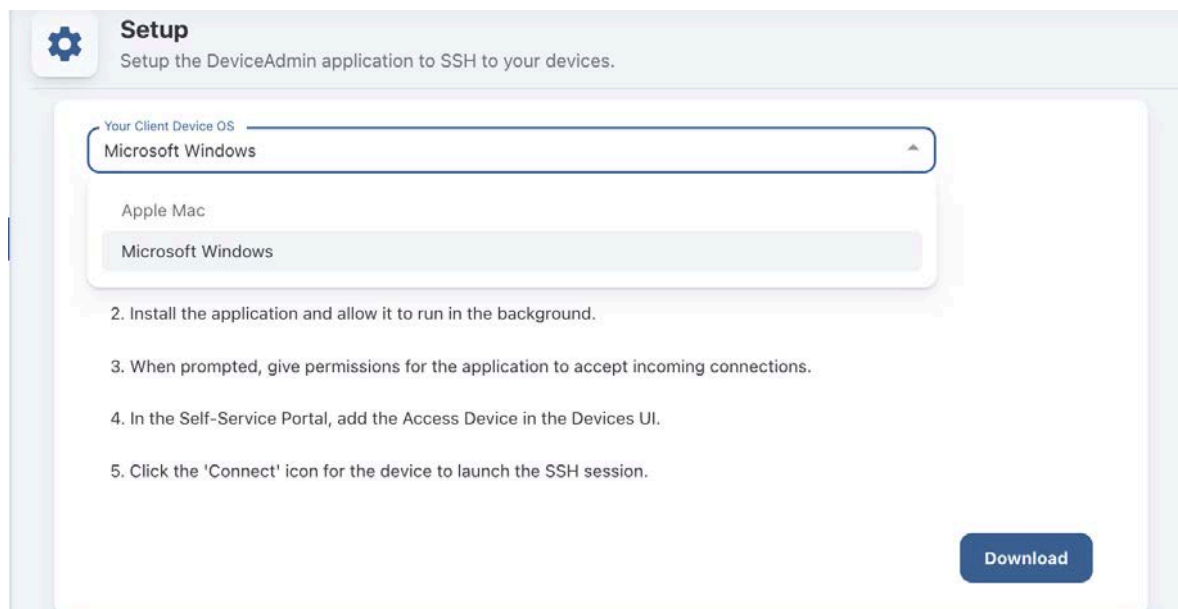


Figure: Self-Service Portal for Windows

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 Login 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 Device Login Credentials that is valid for the duration allowed by the administrator (see the Enabling Device Administration on AGNI section).

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

Generate the Device Login Credentials using the Self-Service portal.

The self-service portal can be customised to suit the customer's theme and logo. (see images below).

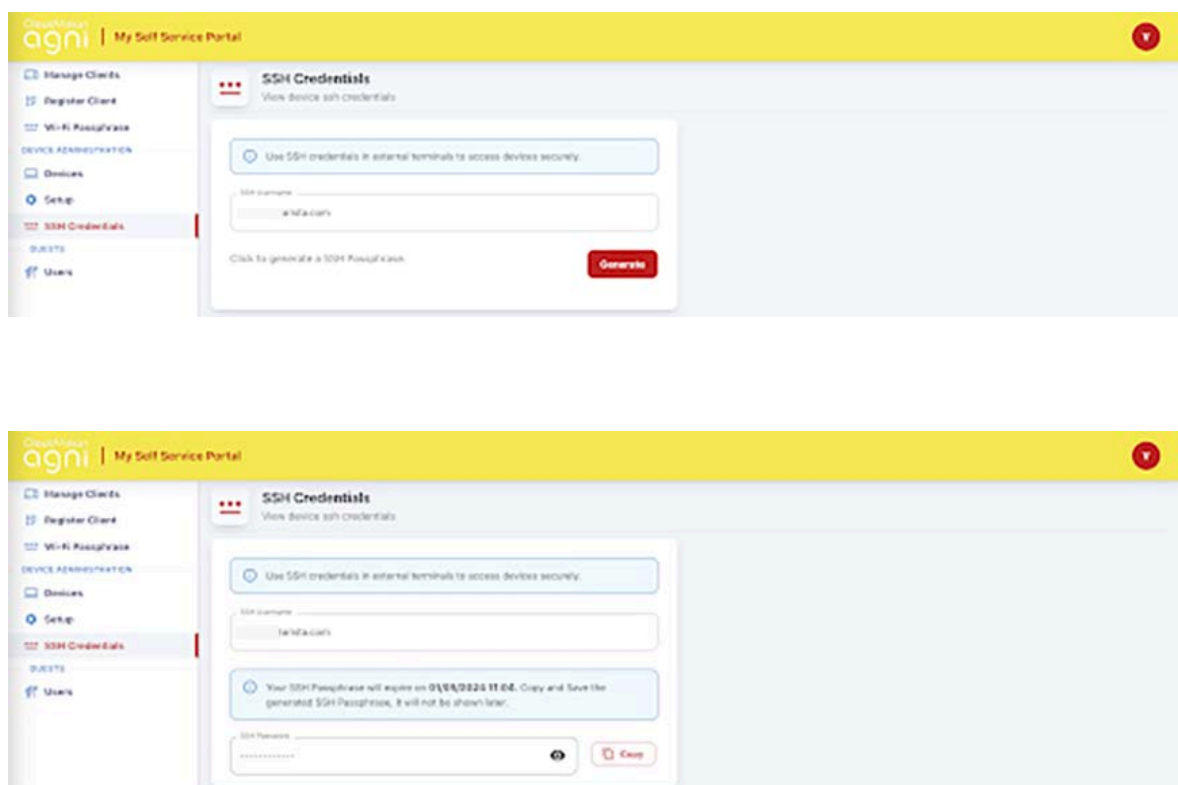


Figure: Device Login Credentials

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#
```

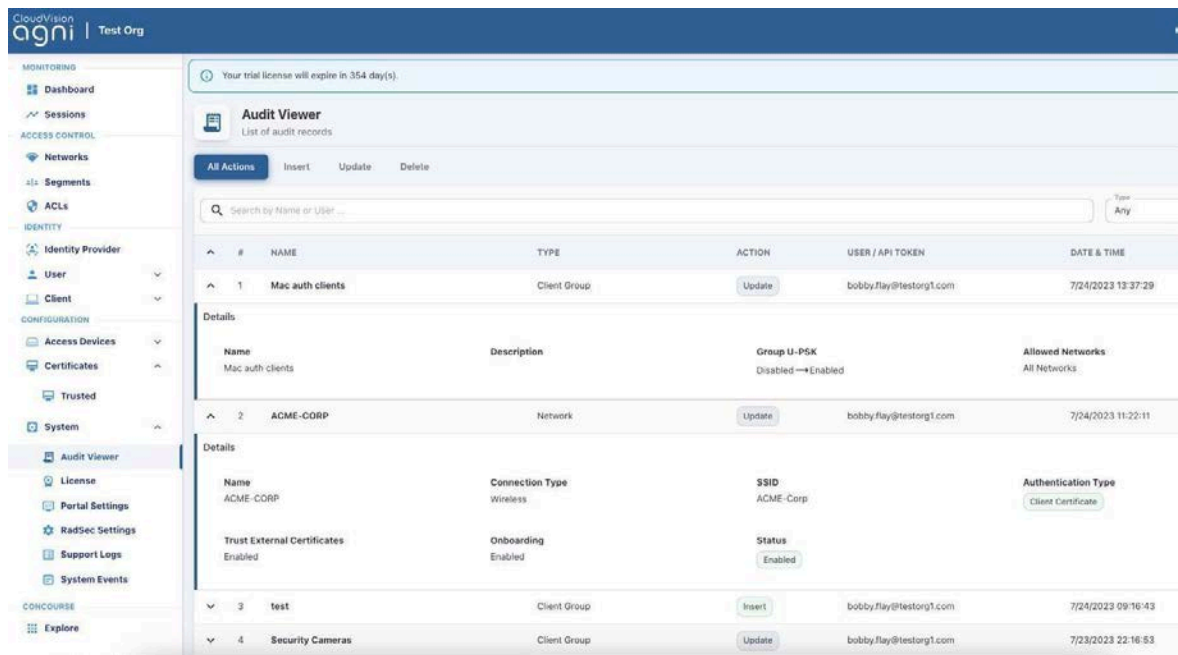
Figure: TACACS+ Authorization Allowed and Denied Output

System

This section captures the administrative tasks at the system level.

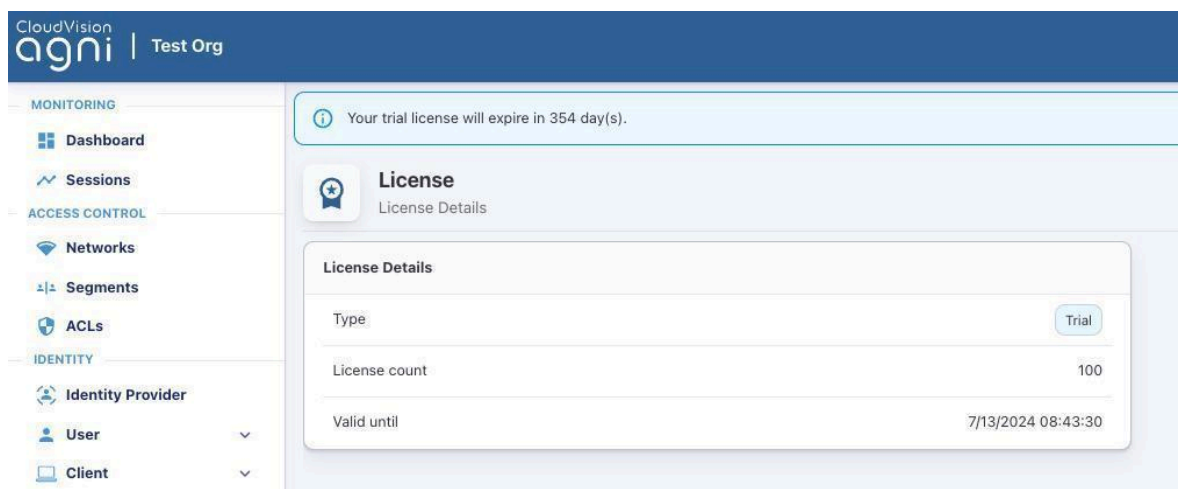
Audit Viewer

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



License

Displays the licensing information about the type, count, and validity period.



Self-Service Portal Settings

The Portal Settings can be used to customize the Self-Service Portal user experience. This allows the customization of logos, text, images, and themes on the captive portal page for the organization's needs. The customization can also be applied to landing and login pages.

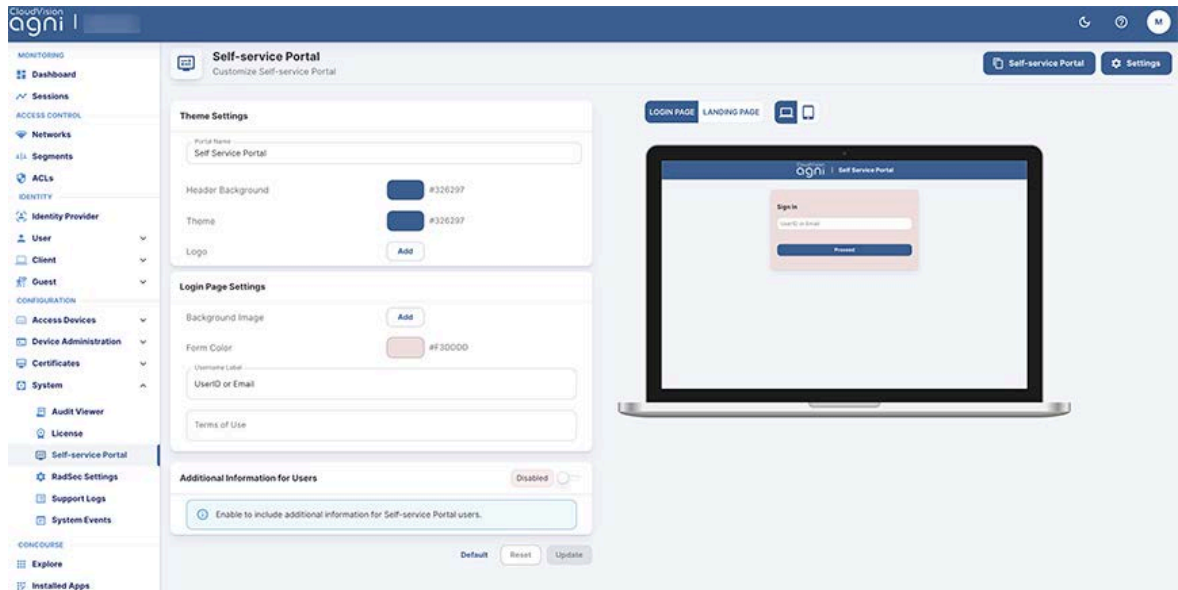


Figure: Self-Service Portal

From AGNI release version 2024.2.0 onwards, you can manage the access privileges of user groups by modifying the Self-Service Portal settings. To modify:

- Click the **Settings** button at the top right of the Self-Service Portal screen.
- In the Manage Self-service Portal Settings pop-up window, add the user groups that you want to provide with read-only access. By default, all user groups have read-write access to the portal.

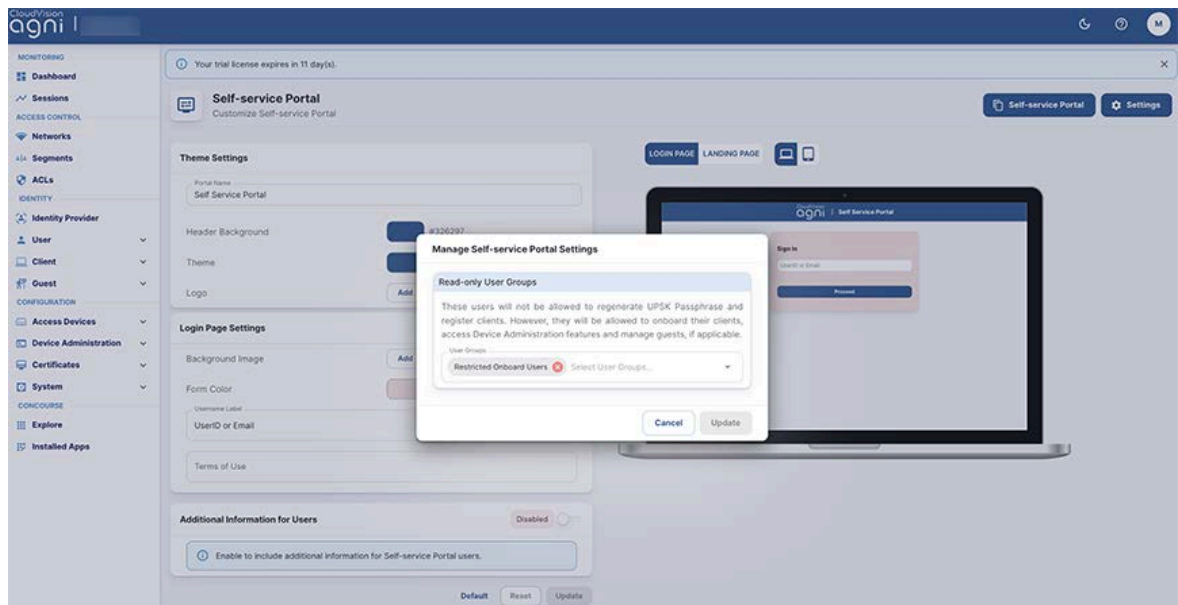


Figure: Self-Service Portal Settings Manage window

Note: User Groups with read-only permission cannot add, update, or delete clients using the AGNI portal or APIs (see image).



Figure: Self-Service Portal Clients with Read-only Access

Additionally, the users with read-only access cannot regenerate and update the passphrase (see image).

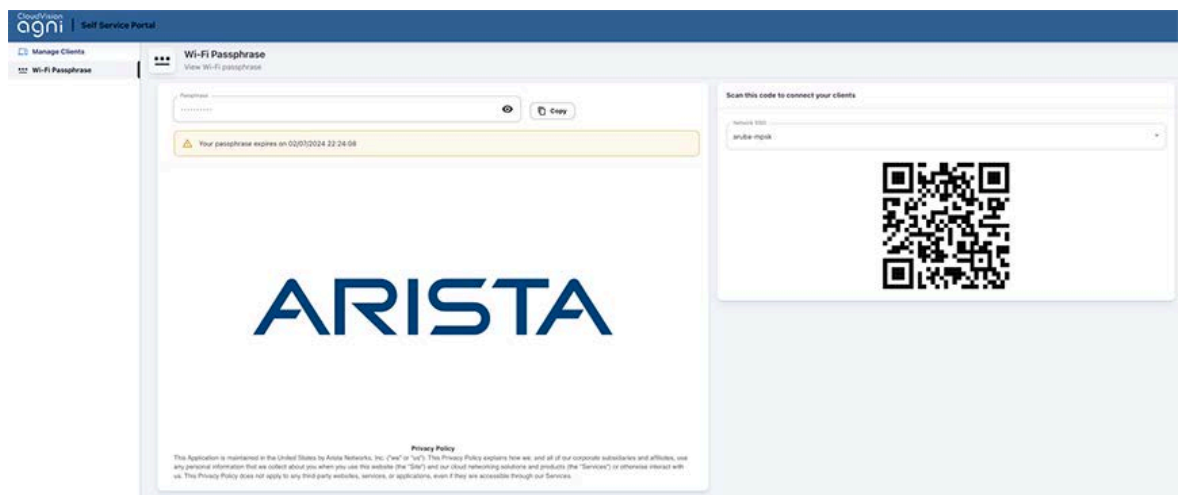


Figure: Self-Service Portal Wifi Passphrase (client with Read-only access)

Note: The users with read-only access privileges can contact the AGNI administrator if they want to regenerate their passphrase. The AGNI administrator can regenerate the passphrase from the User accounts page (see image).

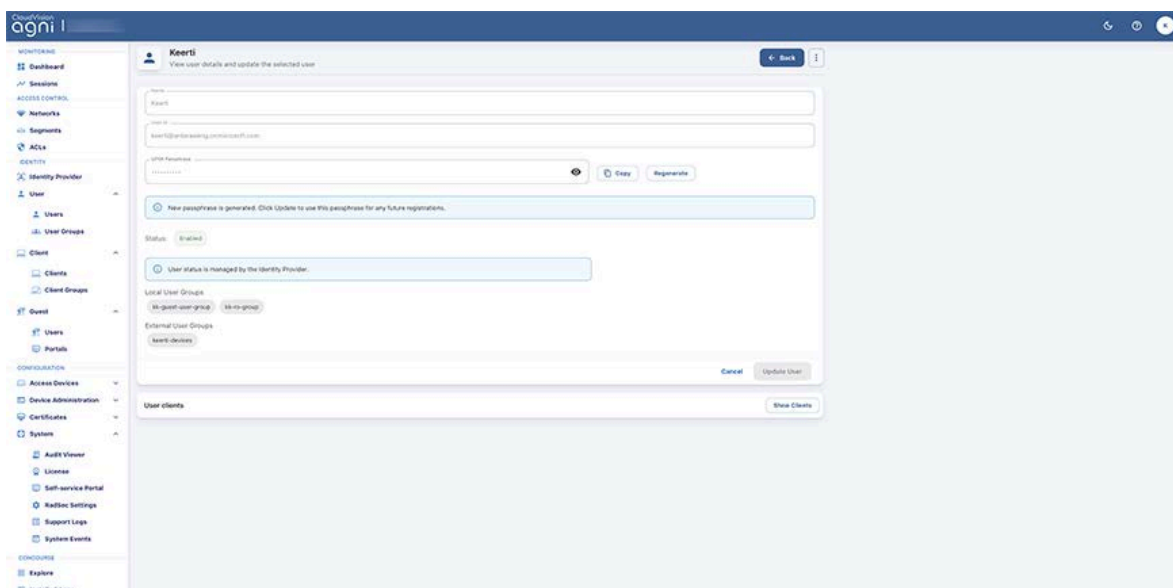


Figure: User Account Details with Regenerate Passphrase option

You can also add additional information for the users using the Self-Service portal. To add additional details, on the Self-Service Portal, enable the **Additional Information for Users** button and add the custom text (see image below).

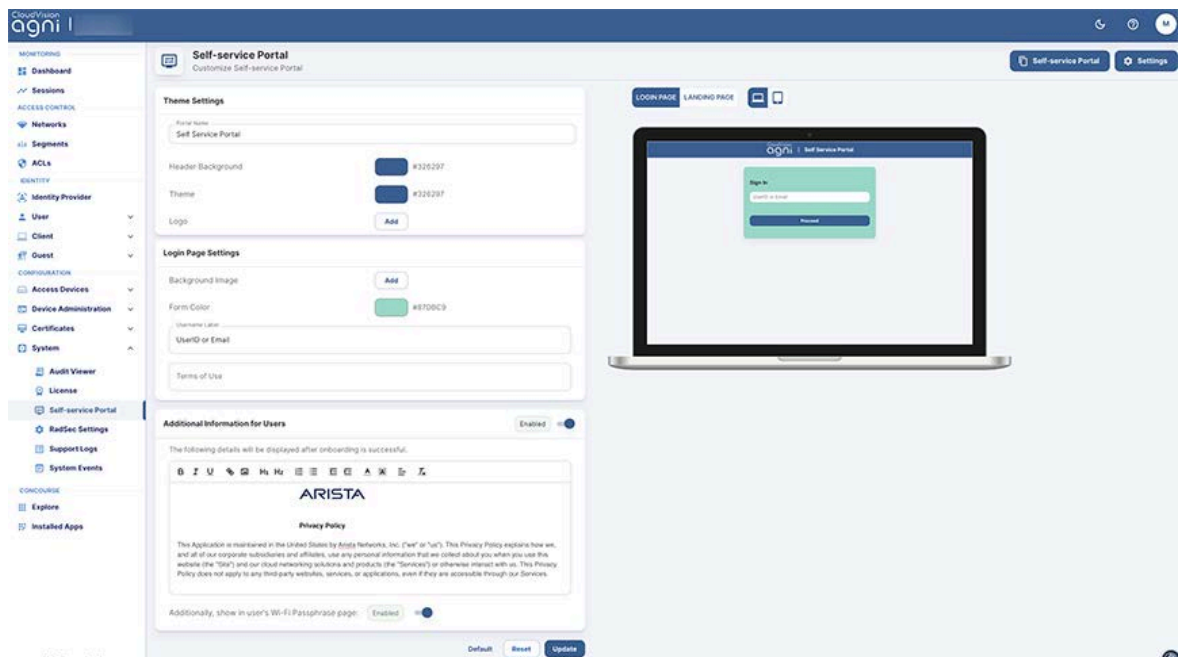


Figure: Self-Service Portal Settings – Additional Details

This added content is displayed on the final page when you register and onboard a new client (see images below). The custom text is displayed in the Wi-Fi Passphrase window of the Self-Service portal:

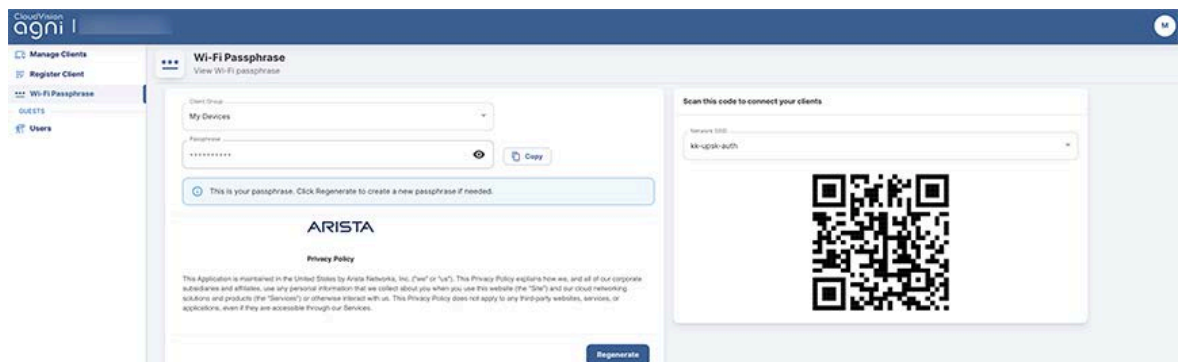


Figure: Self-Service Portal Wi-Fi-Passphrase

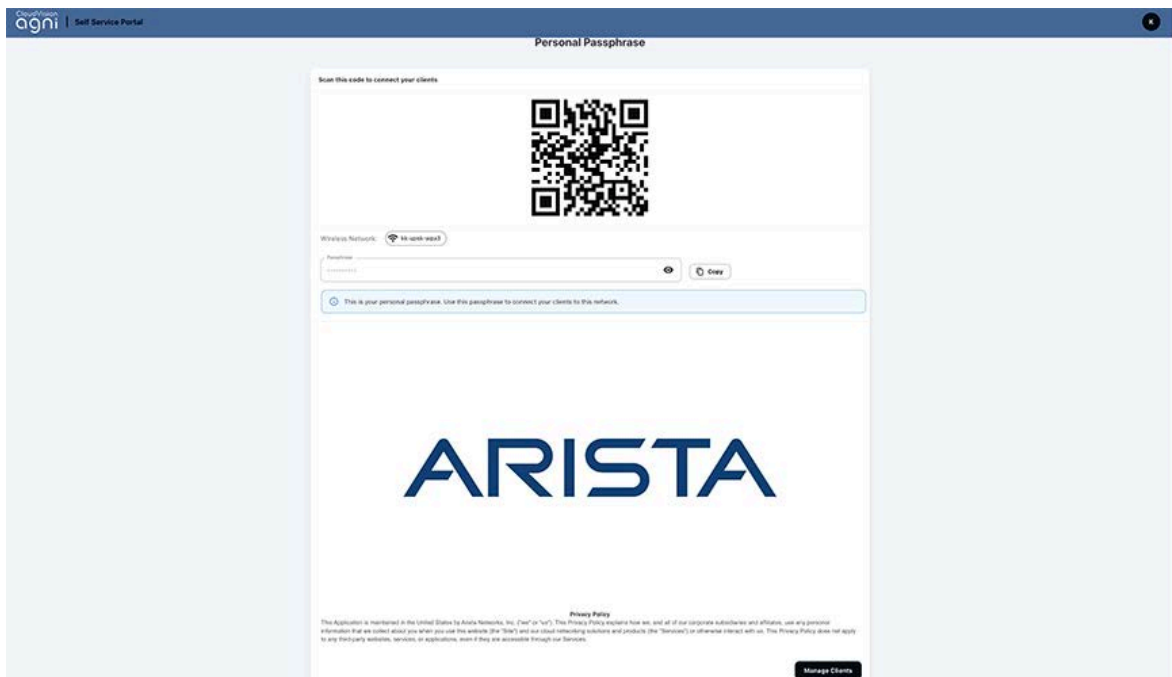


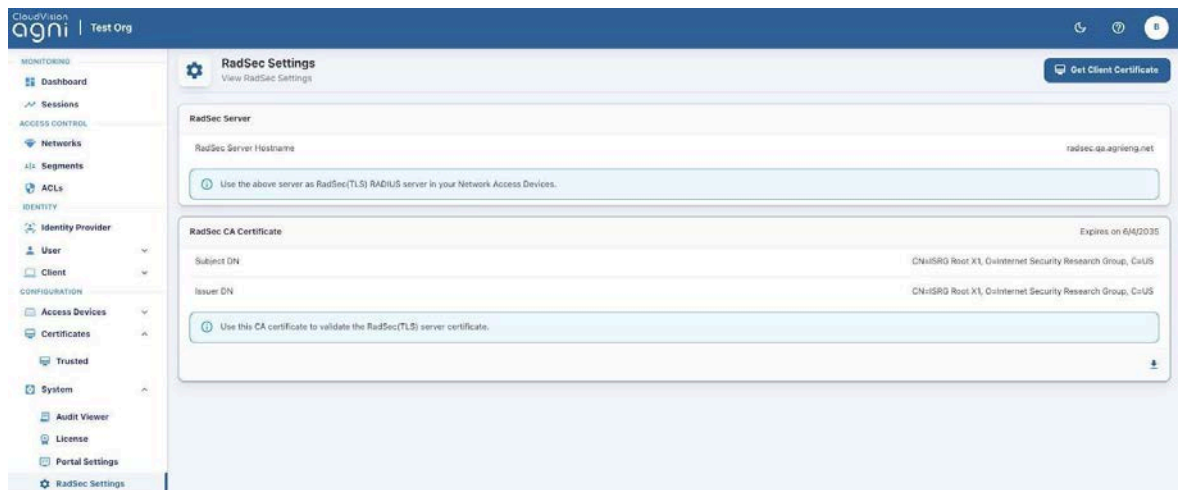
Figure: Self-Service Portal Wi-Fi/UPSK-Passphrase



Figure: Self-Service Portal Registering a Client in the Native Onboarding page

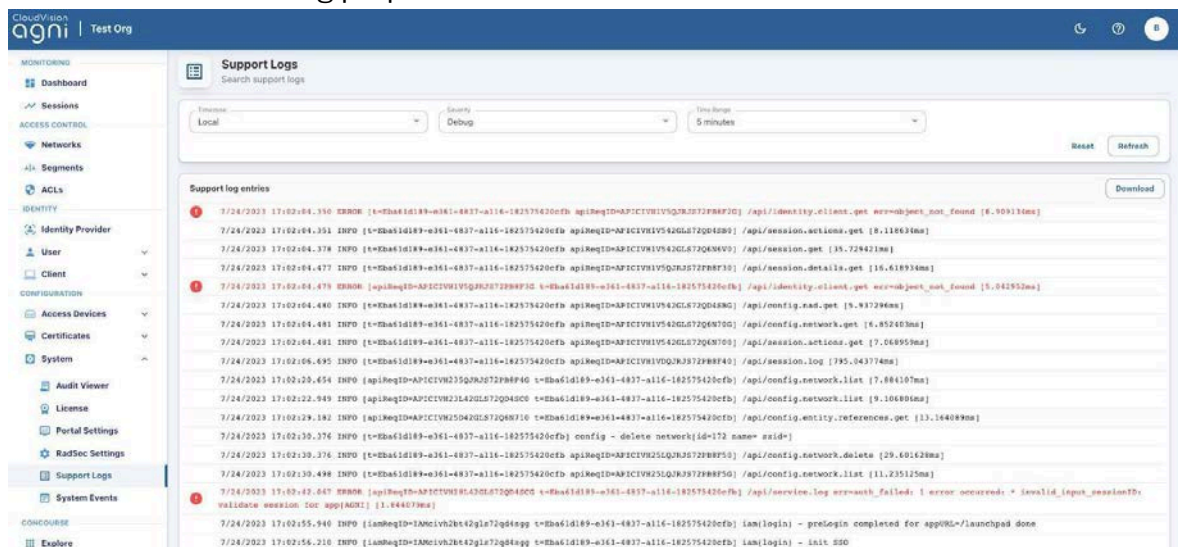
RadSec Settings

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.



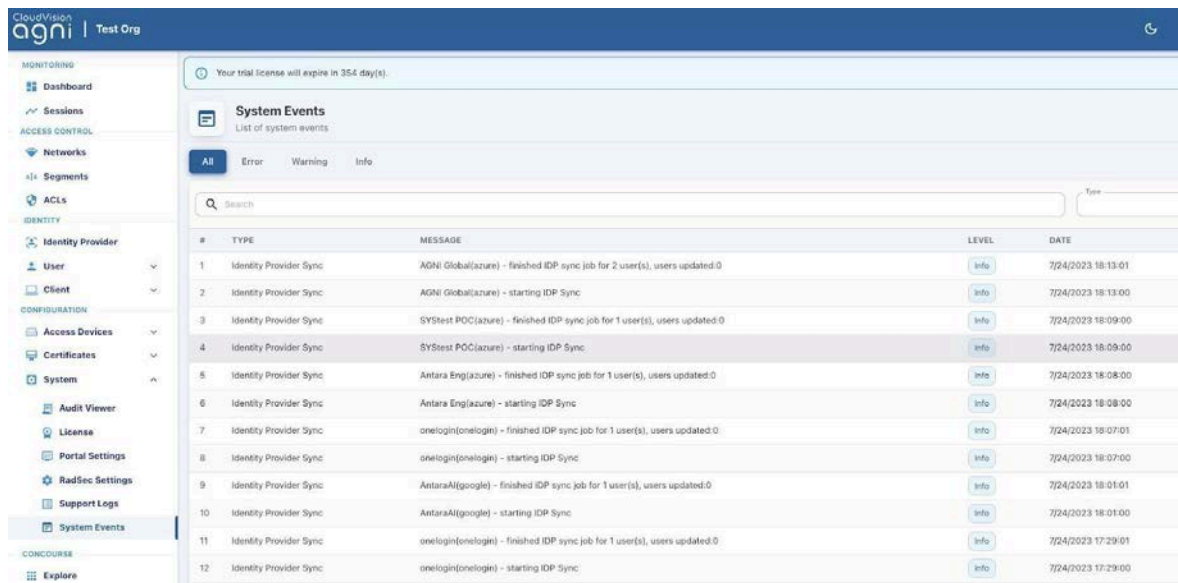
Support Logs

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.



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.



Notification Settings

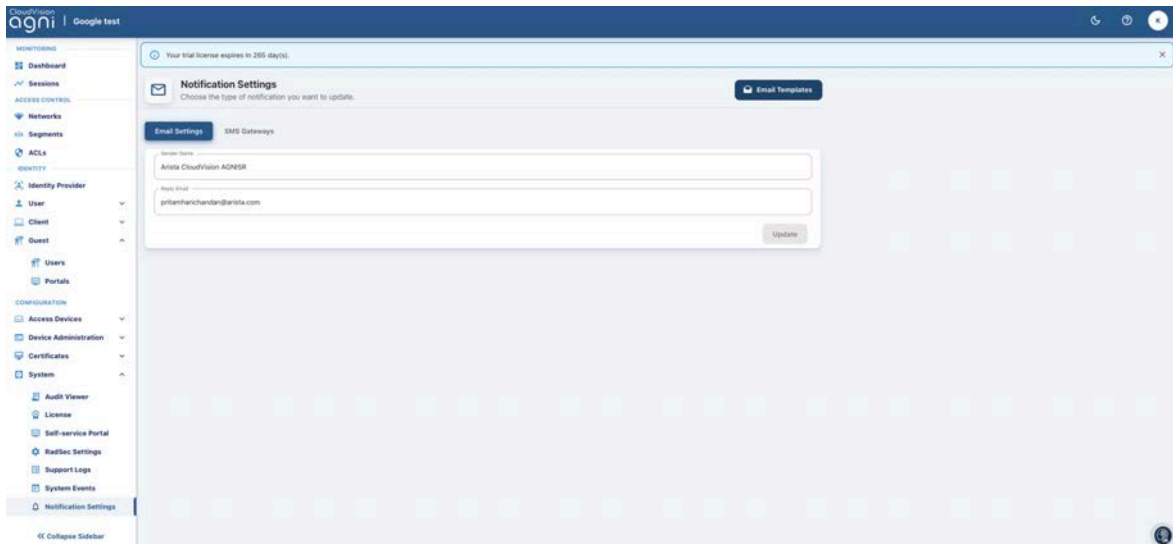
This section explains the configuration details for the Email settings and SMS gateway:

Configuring Email Settings

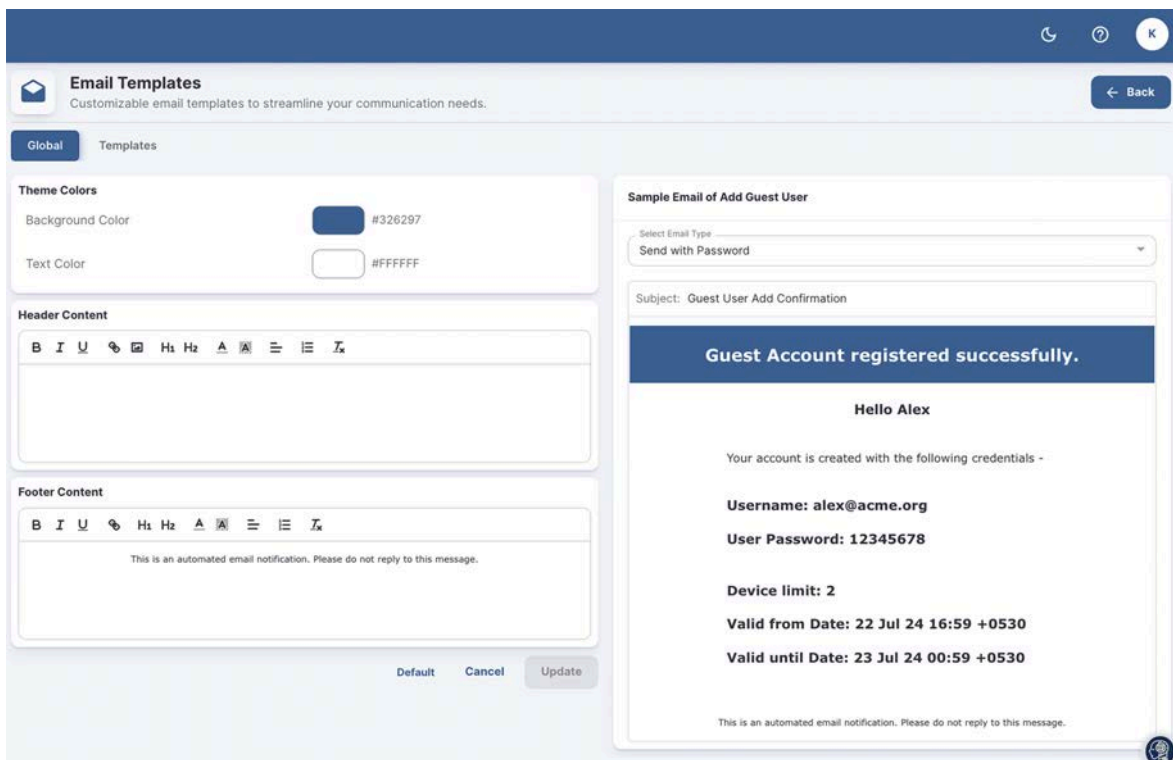
You can customize email templates from the AGNI portal for both guest users and organizational users, for adding, modifying, and disabling the users. You can select a desired workflow from the email template list and customize the email format to their needs. See the image for a sample email template.

To customize the email template, you must log in as an admin and follow the steps:

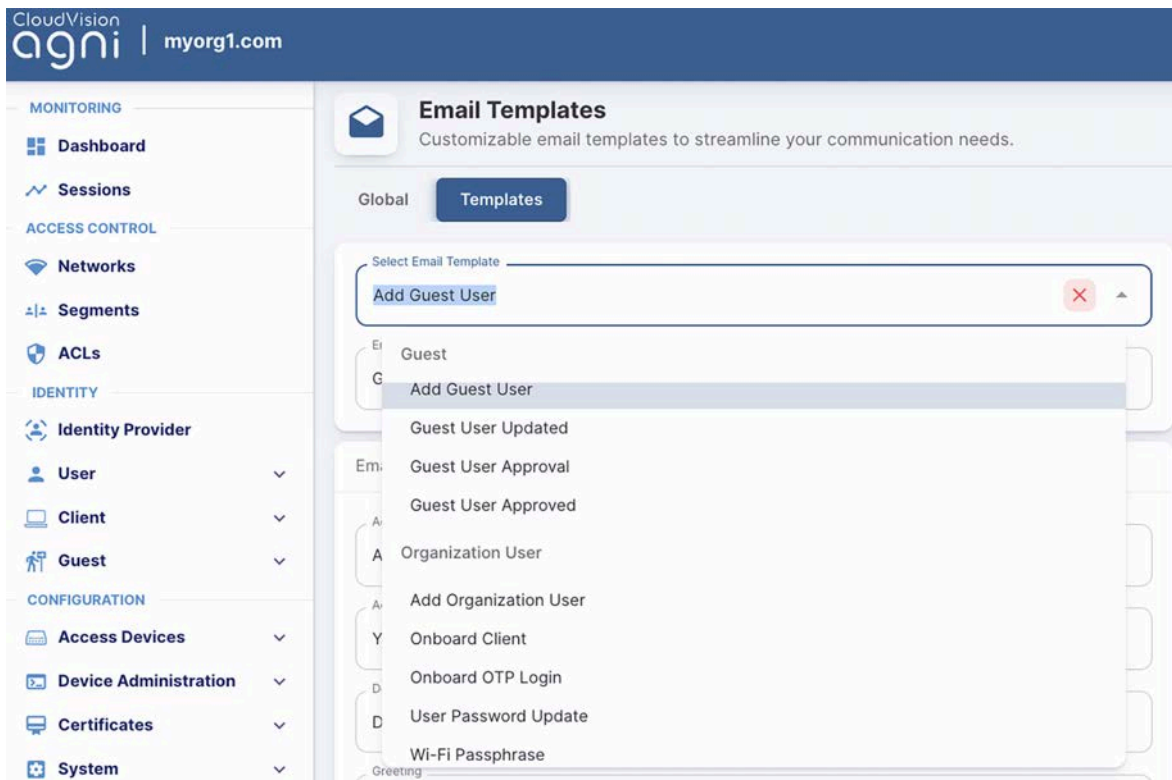
- Navigate to **Configuration**→**System**→**Notification Settings** →**Email Settings**.
- Customize the **Sender Name** and the **Reply Email** and click the **Email Templates** button (see image).



- In the Email templates page, update the **Header Content** and **Footer Content** and customize the Theme Colors text from the **Global** tab. See the preview of the email color and format on the right side (see image).



- Select the **Templates** tab in the Email Templates page (see image).
- Select the desired **Email Template** and customize the placeholder details (image3):
 - In the **Select Email Template** field, choose one of the options from the Organizational User or Guest from the drop-down list (see image).



- Enter the Email Subject
 - Customize the text in the Email Placeholders section.
 - On the right side, choose one of the options (*Send with Password* or *Send with Passphrase*) from the **Select Email Type** field.
 - Preview the Email template and email customizations displayed on the right side and modify, if required (image).
 - Click the **Update** button to save the configuration.
- Note:** You can also reset the email templates to default by selecting the **Default** button.

For more details, see the “*Customizing the Email Templates in AGNI*” article in Community Central.

Email Templates
Customizable email templates to streamline your communication needs.

Select Email Template: Add Guest User

Email Subject: Guest User Add Confirmation

Email Placeholders:

- Account created with Passphrase: A unique Wi-Fi passphrase has been created for you.
- Account created with Password: Your account is created with the following credentials -
- Device Limit: Device limit
- Greeting: Hello
- Header Text: Guest Account registered successfully.
- Passphrase instruction: Use the following passphrase to connect your client devices.
- Password: User Password
- QR code file: QR code file abc
- QR scan instruction: Scan the network QR code and connect to the wireless network.
- Username: Username
- Valid from: Valid from Date
- Valid until: Valid until Date
- Wi-Fi Network: WiFi Network xyz
- Wi-Fi Passphrase: Wi-Fi Passphrase

Default Cancel Update

Sample Email of Add Guest User

Select Email Type: Send with Password

Subject: Guest User Add Confirmation

Guest Account registered successfully.

Hello Alex

Your account is created with the following credentials -

Username: alex@acme.org
User Password: 12345678

Device limit: 2
Valid from Date: 22 Jul 24 16:59 +0530
Valid until Date: 23 Jul 24 00:59 +0530

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

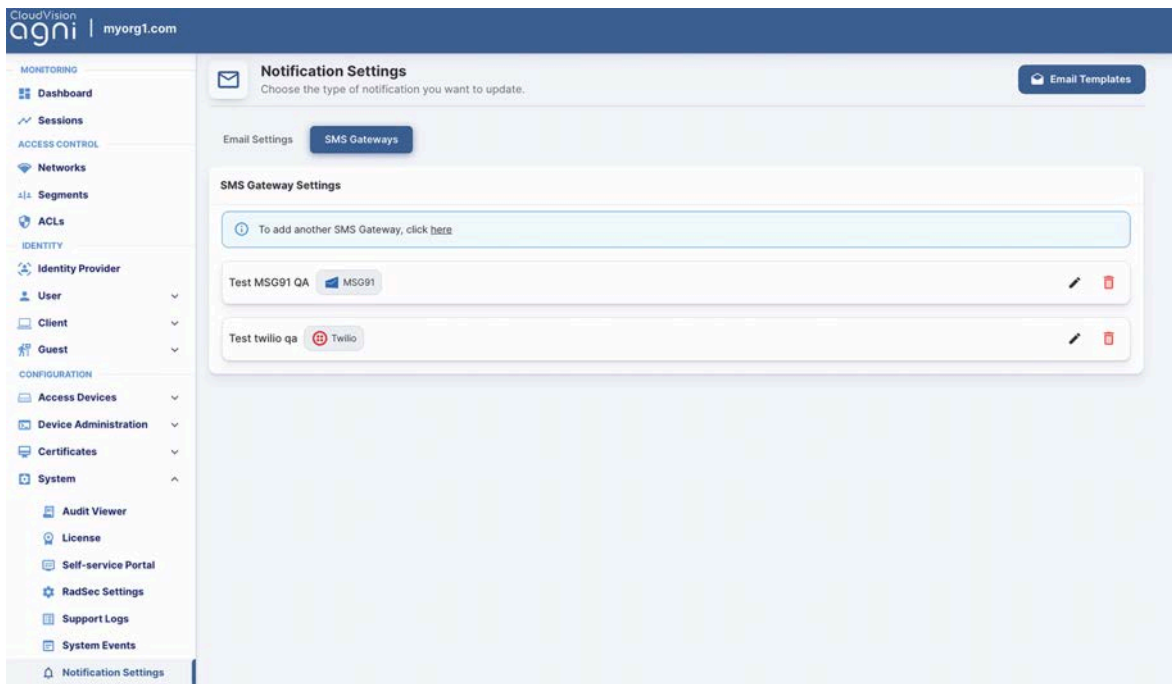
Configuring SMS Gateway

You can configure SMS gateway to enable registered guest users to receive SMS notifications when a guest account is added, modified, or disabled. AGNI supports two SMS Gateway configuration:

- Twilio (A US based cloud communications company that provides programmable communication tools for phone calls, and SMS messages).
- MSG91 (A communication platform, primarily for India audience, that provide businesses to integrate with SMS APIs).

To configure the SMS Gateway, you must log in as an admin and follow the steps:

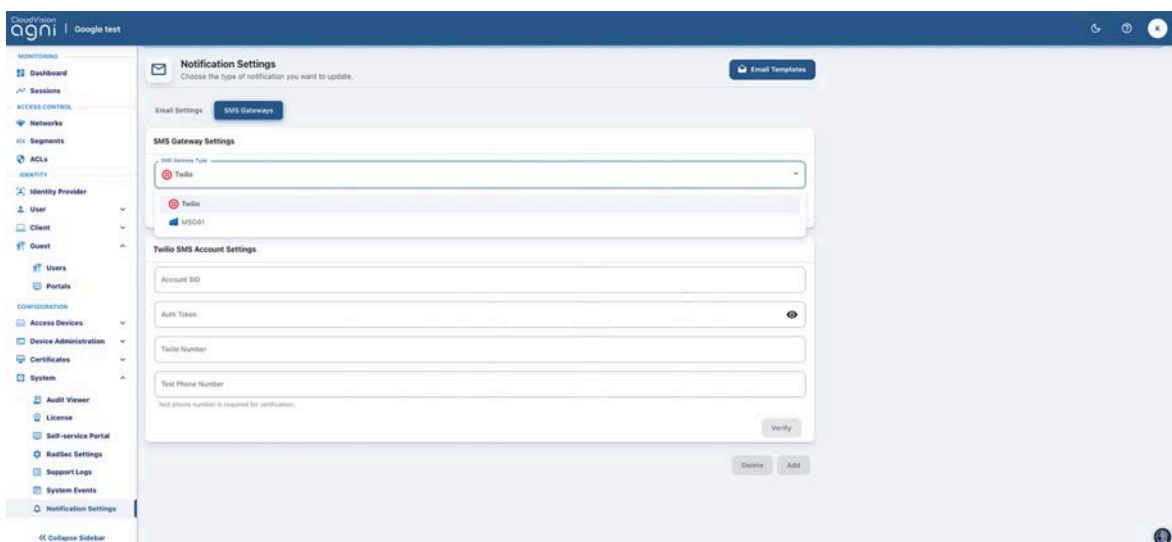
- Navigate to **Configuration**→**System**→**Notification Settings** →**SMS Gateways**.



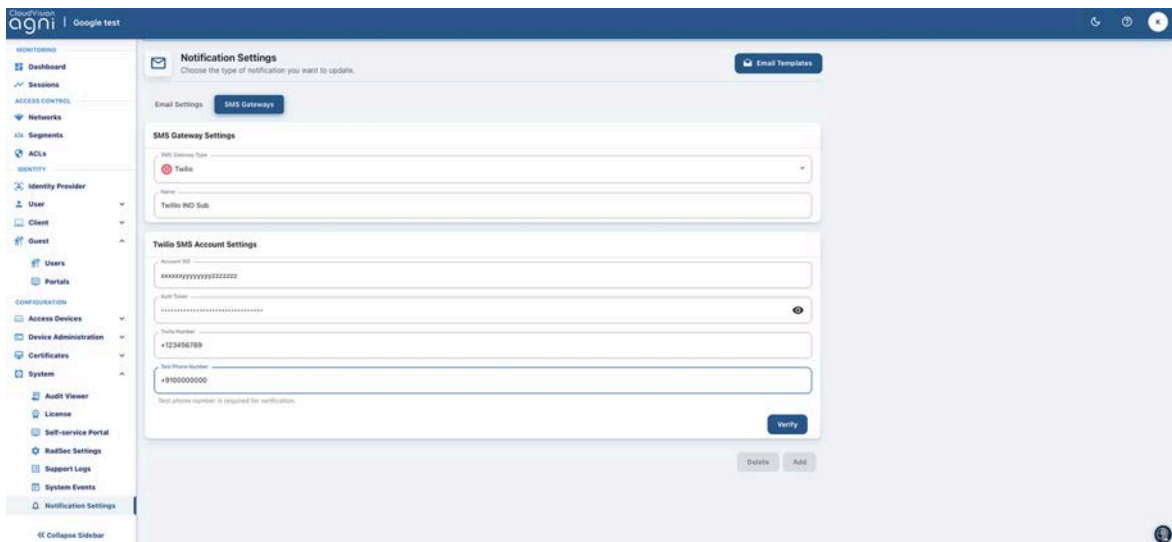
Configuring the Twilio SMS Gateway

To configure Twilio SMS gateway:

- From the Notification Settings > SMS Gateways page, select *Twilio* as the **SMS Gateway Type**.
- Enter a name for the gateway.



- In the Twilio SMS Account Settings section, enter the details:
 - Account SID
 - Auth Token
 - Twilio Number
 - Test Phone Number

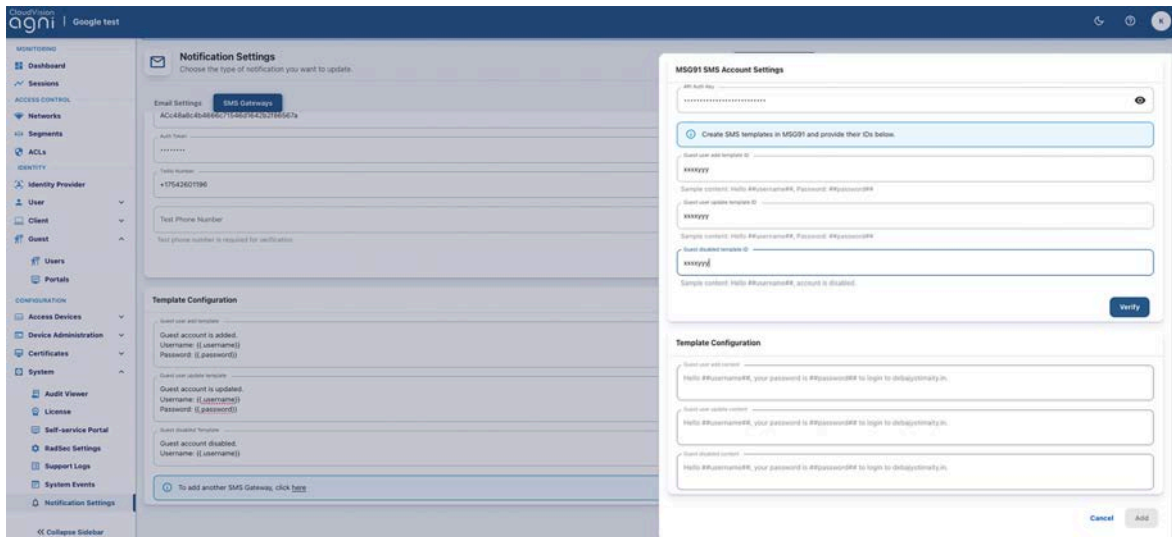


- Click the **Verify** button to verify the configuration and phone number.
- In Template Configuration section, update the details for:
 - Guest user add template
 - Guest user update template
 - Guest disabled template
- Click the **Add** button to update the details.
- Click the **Delete** button if you want to delete a user account from the SMS gateway.

Configuring the MSG91 SMS Gateway

To configure MSG91 SMS gateway:

- From the Notification Settings > SMS Gateways page, select MSG91 as the **SMS Gateway Type**.
- Enter a name for the gateway.
- In the **MSG91SMS Account Settings** section, configure:
 - API Auth Key
 - Guest user add template ID
 - Guest user update template ID
 - Guest disabled template ID
- Click the **Verify** button to verify the configuration.
- In the Template Configuration section, add the details:
 - Guest user add content
 - Guest user update content
 - Guest disabled content
- Click the **Add** button to add the the details.



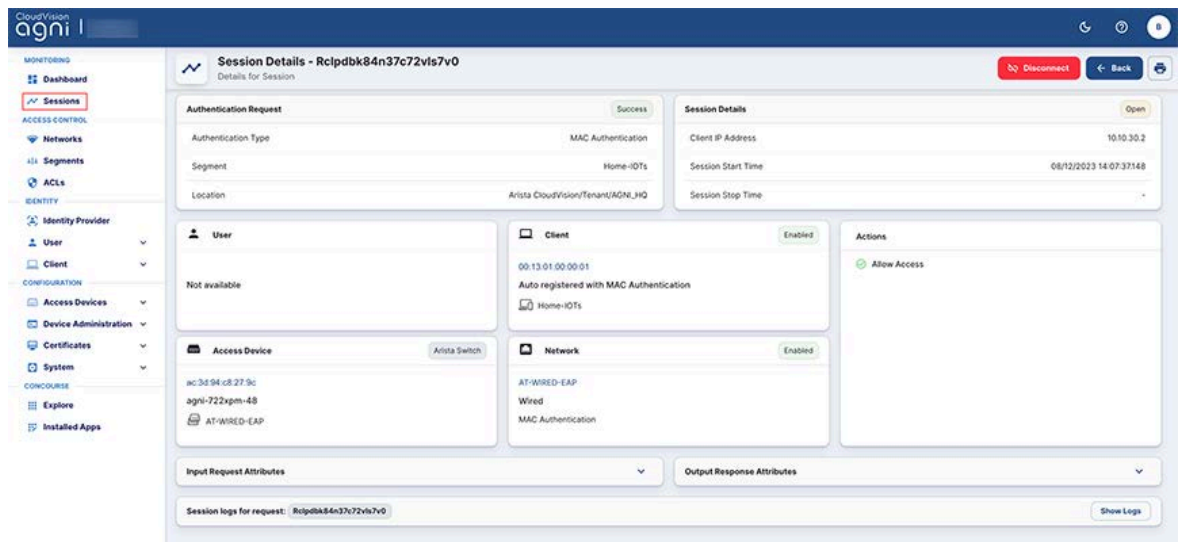
- To delete an account, select the account and click the **Delete** button.

For more details, see the “*Configuring SMS Gateway in AGNI*” article in Community Central.

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).

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success	08/12/2023 14:07:37:148
2	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success	08/12/2023 13:54:16:193
3	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success	08/12/2023 13:48:42:317
4	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success	08/12/2023 13:07:37:065
5	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success	08/12/2023 12:54:16:075
6	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success	08/12/2023 12:48:42:236
7	CAMERA_GROUP	MAC Authentication	f8-e4:3b:c0:0c:1d	192.168.1.12	Success	08/12/2023 12:32:24:121
8	CAMERA_GROUP	MAC Authentication	f8-e4:3b:c0:0c:1d	192.168.1.12	Success	08/12/2023 12:31:47:824
9	Home-IOTs	MAC Authentication	00:13:01:00:00:01	10.10.30.2	Success	08/12/2023 12:07:36:985
10	Home-IOTs	MAC Authentication	00:13:01:00:00:02	10.10.30.3	Success	08/12/2023 11:54:15:993
11	Polycom Phones	MAC Authentication	f8-e4:3b:c0:0c:1d	192.168.1.12	Success	08/12/2023 11:50:47:419
12	Home-IOTs	MAC Authentication	00:11:d9:5e:3d:44	10.201.110.50	Success	08/12/2023 11:48:42:102



On-Demand Disconnecting a Client from the Network

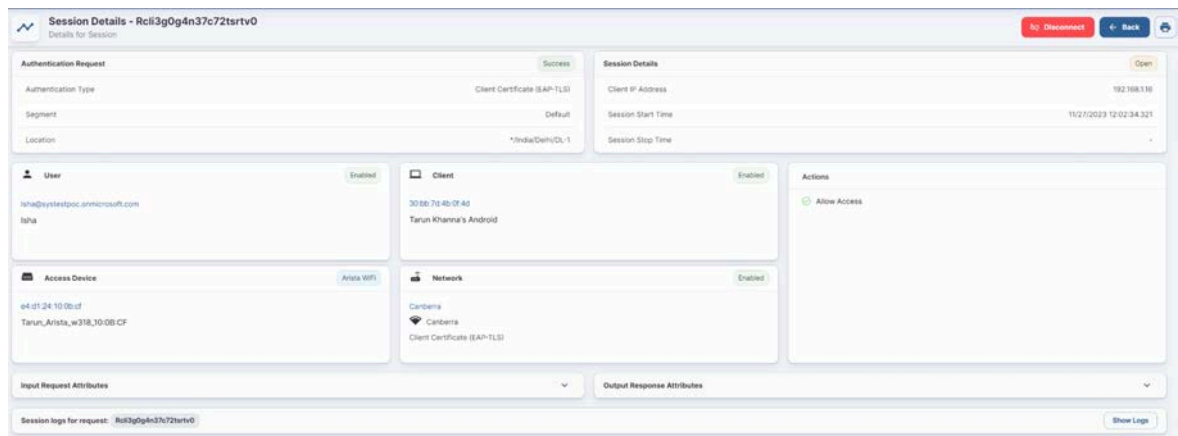
This section describes the steps to manually disconnect a client from the network. You must log in as an admin user to perform the steps.

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

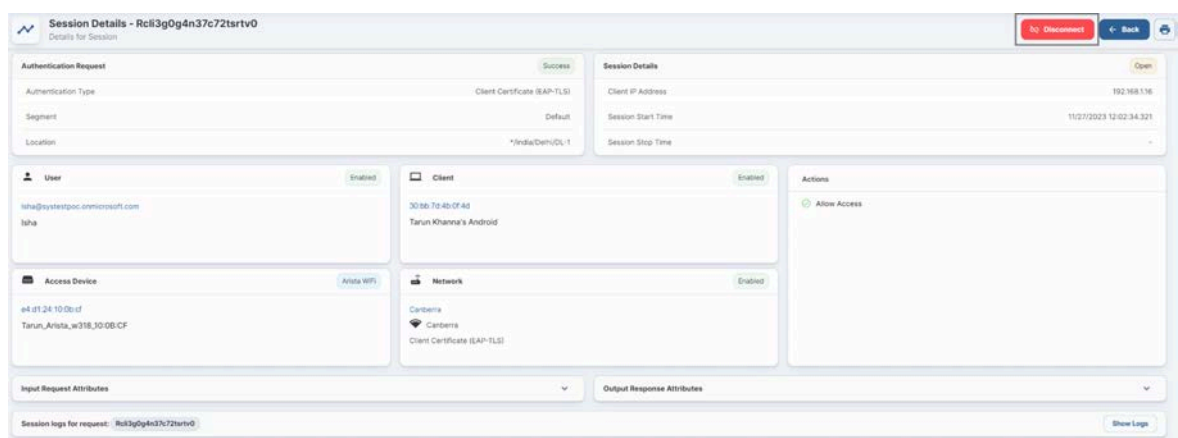
- Open the client's active session (see image below).

ID	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
1	isha@systemtestpoc.onmicrosoft.com	Client Certificate	30:66:7d: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	192.168.1.16	Success	11/24/2023 12:06:26.075
3	POTO	MAC Authentication	28:f1:0e:08:3b:0a	192.168.1.16	Success	11/24/2023 12:04:14.928
4	POTO	MAC Authentication	28:f1:0e:08:3b:0a	192.168.1.16	Failed	11/24/2023 12:02:27.567
5	isha@systemtestpoc.onmicrosoft.com	Client Certificate	30:66:7d:4b:0f:4d	192.168.1.16	Success	11/23/2023 22:29:39.358
6	isha@systemtestpoc.onmicrosoft.com	Client Certificate	30:66:7d:4b:0f:4d	192.168.1.16	Success	11/23/2023 22:20:12.585

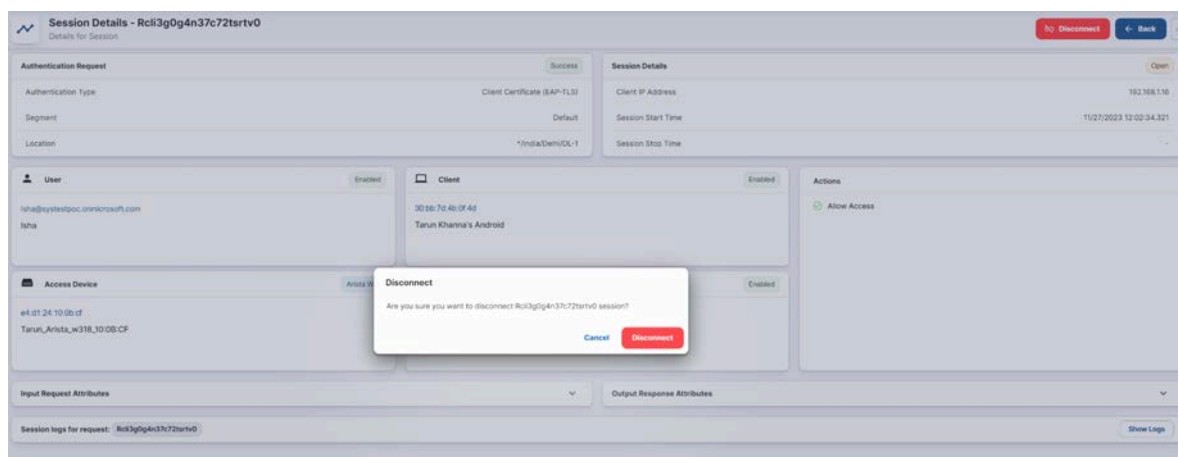
- Click the “eye” icon to open the active session details (see image below).



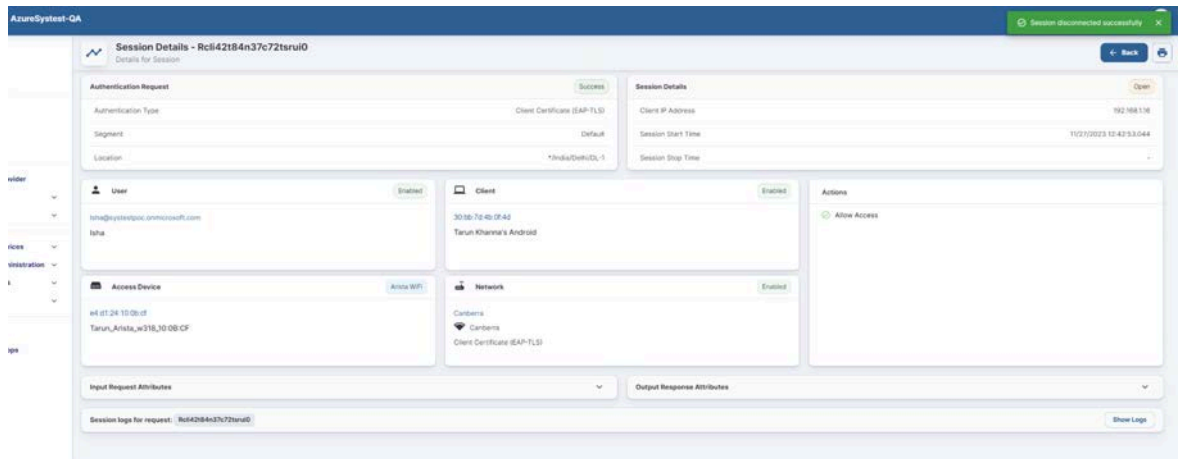
- Click the Disconnect button.



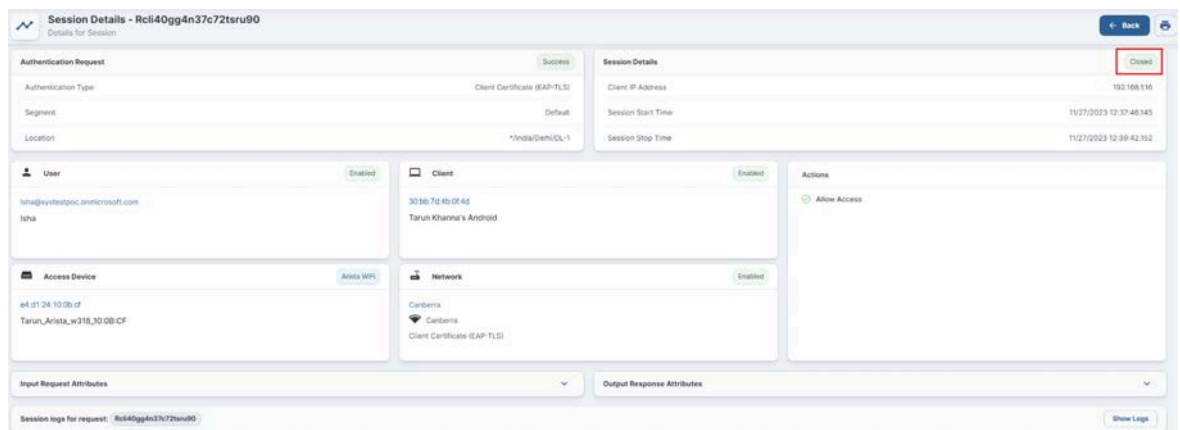
AGNI dashboard displays a confirmation message for admin approval (see image below).



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



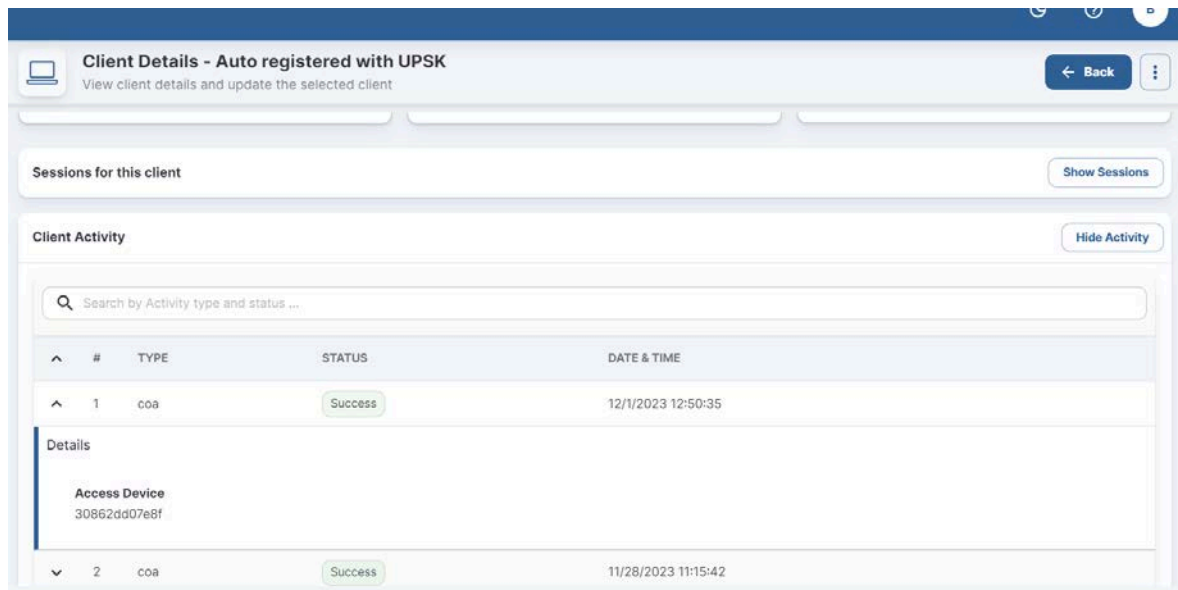
Now the client session status changes from **Open** to **Closed**.



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



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



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**

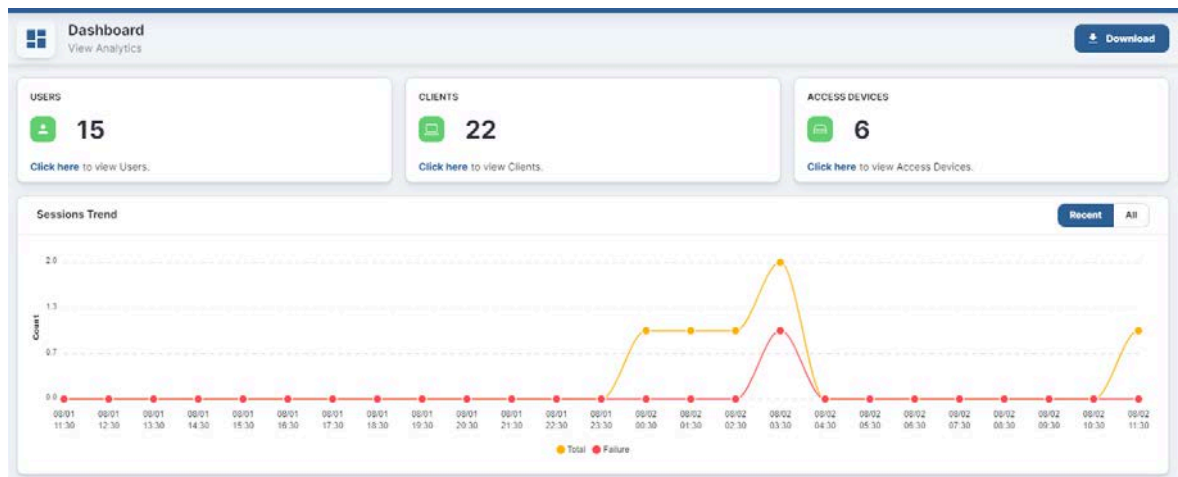


Figure: AGNI Dashboard and Session Trend

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.

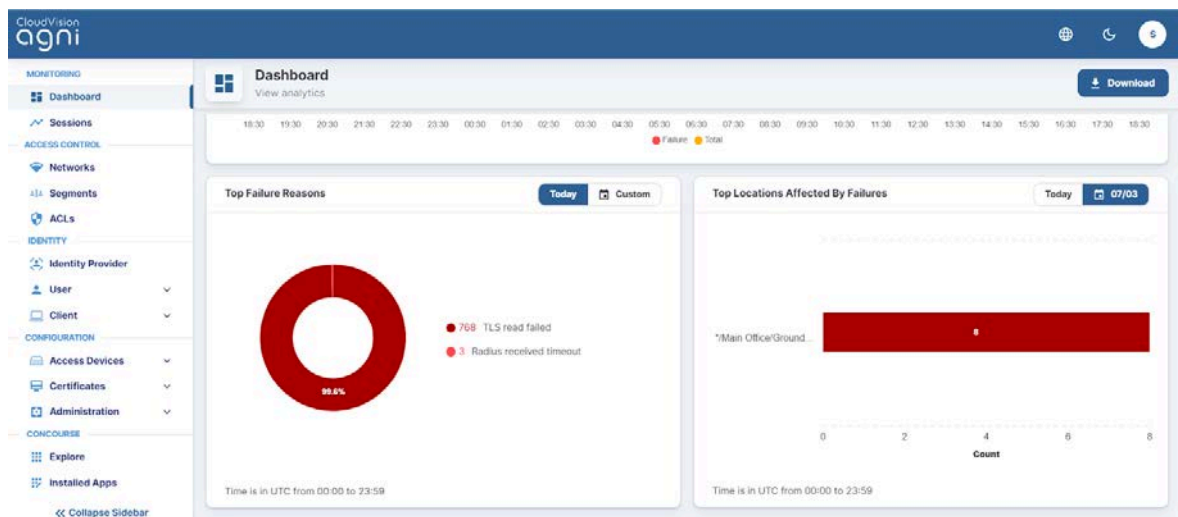


Figure: AGNI Dashboard and charts

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**.

CloudVision agni | Test Org

MONITORING Dashboard Sessions

ACCESS CONTROL Networks Segments ACLs

IDENTITY Identity Provider User Client

CONFIGURATION Access Devices Certificates System

CONCOURSE Explore Installed Apps

Sessions
List of Sessions as on 7/24/2023 21:43:38

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

Auth Type: Any Status: Success

#	IDENTITY	TYPE	MAC ADDRESS	IP ADDRESS	STATUS	TIMESTAMP
128	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:89:bc	192.168.1.102	Success	7/20/2023 18:59:16.781
129	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:89:bc	192.168.1.102	Success	7/20/2023 18:59:08.167
130	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:89:bc	192.168.1.102	Success	7/20/2023 18:58:47.539
131	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:89:bc	192.168.1.102	Success	7/20/2023 18:58:33.477
132	alice@agrilglobal.anmicrosoft.com	Client Certificate	0a:89:f8:e0:29:07		Success	7/20/2023 18:47:15.895
133	rachael.ray@testorg1.com	Captive Portal	ba:ba:d2:15:89:bc	192.168.1.102	Success	7/20/2023 17:58:17.188
134	soham@xyz.com	Unique PSK (UPSK)	98:60:ca:34:7c:ad	192.168.1.138	Success	7/20/2023 17:54:19.136
135	soham@xyz.com	Unique PSK (UPSK)	98:60:ca:34:7c:ad	192.168.1.138	Success	7/20/2023 17:51:18.891
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@antaraii.net	Captive Portal	c4:75:ab:f5:e1:00	192.168.1.105	Success	7/20/2023 17:41:20.771

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

CloudVision agni

MONITORING Dashboard Sessions

ACCESS CONTROL Networks Segments ACLs

IDENTITY Identity Provider User Client

CONFIGURATION Access Devices Certificates System

CONCOURSE Explore Installed Apps

Session Details - Rc1ls9e5j0h1s72sc27mg
Details for Session

Authentication Request: Success

Authentication Type: Client Certificate (EAP-TLS)

Segment: Default

Location:

Session Details: Closed

Client IP Address: 10.86.60.226

Session Start Time: 7/10/2023 14:13:36.306

Session Stop Time: 7/10/2023 14:13:46.924

User: Enabled

steve.kratt
Steve Kratt

Client: Enabled

70:1a:b1:82:10:31
Steve Kratt's Windows

Access Device: Arista WiFi

30:05:28:00:07:af
Pune-C235AP

Network: Enabled

PUNE-WPA2
PUNE-WPA2
Client Certificate (EAP-TLS)

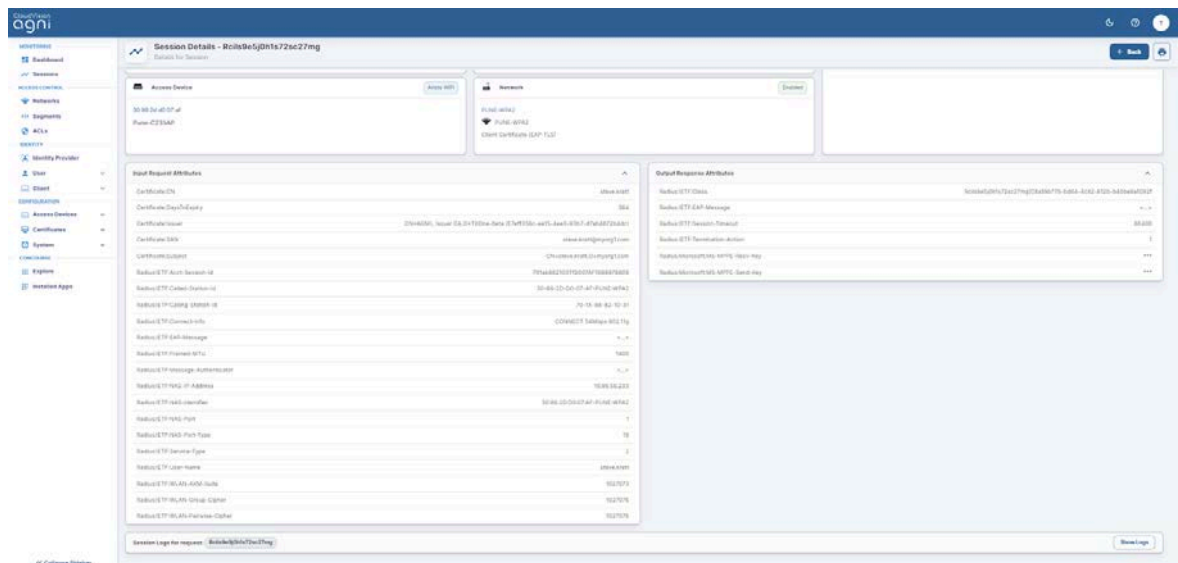
Actions: Allow Access

Input Request Attributes

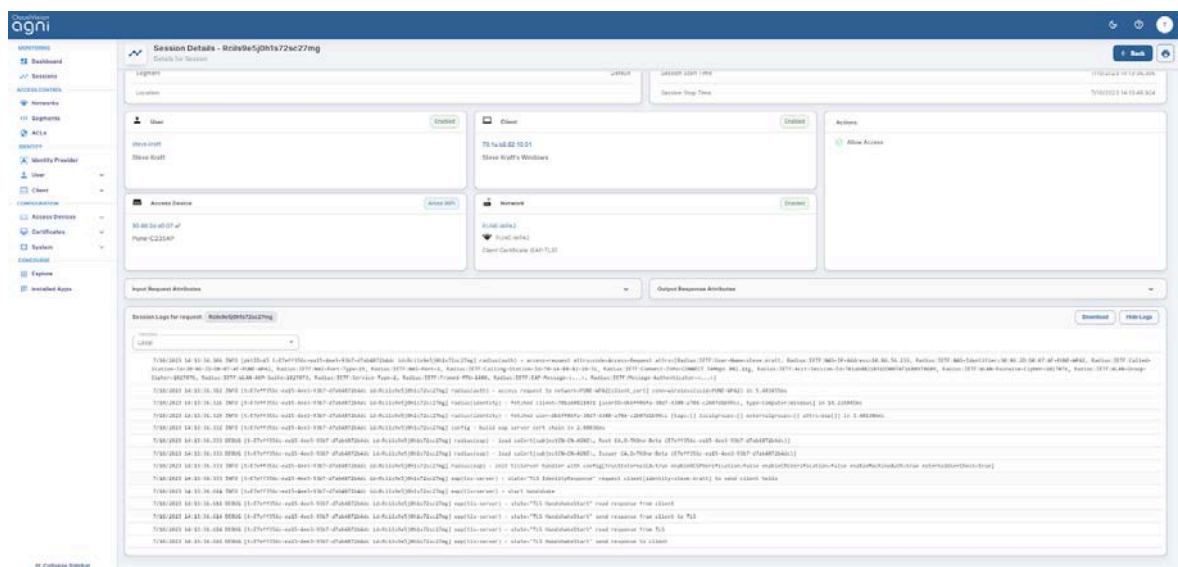
Output Response Attributes

Collapse Sidebar

Figure: Session Details page-1



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.

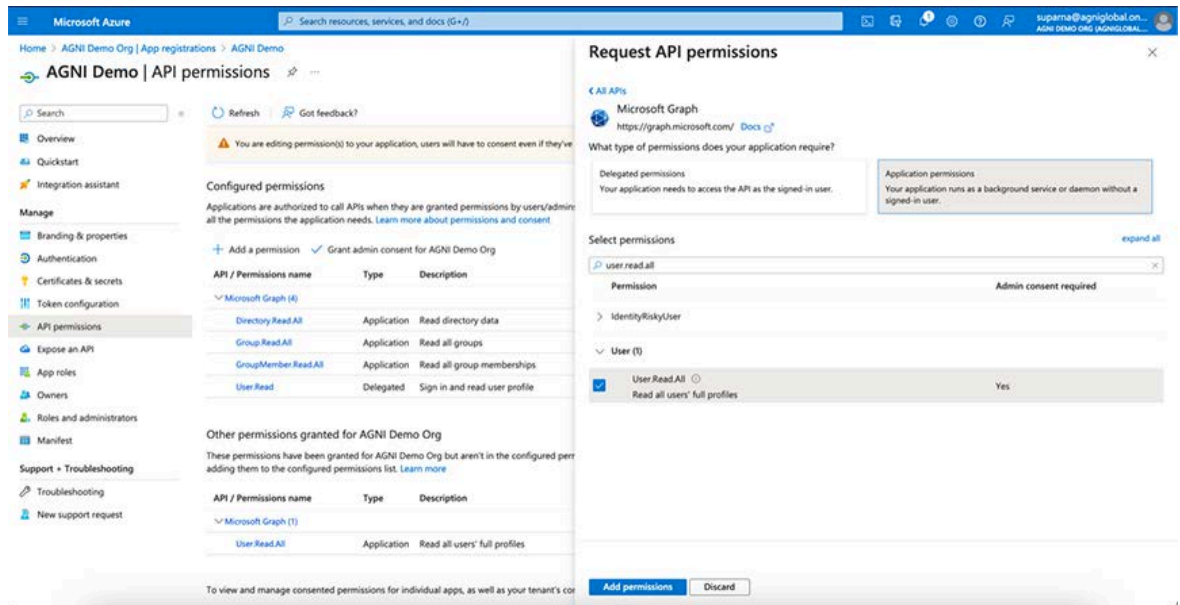


Figure: API Permissions

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

URLs and Open Ports in Firewall

While onboarding an Android device with restrictive access to the Internet, in a Captive Portal flow, add the URL's listed in the table to walled garden list (is a list of websites or domains that users can visit without authentication) on the access point along with other IDP based URLs:

For onboarding of an Android device, see the [EAP-TLS based Enterprise SSID using CV-CUE and AGNI: Configuration and Onboarding](#) article.

URLs	Open Ports
cvagni.page.link	TCP/443
android.clients.google.com	TCP/443, UDP/5228-5230
googleapis.com	TCP/443
firebase.dynamiclinks.googleapis.com	TCP/443
play.google.com	TCP/443
gvt1.com	TCP/443, UDP/5228-5230
ggpht.com	TCP/443, UDP/5228-5230