User Guide

AGNI (On Premises) Arista Guardian for Network Identity

Version P-2024.4.0

Arista.com

Arista Networks

DOC-07691-01

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

Contents

Chapter 1

AGNI On-Prem Overview

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.

Arista has been at the forefront of the cloud networking revolution, leveraging a software-driven approach based on Cloud Native principles, open standards based designs, and native programmability to deliver consistent, reliable software solutions. Arista Guardian for Network Identity (CloudVision AGNI) has adopted a similar architectural approach to other products to deliver a state of-the-art solution for managing network identity. CloudVision AGNI embraces modern design principles, Cloud Native micro-services architecture, and Machine Learning/Artificial Intelligence (ML/AI) technologies to significantly simplify administrative tasks and reduce complexities. It offers a comprehensive range of features to meet the requirements of modern networks, including support for scaling, operational simplicity, stability, and zero-trust security. CloudVision AGNI enables a substantial reduction in total cost of ownership, making it a very cost-effective choice for businesses of all sizes. With its cutting edge features and advanced technology, CloudVision AGNI is the ideal choice for businesses looking to enhance their network security infrastructure.

The key features of CloudVision AGNI includes:

- Centralized configuration and segment policy management.
- Simple, Secure, and scalable next-generation Network Identity solution.
- Cloud Native architecture.
- Ask Autonomous Virtual Assistant (AVA).
- Micro-segmentation with Arista MSS and UPSK.
- Profiling and Posturing.
- Continuous posture check with Arista NDR solution.
- Multi-Vendor Support.
- Publisher/Subscriber APIs for 3rd party integration.

1.1 Prerequisites

Before reviewing the AGNI User Guide, familiarize yourself with the following documents:

- Release Notes for AGNI ON Premises available on Arista website:
- DCA-AGNI-100 Appliance Quick Start Guide available on Arista website: https://www.arista.com/en/support/product-documentation/hardware.
- Setup and Access Guide for DCA-AGNI-100 appliance available on Arista website: https://www.arista.com/en/support/product-documentation.

- Design and Scalability Guide available on Arista Products page: https://www.arista.com/en/products/network-access-control/literature.
- Log in as an administrator to access and configure the AGNI portal.

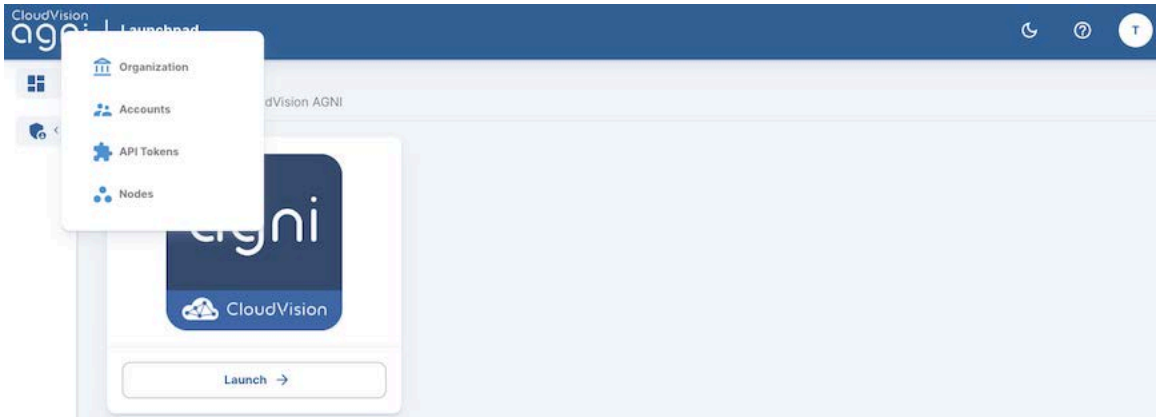
1.2 Accessing Launchpad App

Once the Arista DCA-AGNI-100 appliance is setup, login to the appliance using the customer provisioning account credentials to view the CloudVision AGNI Launchpad application (see image). From the Launchpad, you can access the configuration menus in AGNI and manage the different nodes in the cluster. For details on nodes, see Viewing Nodes in Cluster section.

Figure 1-1: AGNI On Prem Launchpad

The administrative tasks are available from the **Admin** console menu (see image). You can configure the organization details, account details, API tokens, and view the available nodes from the launchpad.

Figure 1-2: On Prem Launchpad with Admin Tasks

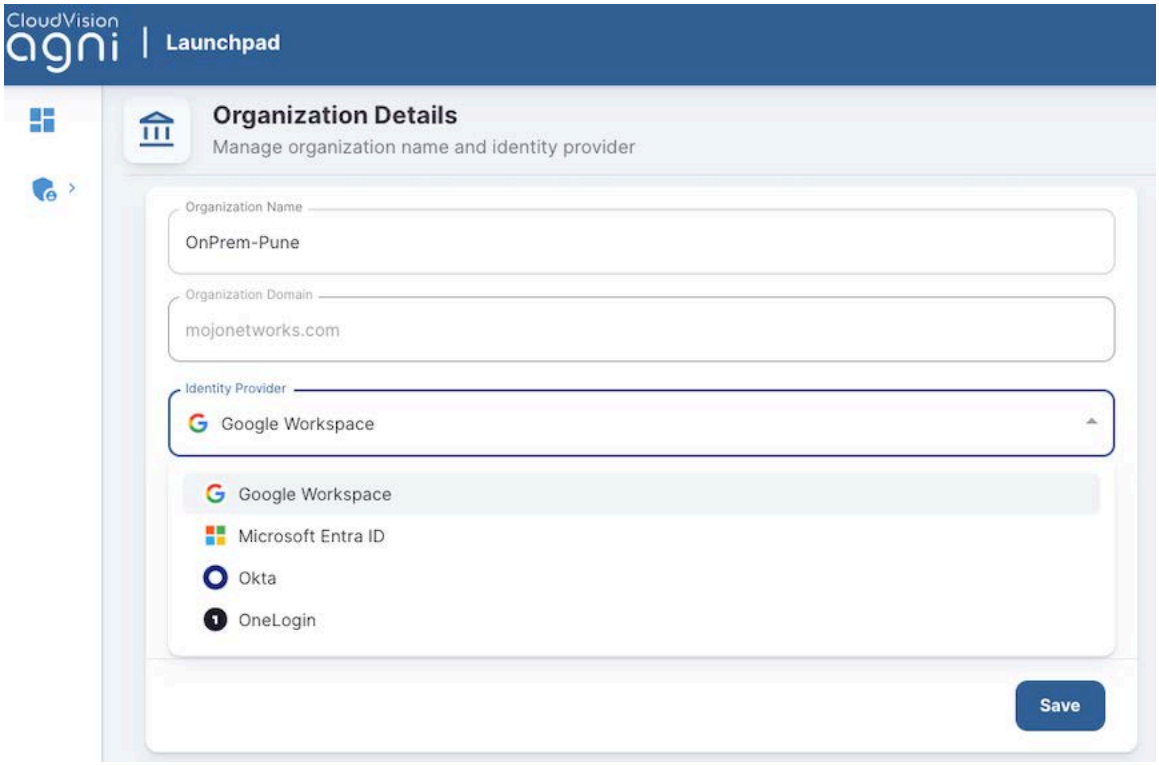


1.2.1 Adding Organizational Details

To make your AGNI access secure, use the single sign-on (SSO) based accounts by adding additional organizational accounts with different privileges. To add a new organization account, click on the **Organization** menu on the left pane.

- Enter your Organization Name. The domain name is displayed based on the registration information.
- Select the Identity Provider for your organization to enable a federated login criteria. You can integrate AGNI with any of the identity providers such as Google Workspace, Microsoft Entra, Okta, or OnLogin IDPs.

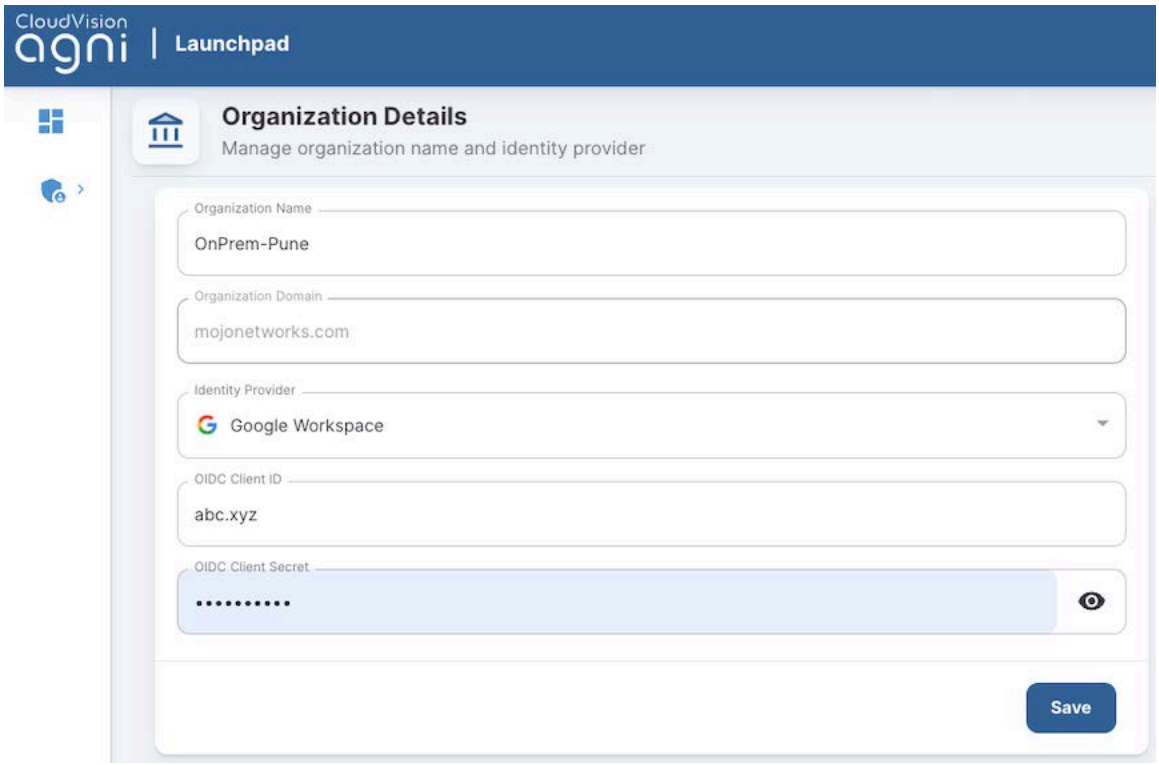
Figure 1-3: Organization Details with Identity providers



- Enter the respective client details and secret key provided from the respective identity providers.

> **Note:** For details on Client ID and Client Secret, see the respective IDP configuration details in the Configuring Identity Providers section.

Figure 1-4: Organizational details on AGNI Launchpad



1.2.2 Adding Account Details

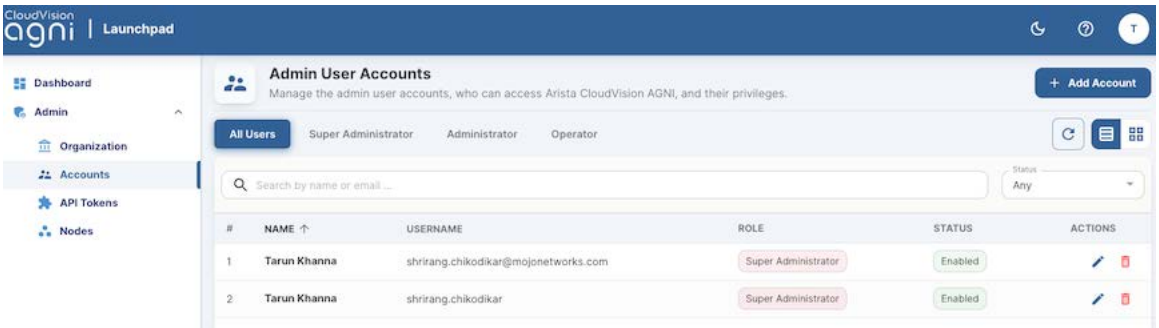
If you do not have an IDP, you can create local login accounts with super administrator, administrator, or operator privileges. The Super Administrator account has all the read-write permissions and can access and create other accounts.

> **Note:** As part of the initial AGNI Appliance (DCA-AGNI-100) bring-up and setup, the following default accounts are created in the **Admin** > **Accounts** section.
>
> - **Organization Account** - An Organizational User account is created with the customer's registered email. This would be the same account used during the initial AGNI Appliance bring-up and registration.
> - **Local Account** - A Local User account is also created with the same name used in Organization User Account Name. This would be the primary account for users when they login to the AGNI GUI for the first time.

For any additional user account creations, follow the steps in this section. To create a local account, perform the following steps:

1. Navigate to **Admin** > **Accounts**.
2. Click on the **+Add Account** button on the top right side of the page.

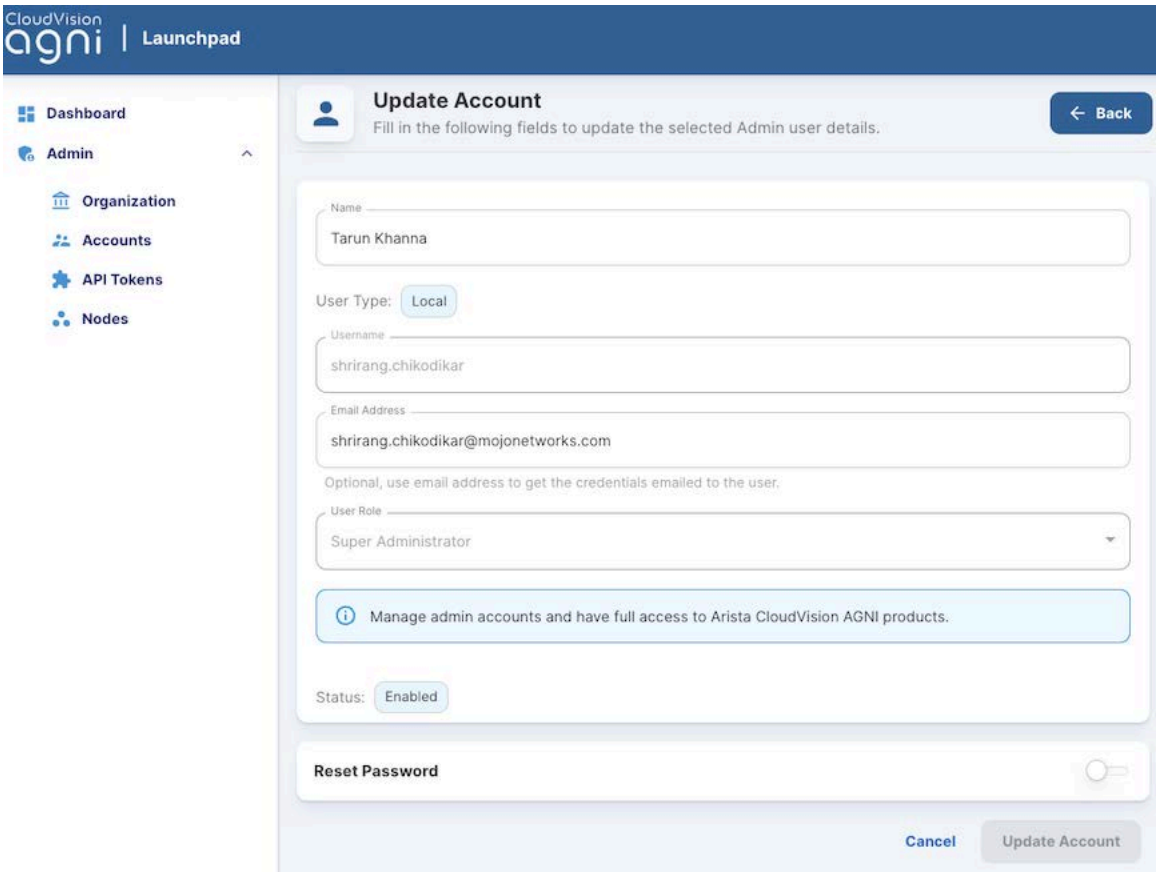
   Figure 1-5: Admin User Accounts



3. Enter the following details:
   a. **Name** of the user.
   b. **Username**
   c. **Email Address**
   d. Choose the **User Role** from the drop-down menu
   e. Enter a **Password**
   f. Toggle to **Enabled** if you want the user to change the password at next login.
4. Click the **Add Account** button.

   Once the account is created, you can modify the User Role and update the user account.

Figure 1-6: Update Accounts

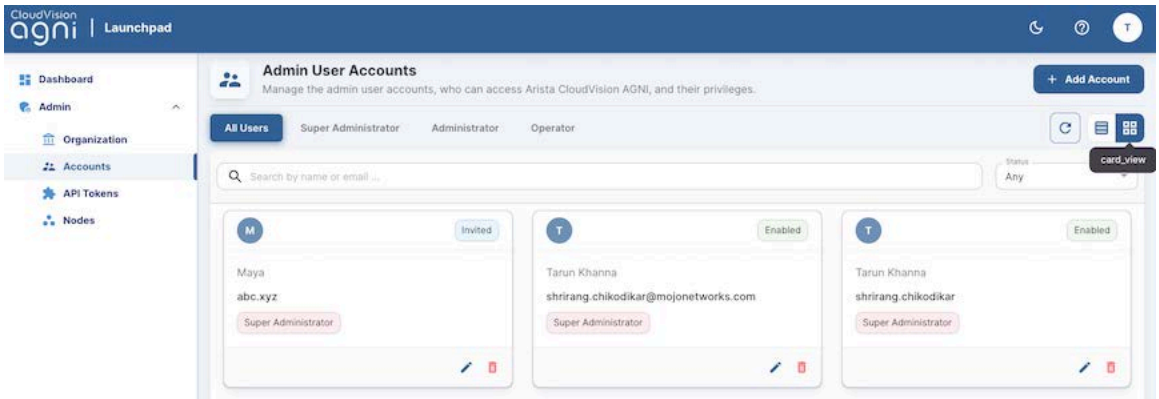


A local account with the specified privileges is created.

You can filter the account details by selecting the respective tabs: **All Users**, **Super Administrator**, **Administrator**, and **Operator**.

You can view the account details in table view mode or card view mode by selecting the respective modes (see image)

Figure 1-7: Card View of User Accounts

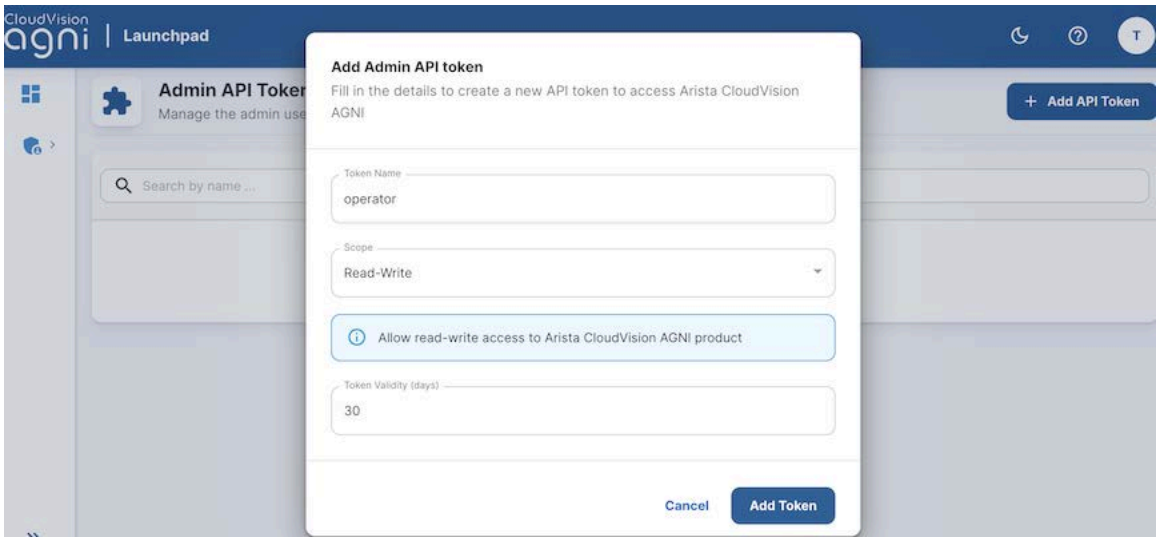


1.2.3 Adding API Tokens

If you want to have API based integration of any functionality with AGNI, you can create scripts that will periodically query the AGNI APIs and download the data for verification by creating API tokens, which authorizes the user to use the API query. To create an API token:

Click the **API Tokens** from the **Admin** console menu.

Figure 1-8: Add Admin API Tokens

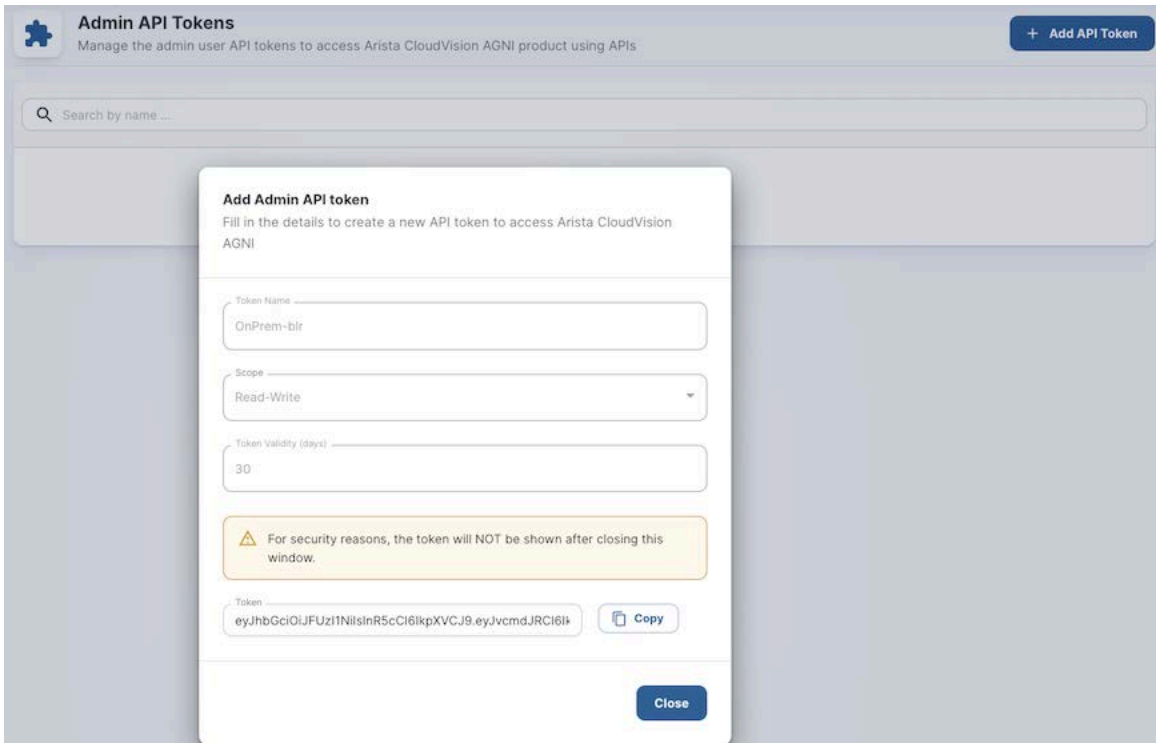


This will generate a one-time token which will be valid for the number of days specified in the **Token Validity** field.

> **Note:** Copy and save the token in a safe and accessible location. This token is required to access the APIs in swagger.

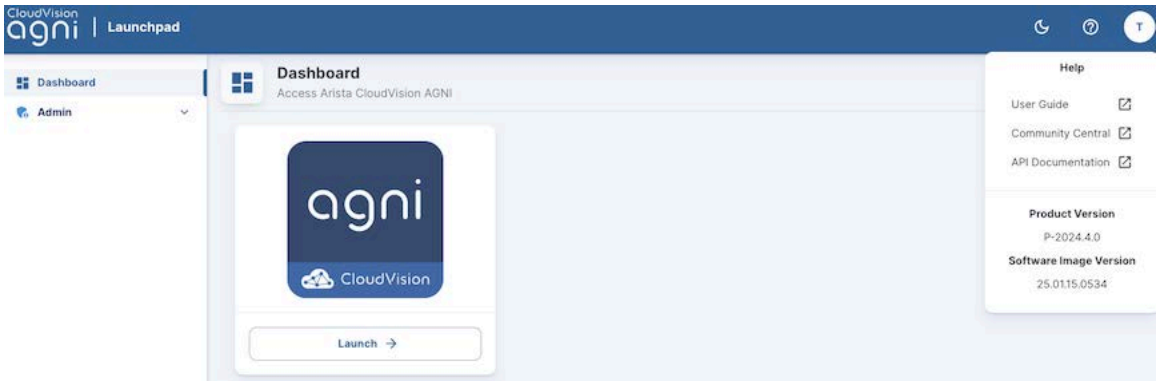
> **Note:** If you want to extend the validity of a token, you must create a new token. You cannot extend a token by editing the token details. Replace the existing token value with the new token in the API script to fetch the data.

Figure 1-9: API Token Details



Add this API token in the curl command to fetch the details from the API documentation. You can access the API documentation from the Help menu on the top right side of any AGNI page.

Figure 1-10: API Documentation Access



1.2.4 Launch App from Dashboard

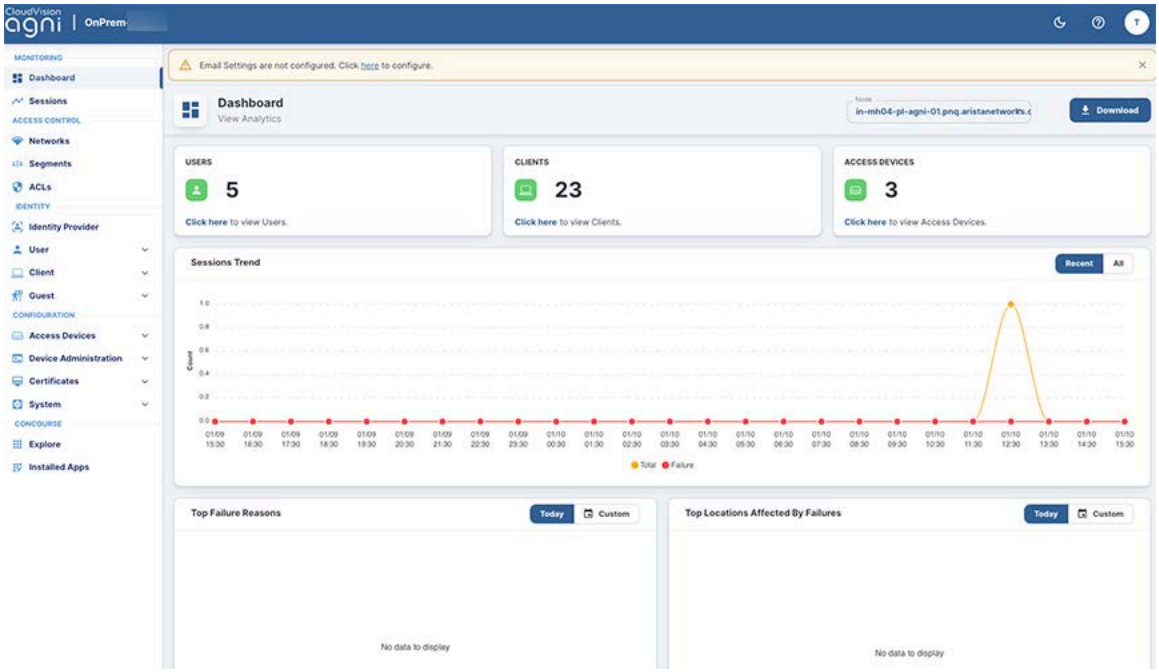
From the Dashboard, click the **Launch** → button to launch the AGNI dashboard of the selected server.

The *Email Settings are not configured* message is displayed on the dashboard and you must configure the email settings by clicking the link. Email Settings are required for AGNI to send email notifications during the User, Device, Guest registrations, Onboarding of users, and during update to any configurations.

The dashboard displays the details about the users, clients, access devices, sessions trend, reasons for top failures, and the top locations affected by the failures for the selected node in the **Nodes** drop-down field. Click the "**click here**" link to view the details.

You can also select a node from the **Node** drop down menu to view the statistics details of a different node. You can view the statistics of individual nodes from the AGNI dashboard.

Figure 1-11: Dashboard



To configure the Email Settings, see the Configuring Email Settings section.

1.2.5 Viewing Nodes in Cluster

Node is a single AGNI appliance that perform the basic product functionality. A node role can be Principal, Standby, or Auxiliary servers. A group of nodes performing the management of appliances is called a cluster. You can add or remove a node from a cluster. A cluster includes the following nodes:

- One Principal node
- One Standby node
- Many (up to six) Auxiliary nodes

For details on creating a cluster and adding nodes, see the Setup and Access Guide for DCA-AGNI-100 appliance available on Arista website.

> **Note:** You can make the configuration changes only on the Principal node, all other nodes are read-only servers. If you login to a standby or auxiliary node, a message is displayed at the top of the page: *This is a ready only server. To make configuration changes, go to Principal server.*

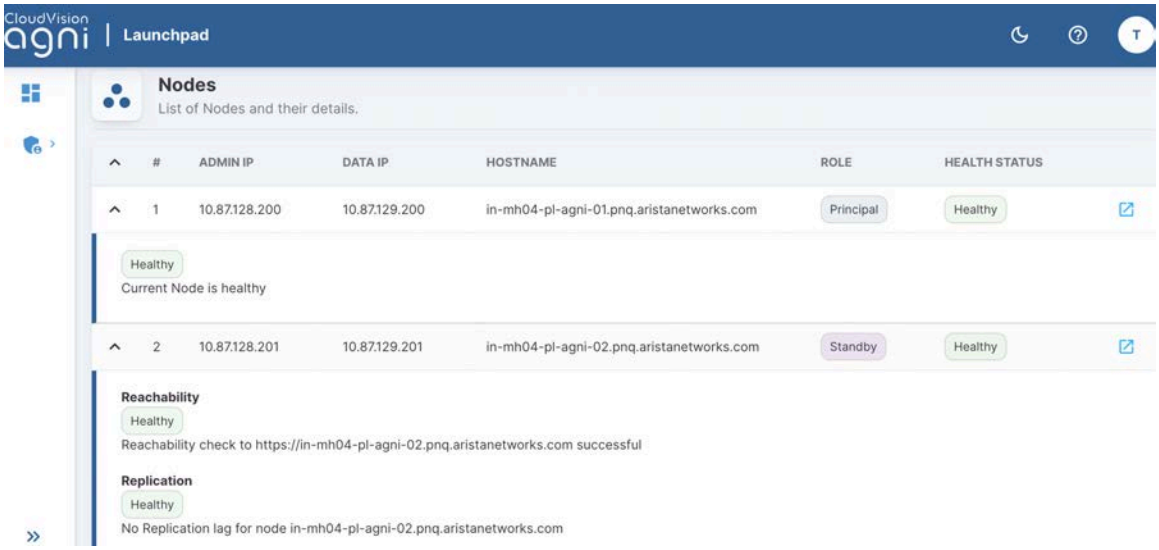
> **Note:** If the Principal node goes down, you have to manually log in to the CLI of the Standby node and promote it as the Principal node.

Figure 1-12: Nodes List and Status

The **Health Status** indicates the health of the nodes and if all nodes are healthy, then the cluster is considered healthy.

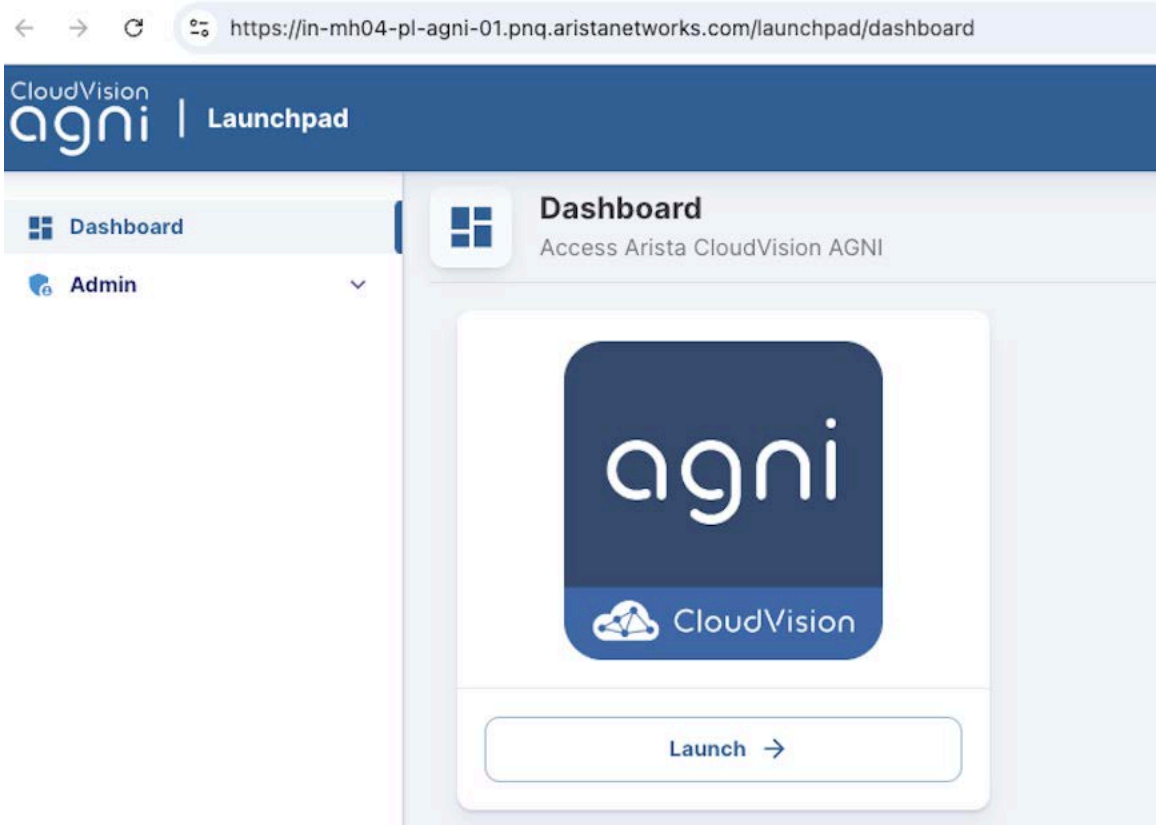
> **Note:** Check the node separately if any node's health status displays the status as "Needs Attention".

Figure 1-13: Viewing Health Status of Nodes



Click the Launch icon at the right end of the page against each node to launch the dashboard of the respective node. For example, see image of the launchpad for the principal node:

Figure 1-14: Launchpad for Nodes



1.2.6 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.

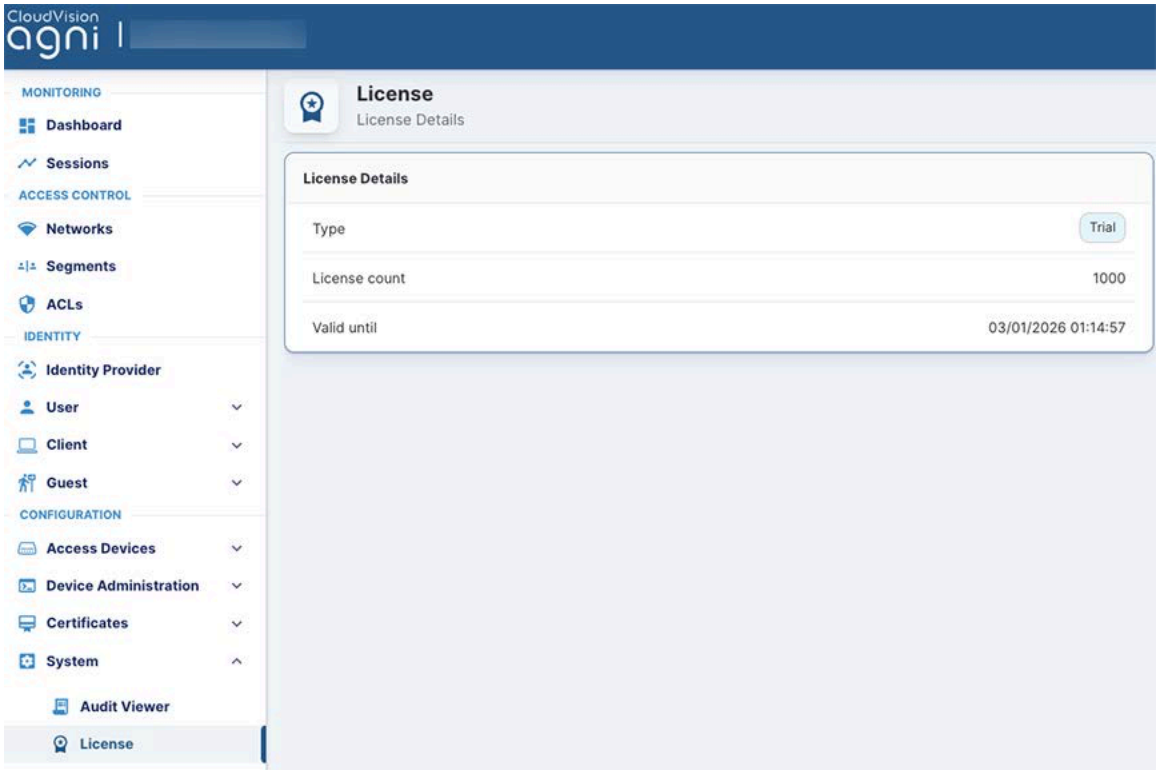
To change the theme and the placement of options, select **Navigation** from the top right side of the portal (see image).

Figure 1-15: AGNI UI Theme (Navigation & Color) Settings

1.2.7 Viewing Licensing Details

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

Figure 1-16: AGNI License Details

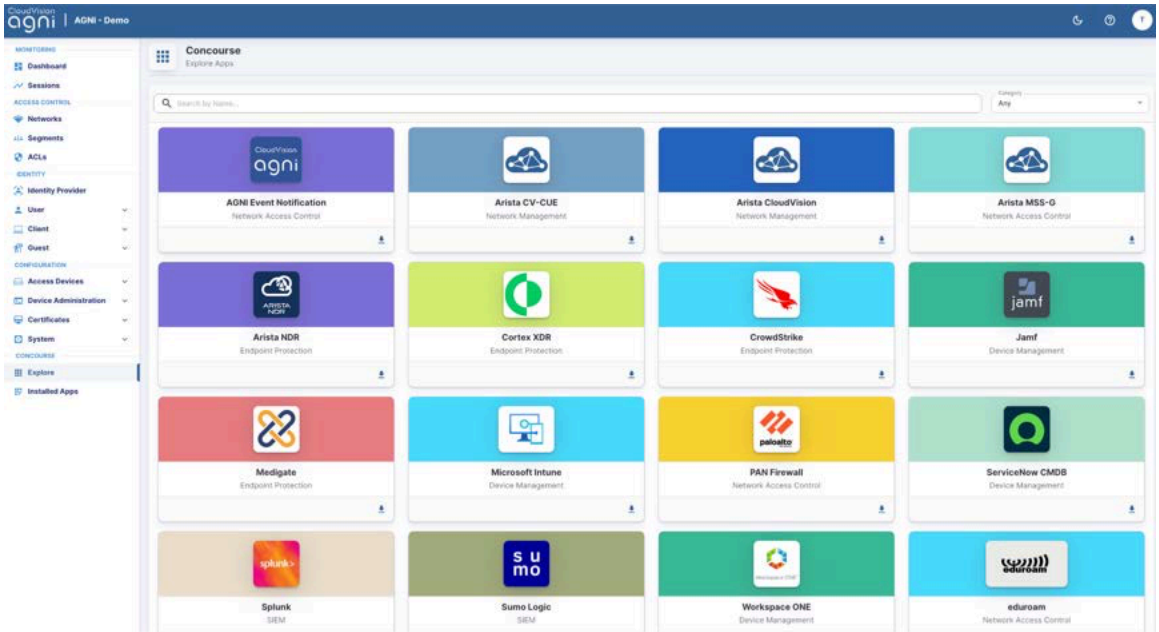


Chapter 2

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 2-1: AGNI Concourse Applications



2.1 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, perform the following steps:

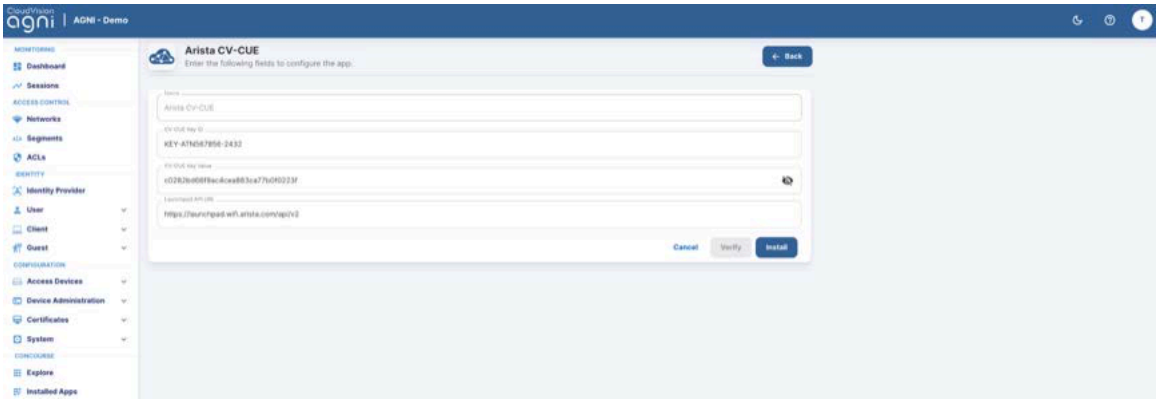
1. Navigate to **Concourse** > **Explore**, select Arista **CV-CUE**.
2. Select the down arrow to install the **Arista CV-CUE** application.
3. Enter the following parameters (see the document to get the Key ID and Value):
   a. Arista CV-CUE in the **Name** field
   b. CV-CUE Key ID

c. CV-CUE Key Value

Figure 2-2: Verify CV-CUE Application

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

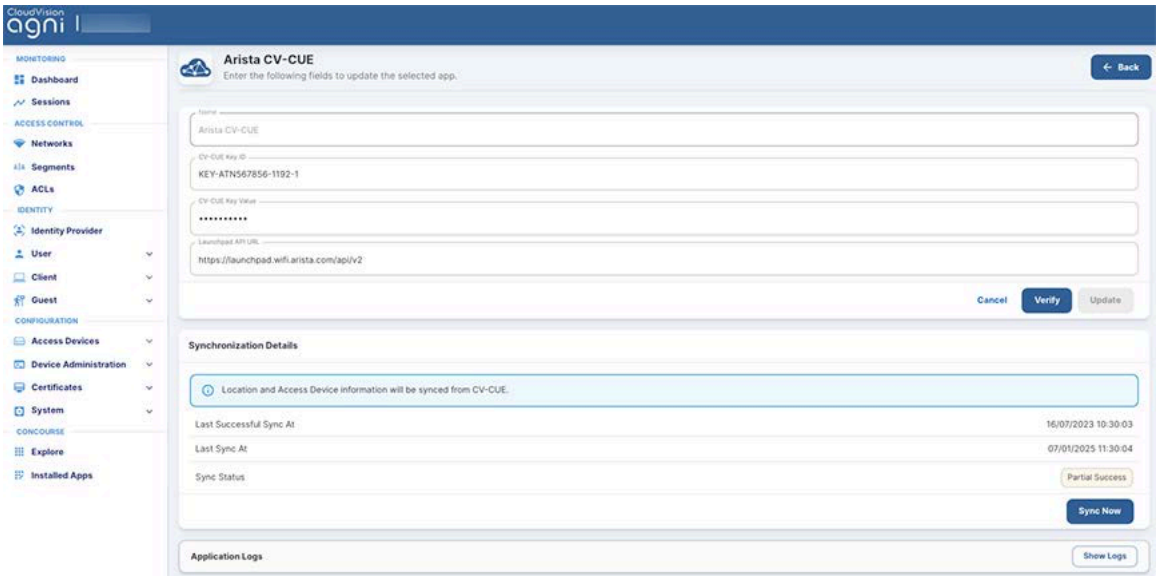
Figure 2-3: Installing CV-CUE Application



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.

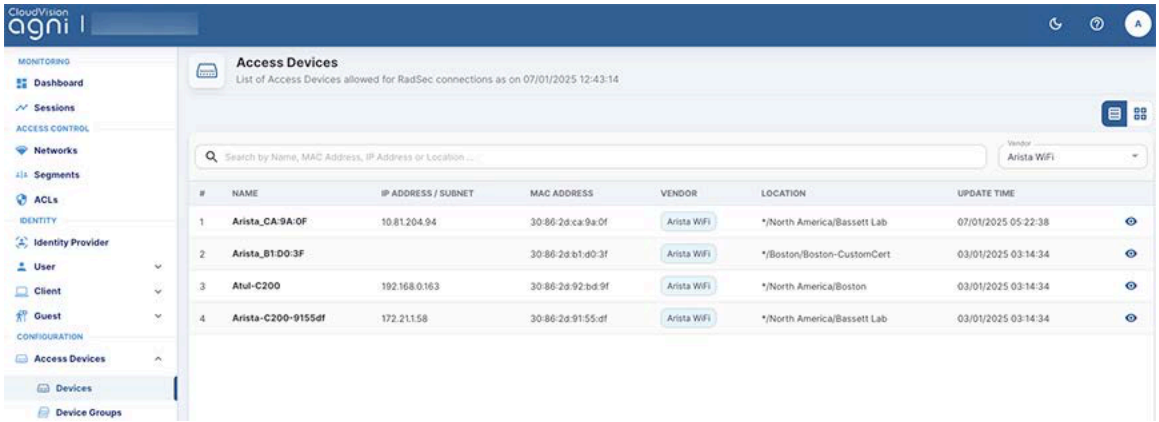
Figure 2-4: Synchronizing CV-CUE App



You can view the synchronized Access Points by navigating to:

Configuration > **Access Devices** > **Devices** (see image).

Figure 2-5: Synchronized Access Points



2.2 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.

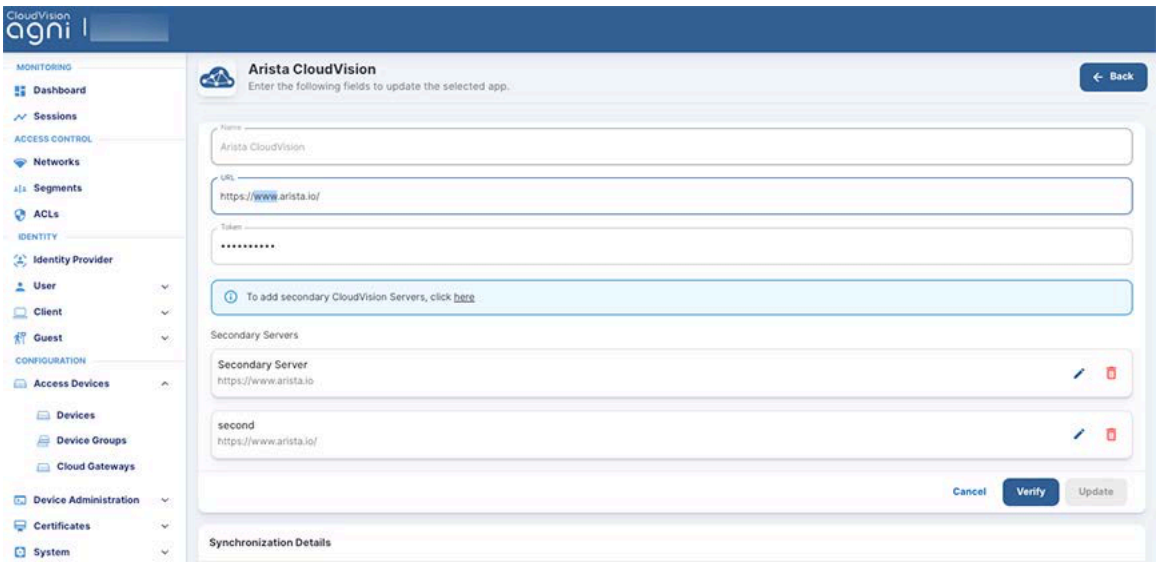
Prerequisites

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, perform the following steps:

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 2-6: 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).

2.3 Arista CloudVision Portal (CVP) 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.

CHECK THIS PAGE AFTER GETTING DETAILS FROM SHRIRANG/Venky

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.

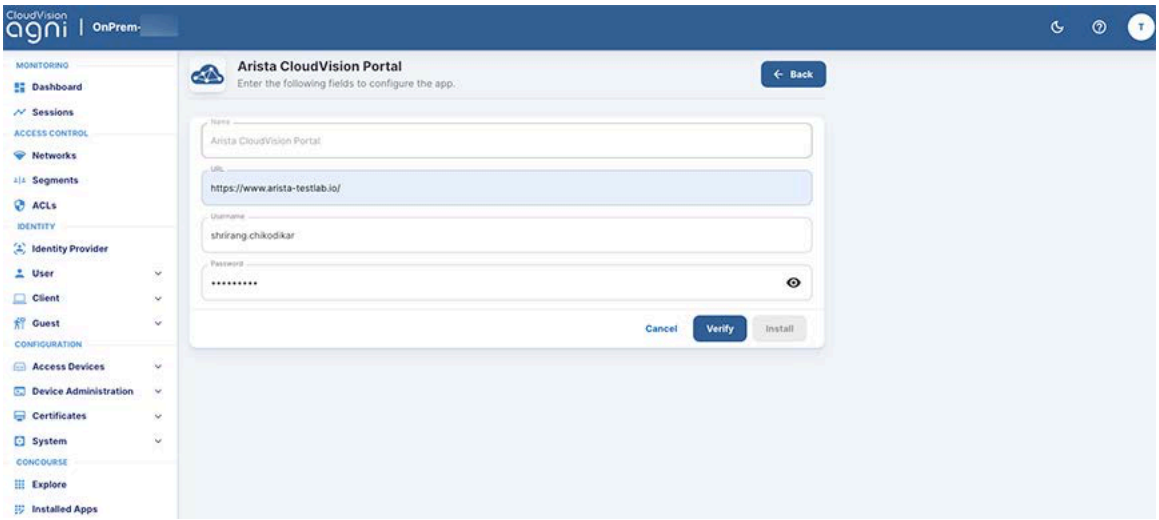
Prerequisites

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 Arista CloudVision Portal, perform the following steps:

1. Navigate to **Concourse** > **Explore**.
2. Install the **Arista CloudVision Portal** application.
3. Enter the following parameters:
   a. Arista CloudVision Portal in the **Name** field.
   b. The URL of the CloudVision Portal application.
   c. Username.
   d. Password

Figure 2-7: Installing Arista CloudVision Portal Concourse Application



4. Click the **Verify** button to validate the credentials.
5. Click the **Install** button to complete the installation process.
   The CloudVision Portal application is displayed as an installed application on the Concourse page.
6. Click the **Sync Now** button on the Arista CloudVision Portal page to initiate the synchronization process.

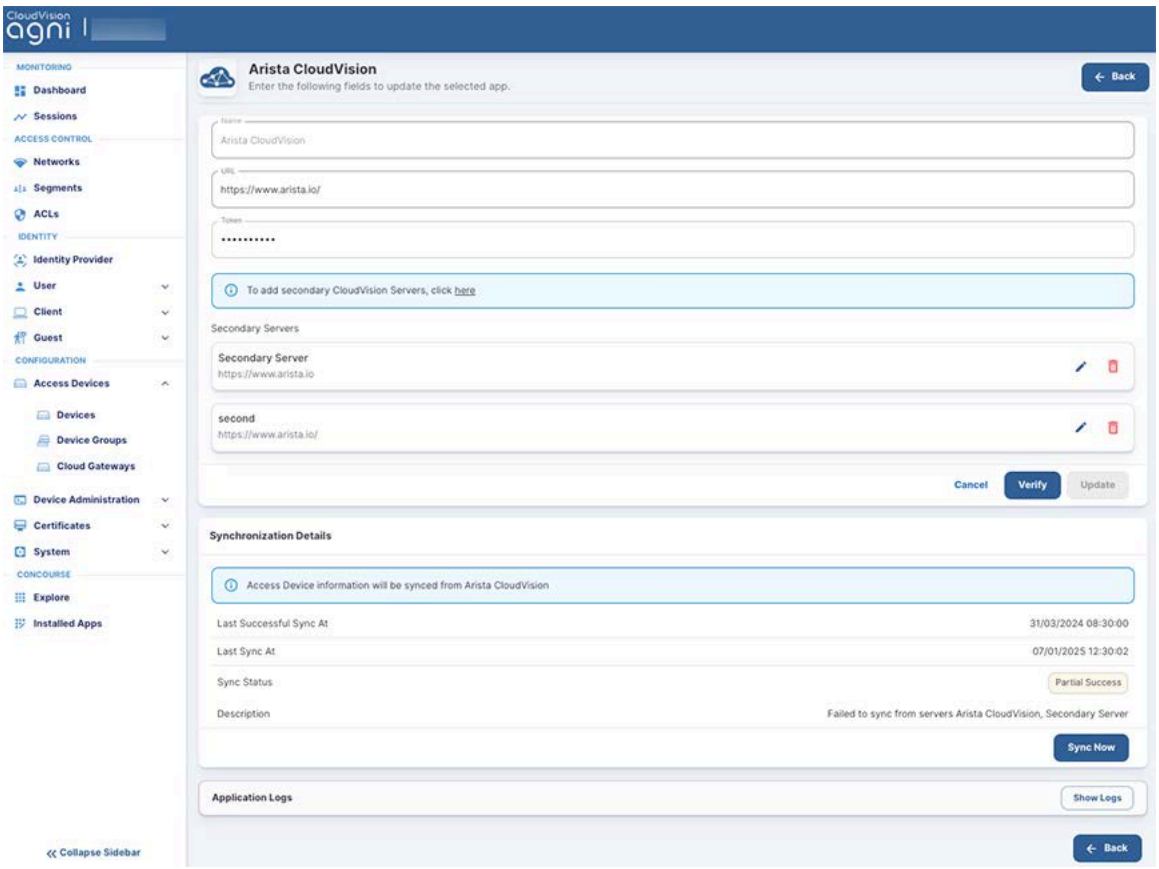
You can view the synchronized switch details by navigating to: **Configuration** > **Access Devices** > **Devices** (See image Synchronized Access Points).

2.4 Configuring CVaaS Instances

To configure CVaaS instances, perform the following steps:

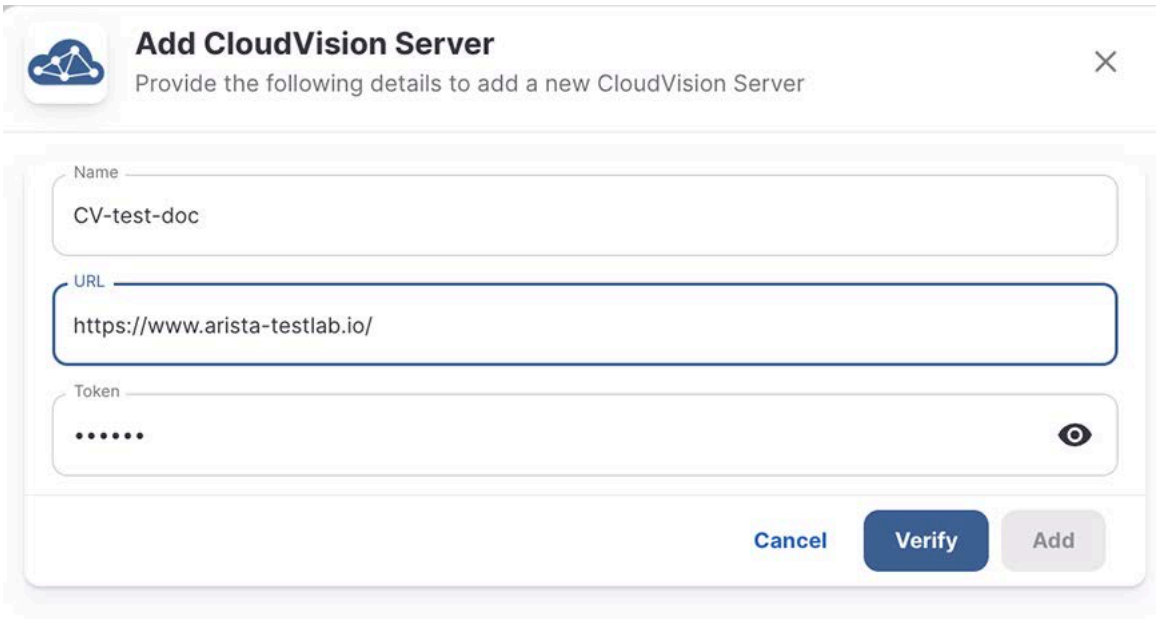
1. Log in to AGNI and navigate to **Concourse** > **Explore** > **Arista CloudVision**.
2. Add a CVaaS instance **URL** and **Token** to add a primary CVaaS in AGNI.
3. Click **Verify** and then **Update** to save the profile.
4. To add multiple CVaaS instances, click the **here** link in the UI while editing the previously added CVaaS profile (see the image).

Figure 2-8: Adding Secondary Servers (CVaaS Instances)



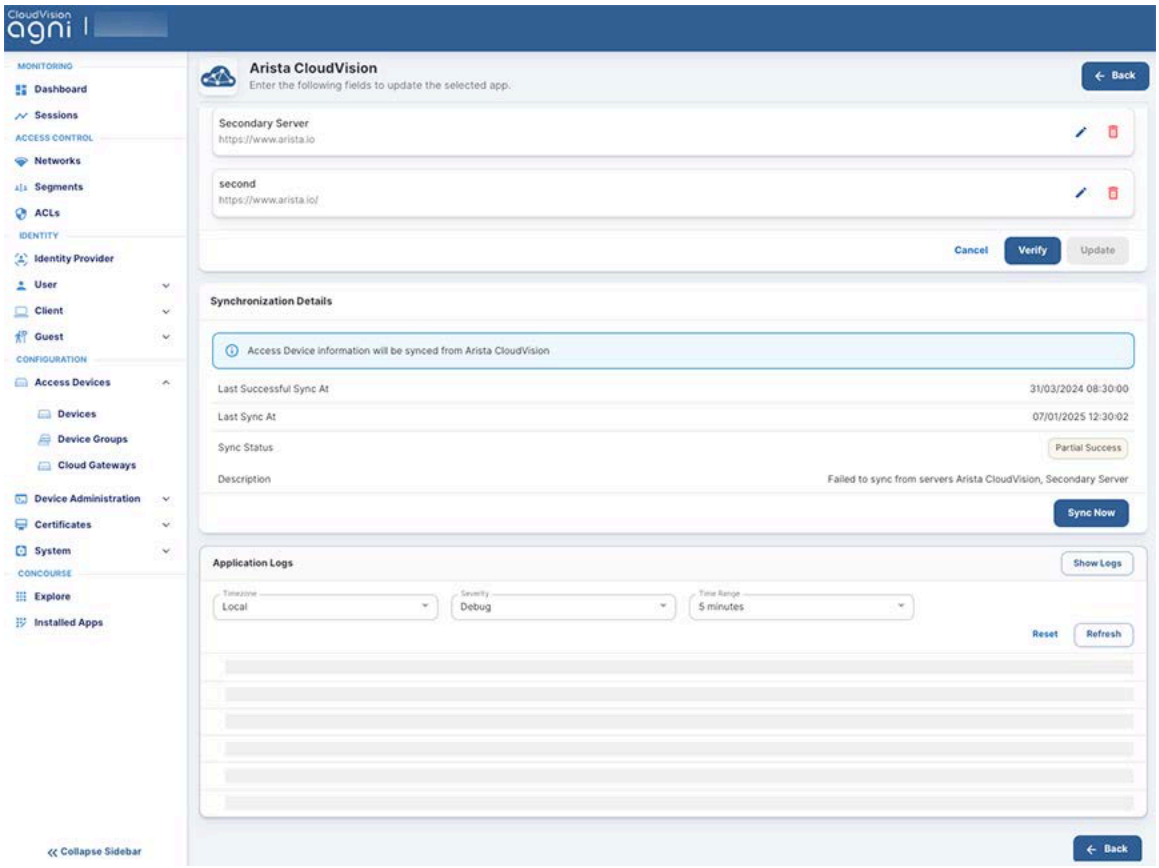
5. On the displayed pop-up window, add the secondary CVaaS **URL** and API **Token**.

Figure 2-9: Adding Secondary Servers



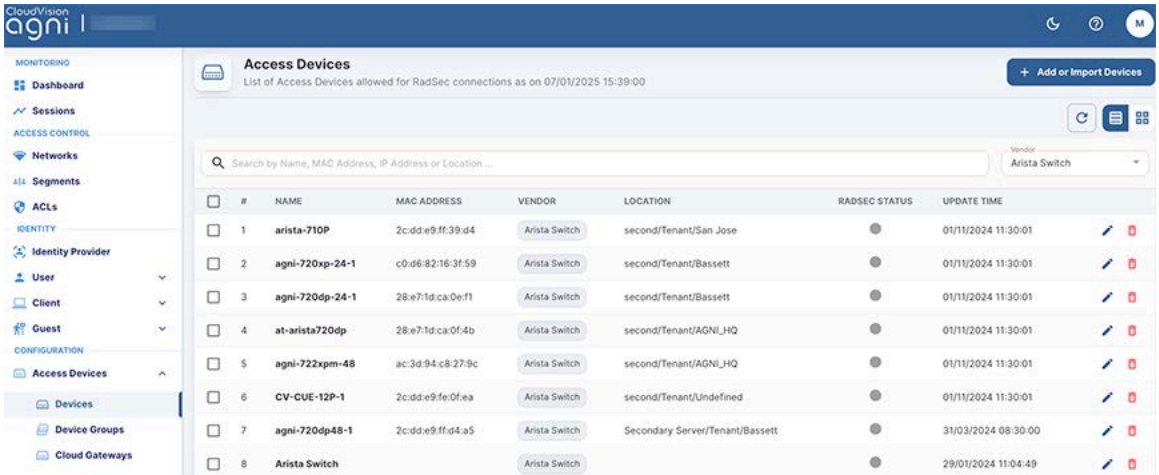
6. Click **Verify** and then **Add** to save the secondary CVaaS. The dashboard displays multiple CVaaS instances in the Concourse application (see image below).

Figure 2-10: CVaaS Synchronization



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.

Figure 2-11: View Access Devices



2.5 Adding Multiple CVaaS Instances in AGNI

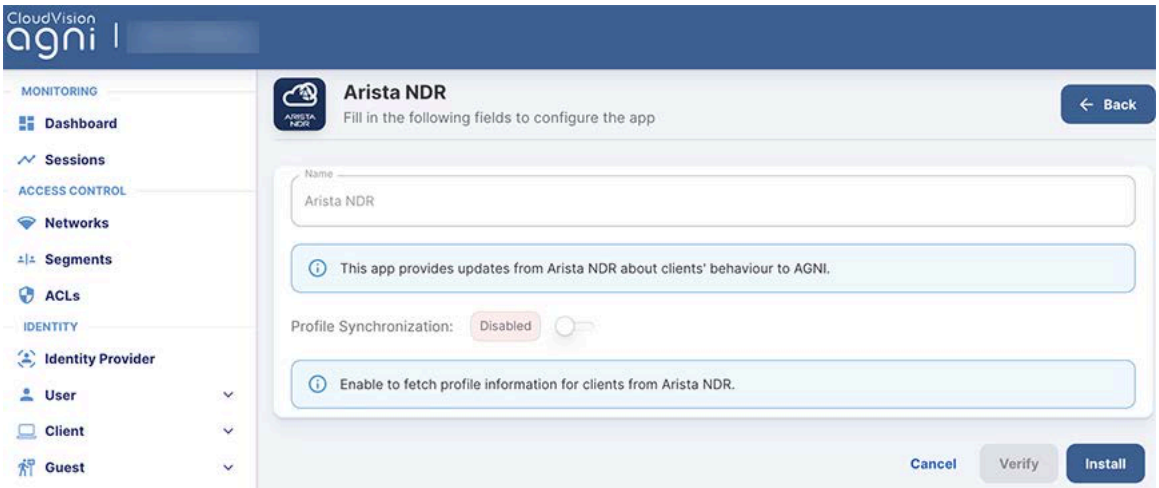
You can configure multiple CVaaS instances that are linked to AGNI. As you add multiple CVaaS instances, AGNI fetches all the managed switches and adds them to the AGNI database. To add multiple CVaaS instances, you must log in as an admin and complete the AGNI configuration. For more details, refer to the document.

2.6 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, perform the following steps:

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

   Figure 2-12: 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).

Figure 2-13: Arista NDR Integration API Details

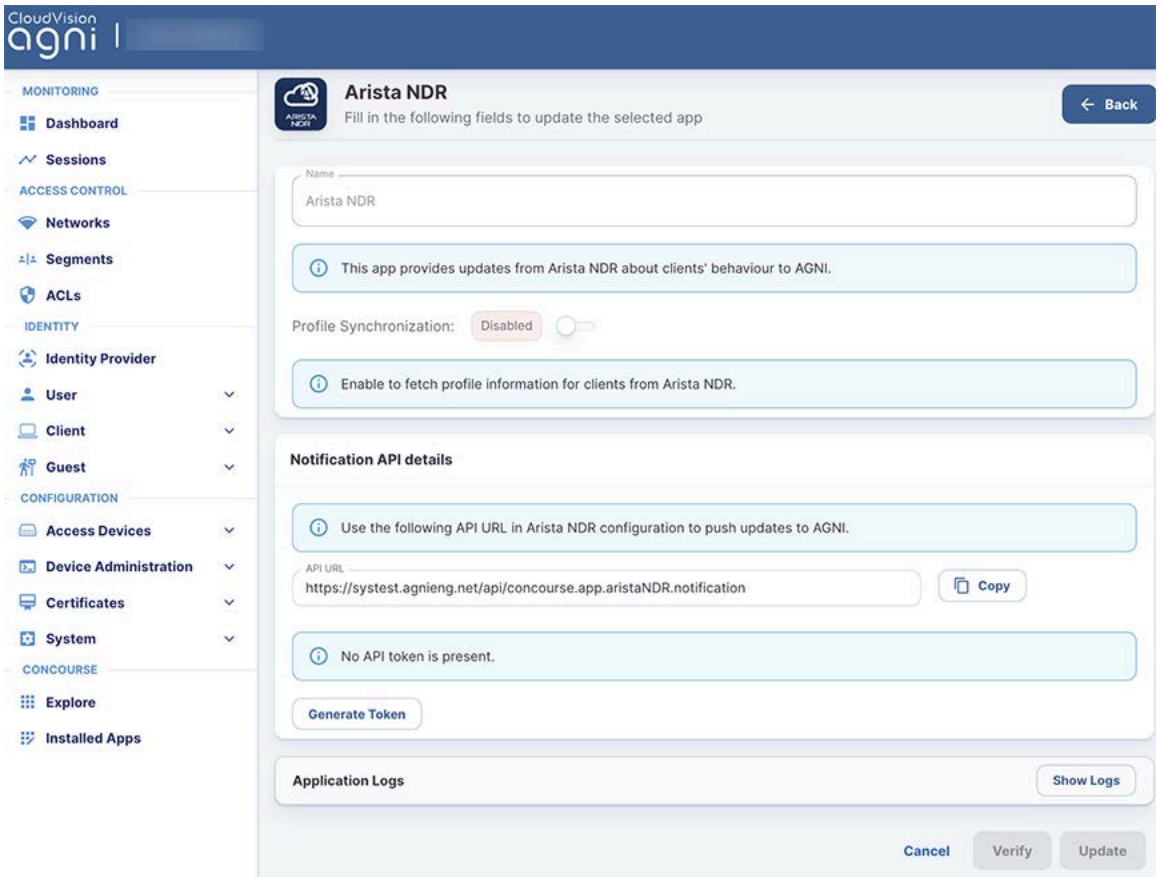
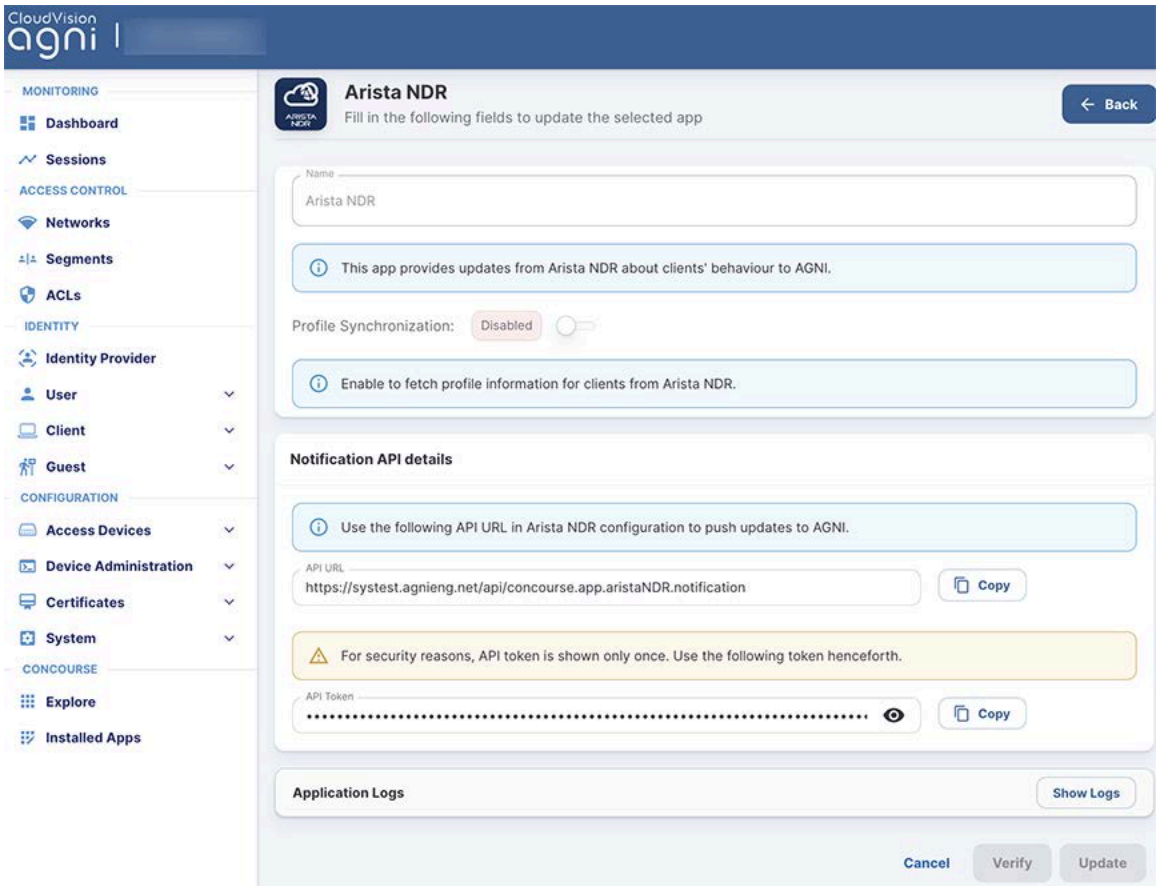


Figure 2-14: Arista NDR Integration API and Token Details

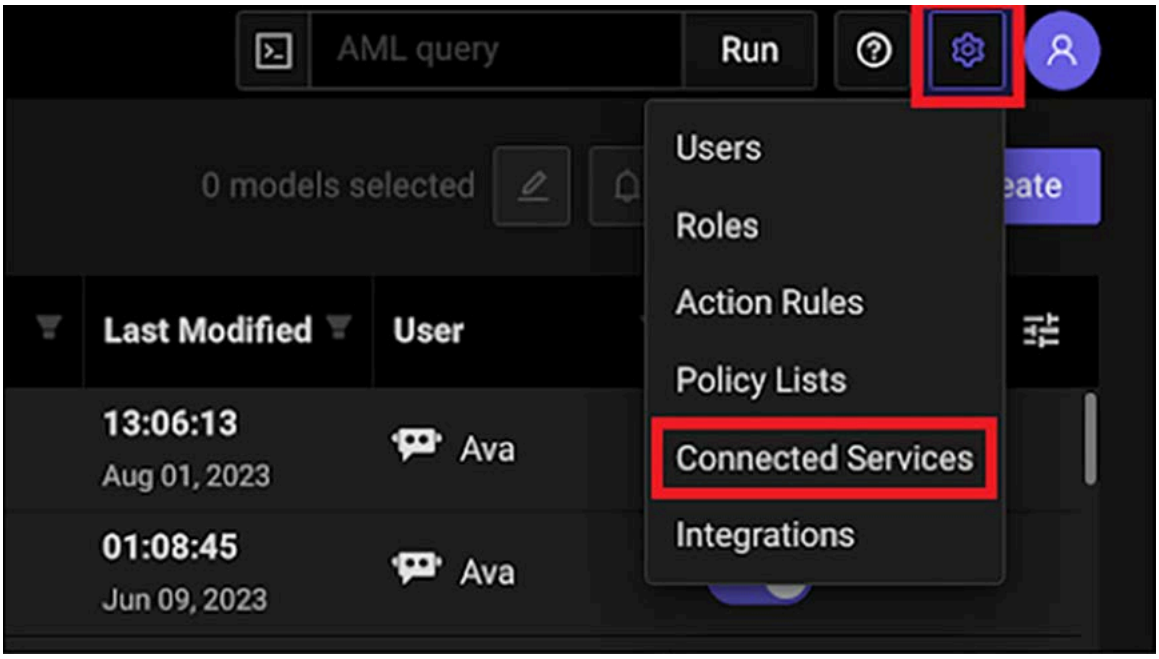


2.6.1 Configuring Arista NDR

To configure Arista NDR, perform the following steps:

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

   Figure 2-15: Arista NDR Settings Page

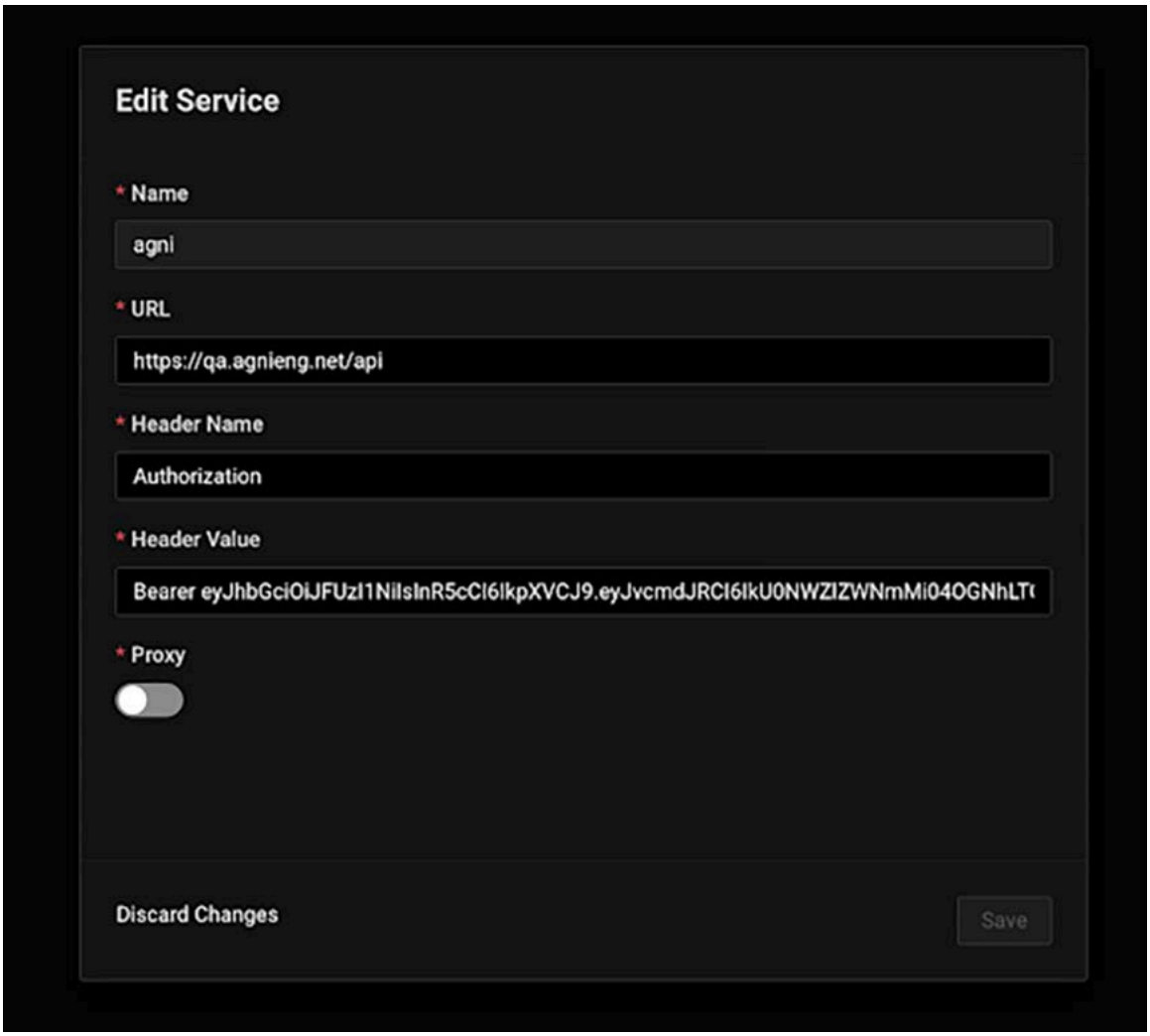


2. Click on the **Add Service** option to add a new connected service in NDR (see image below).

   Figure 2-16: Arista NDR Configuration - Add Service

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

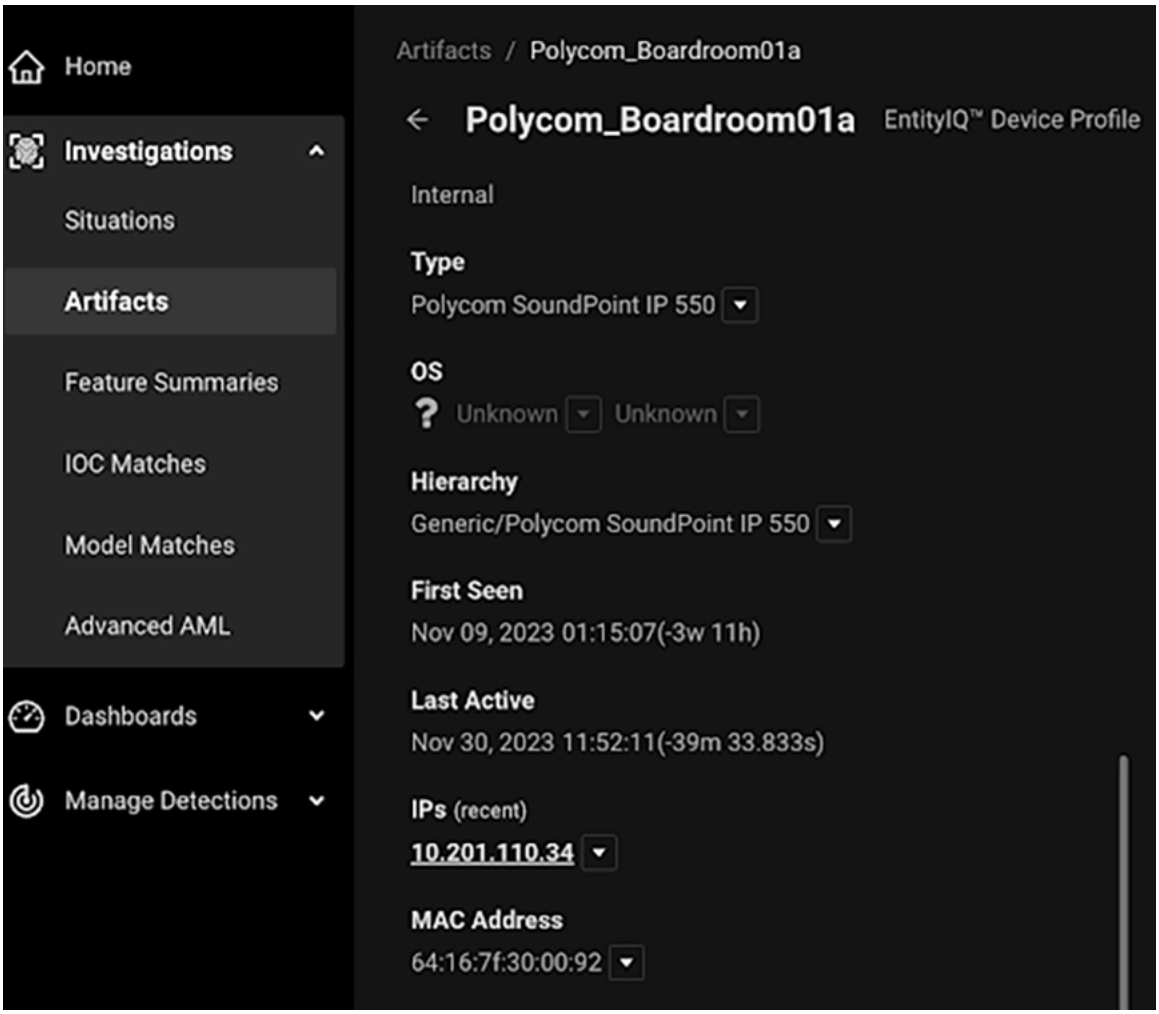
Figure 2-17: Arista NDR Configuration Details



4. Click the **Save** button to add AGNI service to NDR.

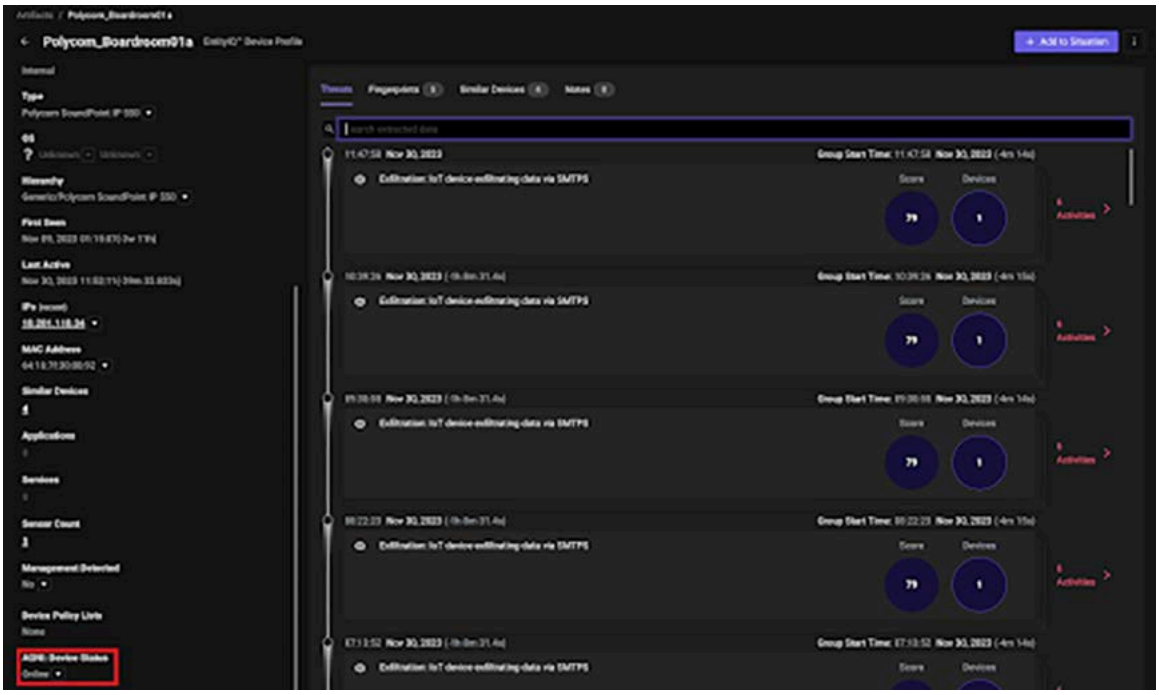
5. Navigate to **Investigations** > **Artifacts** from the left panel.

Figure 2-18: 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 2-19: Arista NDR - AGNI Integration Status



2.6.2 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.

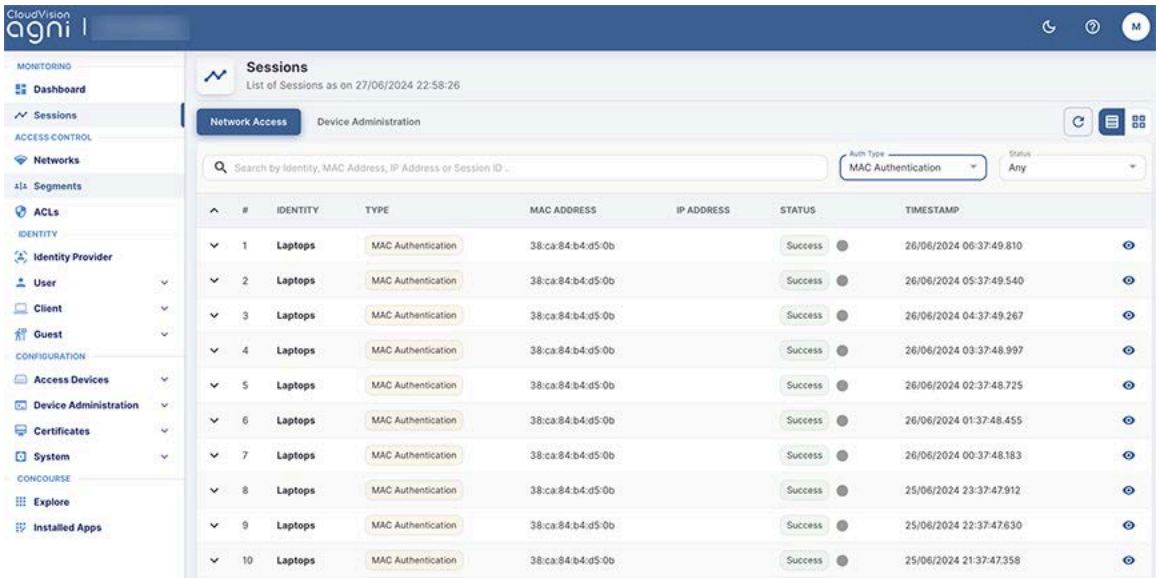
The profiling information includes - Device Brand, Device Hierarchy, and Device Type. The **Risk Action** is administrator-driven. This is pushed to AGNI at the discretion of the administrator when the device is deemed risky through the NDR detection process.

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

- Navigate to **Sessions** and select a device.

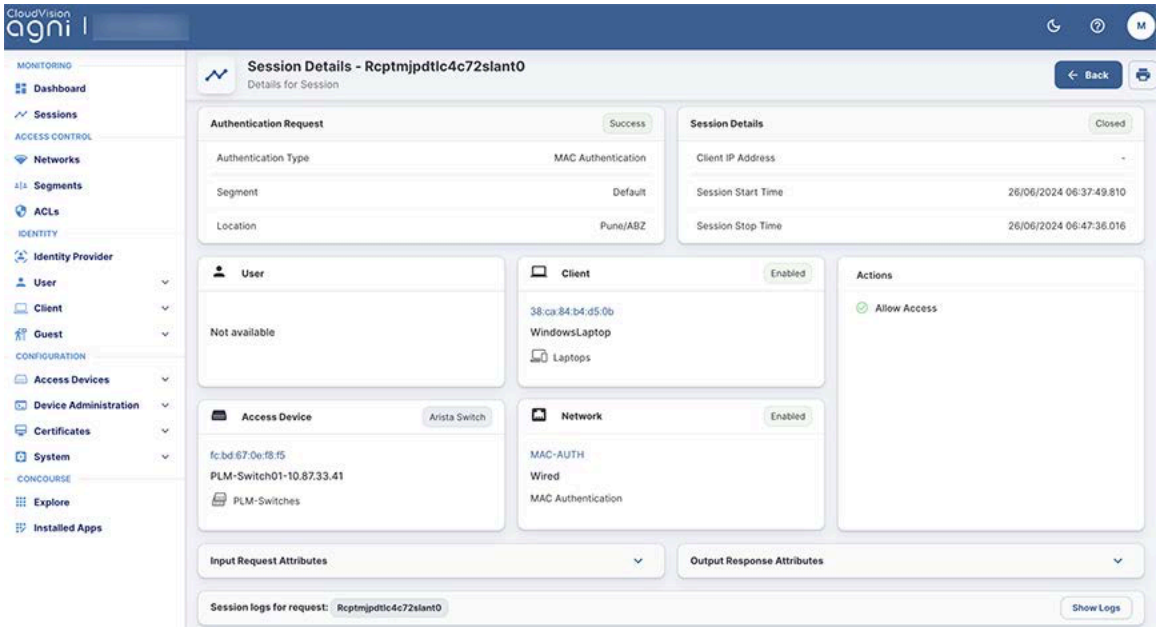
- Click the MAC address of the device.

Figure 2-20: Sessions Details



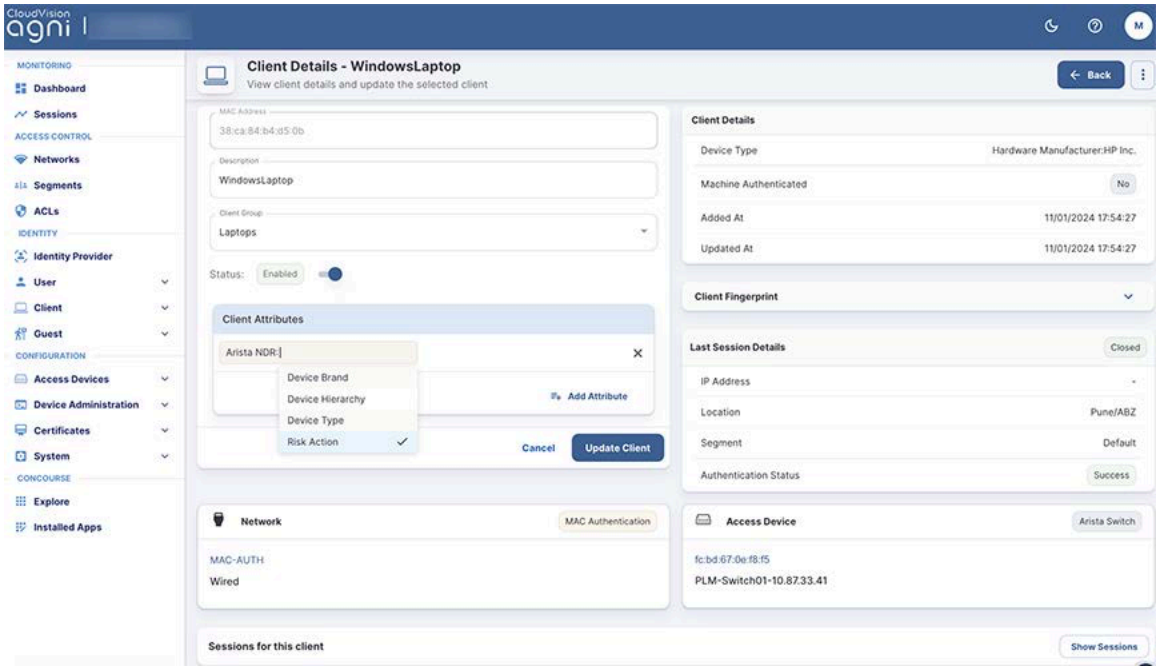
- In the **Client** tab, click the MAC address of the device.

Figure 2-21: Sessions Client Details



- Add the details and click **Update Client**.

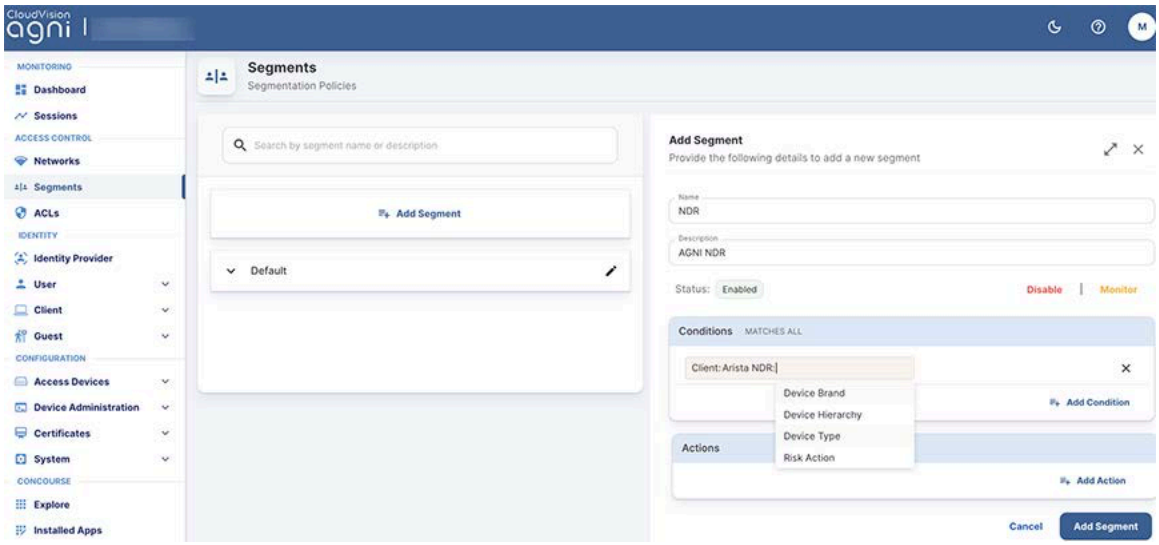
Figure 2-22: NDR Client Details



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

- Navigating to **Access Control** > **Segment**.
- Selecting **Add Segment**, based on the **Client:Arista NDR**.
  - Device Brand
  - Device Hierarchy
  - Device Type
  - Risk Action

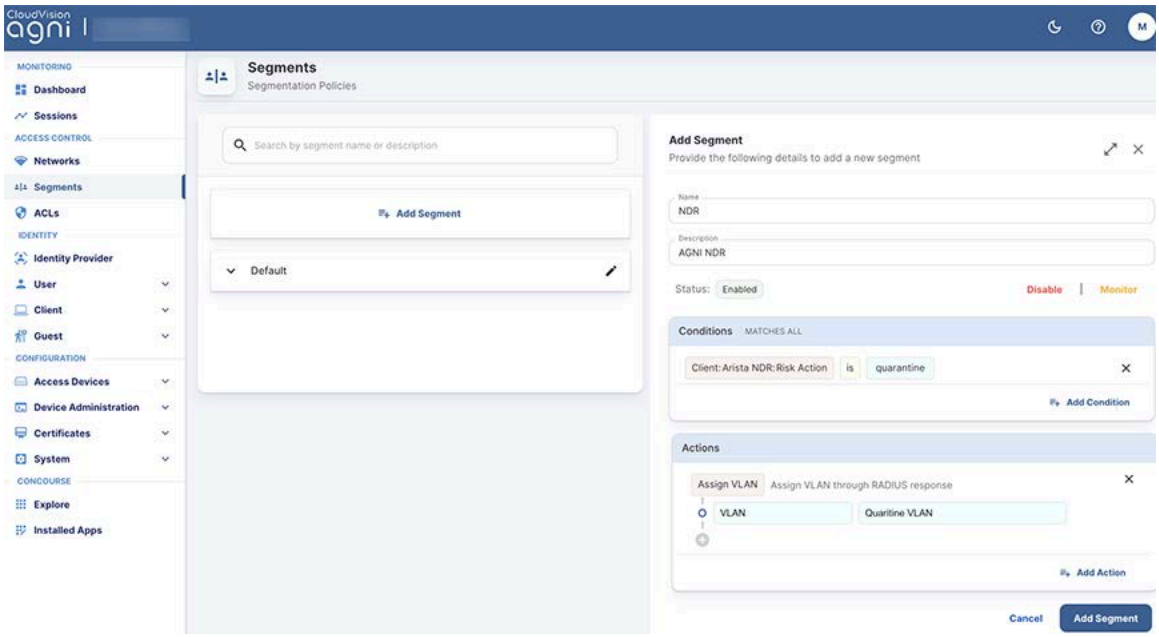
Figure 2-23: Add Segment Details



2.6.3 Using Risk Action in Segment Policies

To use **Risk Action** in segmentation policy:

Figure 2-24: Add Segment Details for Risk Action



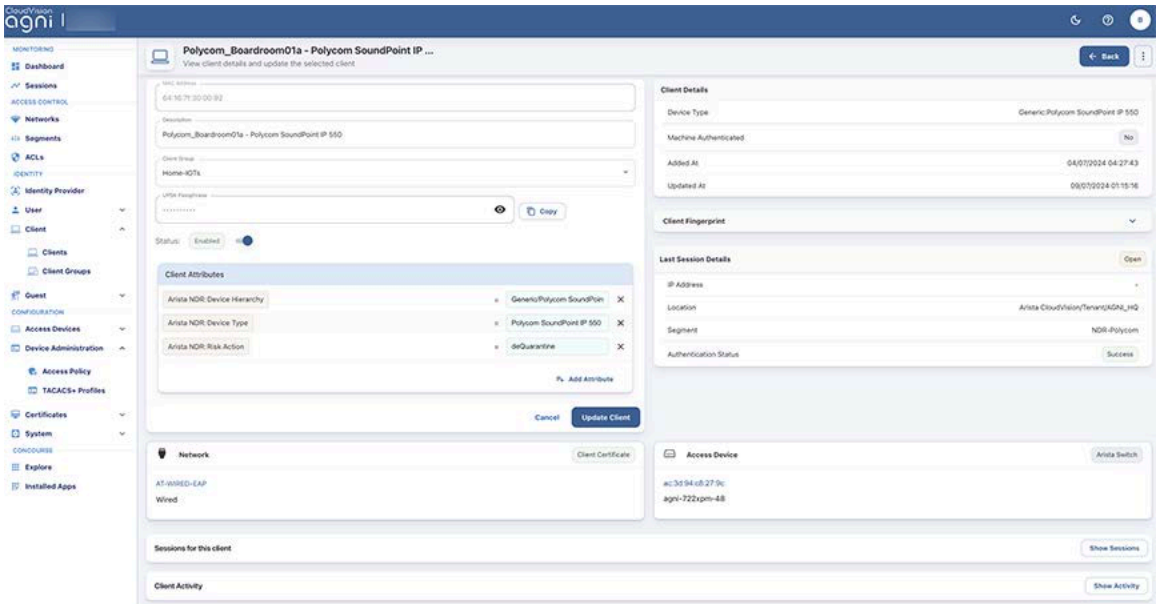
In Arista NDR, when a device is at risk, the admin changes the risk action to Quarantine, after which AGNI applies the segment policy, and as displayed in the above configuration, AGNI moves the client to **Quarantine VLAN** after matching the segment policy. However, triggering the Risk Action is an administrative action on NDR. Refer to the 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 2-25: Update Client Details for Risk



Chapter 3

Integrating with Concourse Applications (External)

AGNI enables you to integrate several third-party vendor applications as described in the following sections:

3.1 Palo Alto Cortex XDR Integration

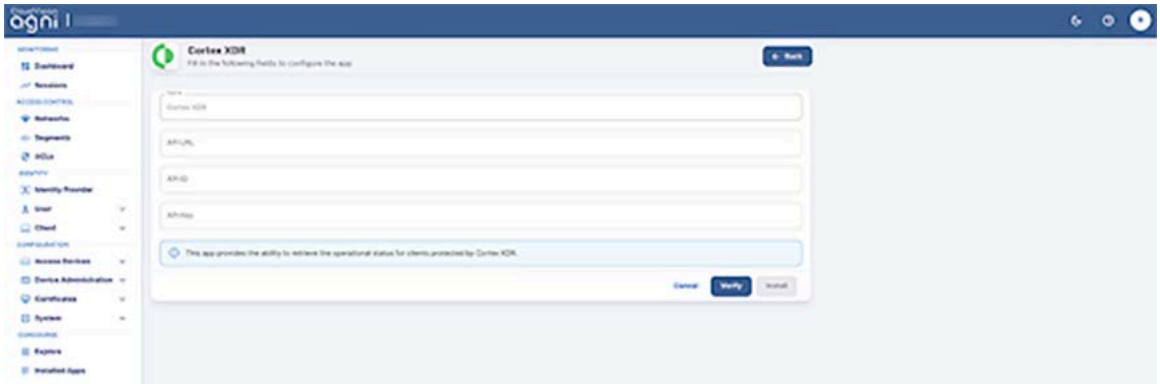
Palo Alto Cortex XDR is an Endpoint Protection concourse application. Enabling Cortex XDR integration facilitates AGNI's retrieval of posture details from client devices managed by this external application. The posture details are associated with the clients and can be used in the segmentation conditions.

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, perform the following steps:

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 3-1: 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.

3.2 Medigate Integration

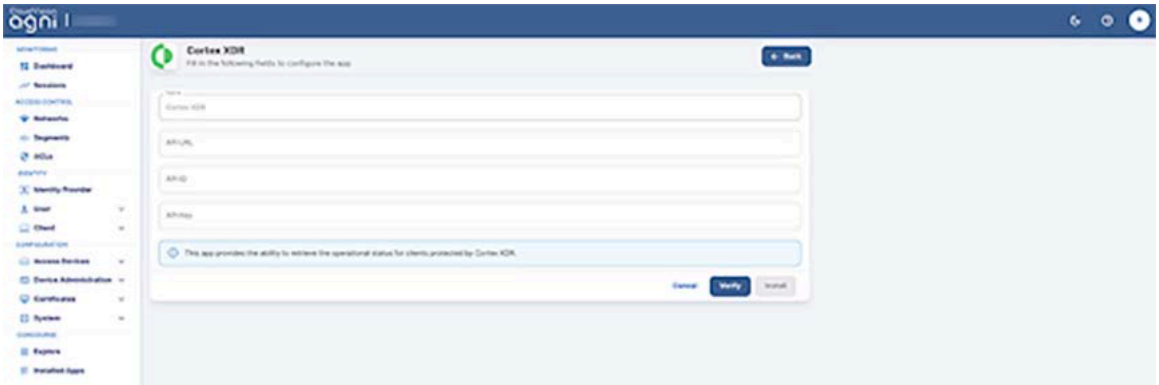
Medigate is an Endpoint Profiling concourse application. Enabling Medigate integration facilitates AGNI to retrieve device profile details of the clients connecting to the network. Medigate profiles include medical, IoT, IoMT, and several other devices that are connected to the network. The profiled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

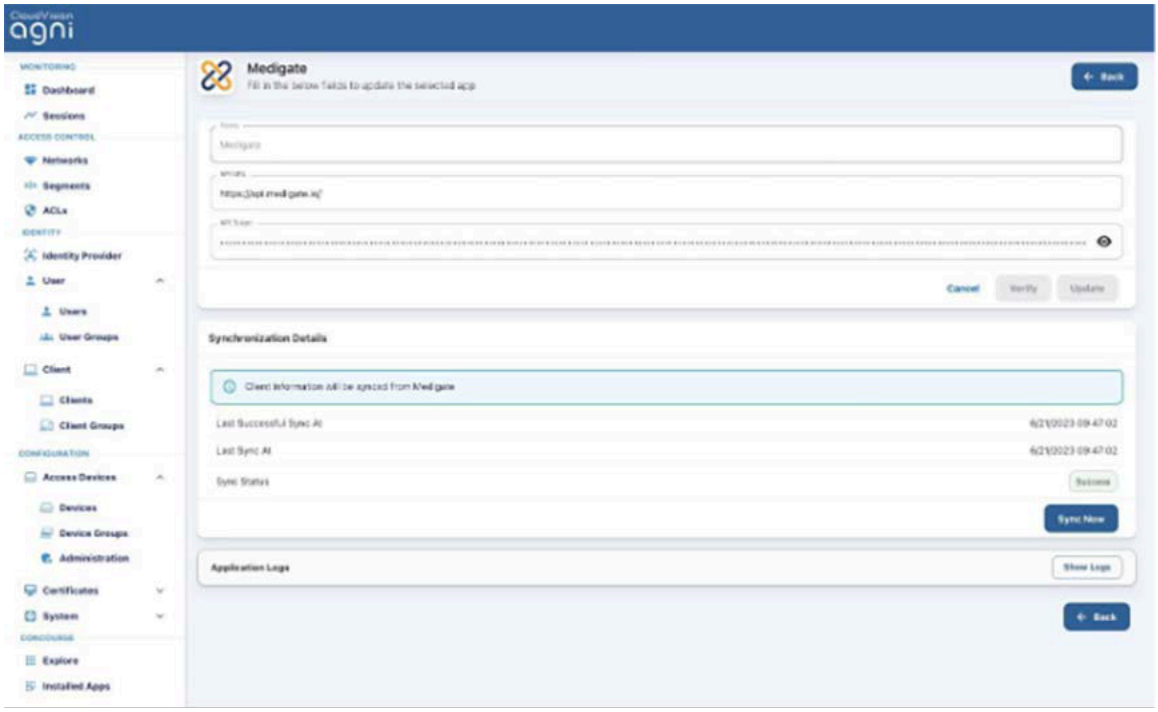
   Figure 3-2: Installing Medigate Concourse Application



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 3-3: Installed Medigate Concourse Application



3.3 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.

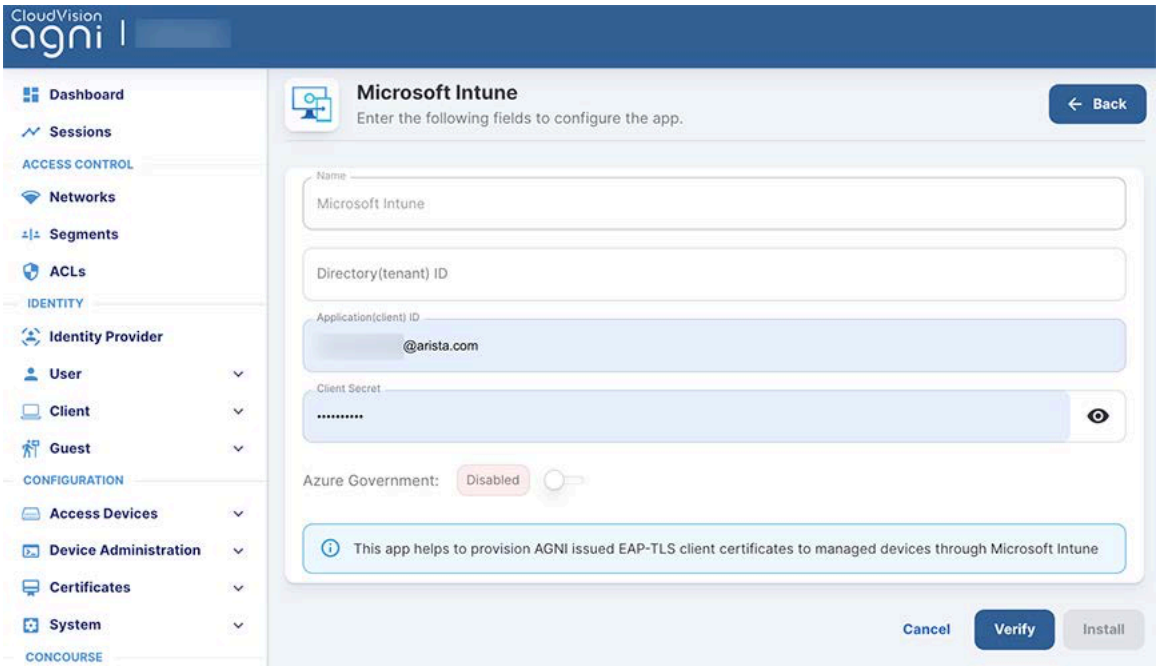
Prerequisites: The Intune integration requires API credentials with necessary permissions to fetch the client attributes and compliance information. Refer to vendor documentation to configure and obtain the API credentials.

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

1. Navigate to **Concourse** > **Explore**.

2. Install the **Microsoft Intune** application (see image below).

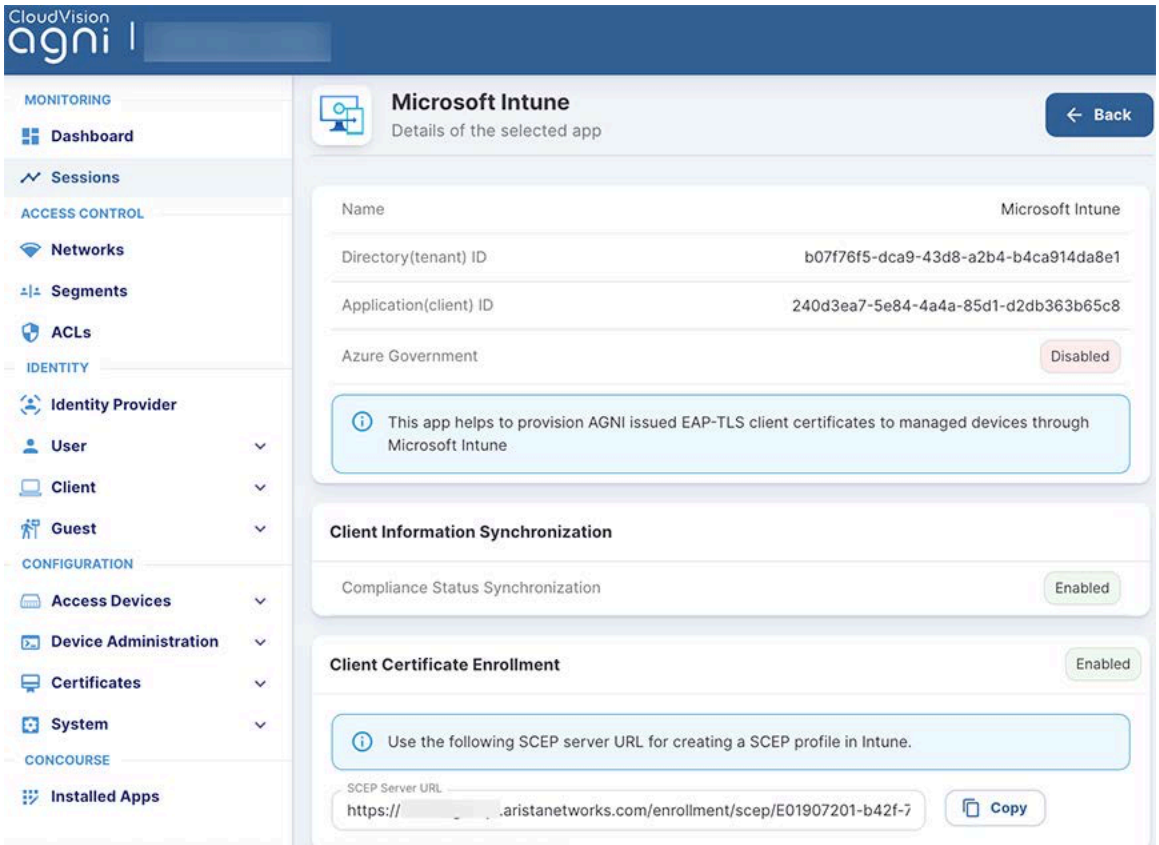
Figure 3-4: Installing Microsoft Intune Concourse Application



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.

Figure 3-5: Installed Microsoft Intune



3.4 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.

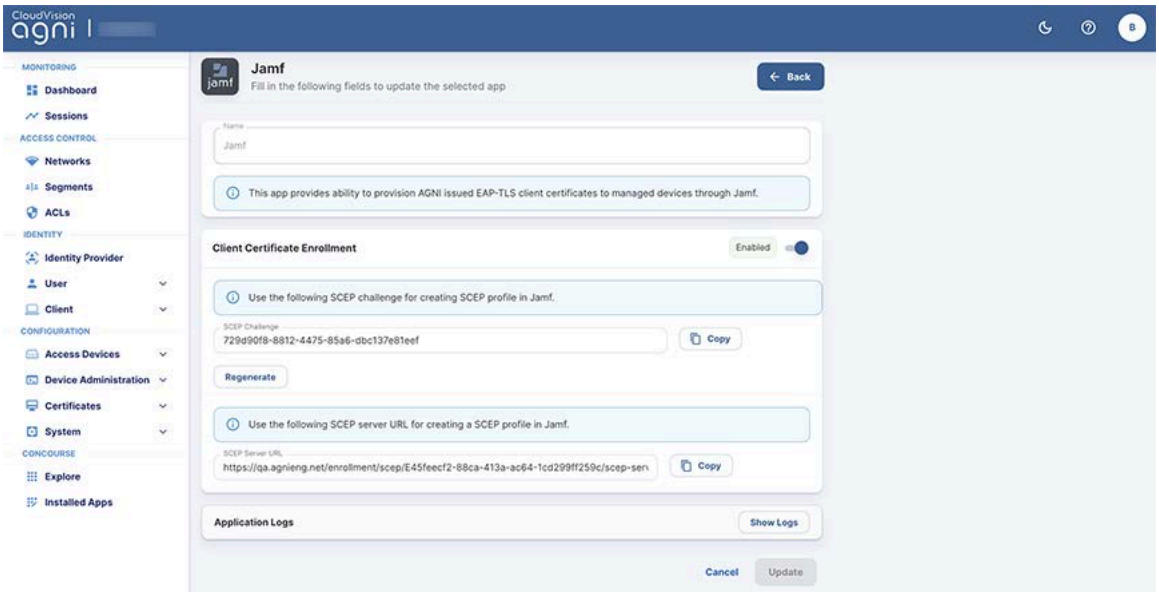
Prerequisites: The Jamf integration requires the SCEP challenge and the URL generated in AGNI to be configured in the Jamf administration portal. Refer to vendor documentation for details on configuring these parameters.

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

1. Navigate to **Concourse** > **Explore**.

2. Install the **Jamf** application (see image below).

   Figure 3-6: 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.

3.5 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.

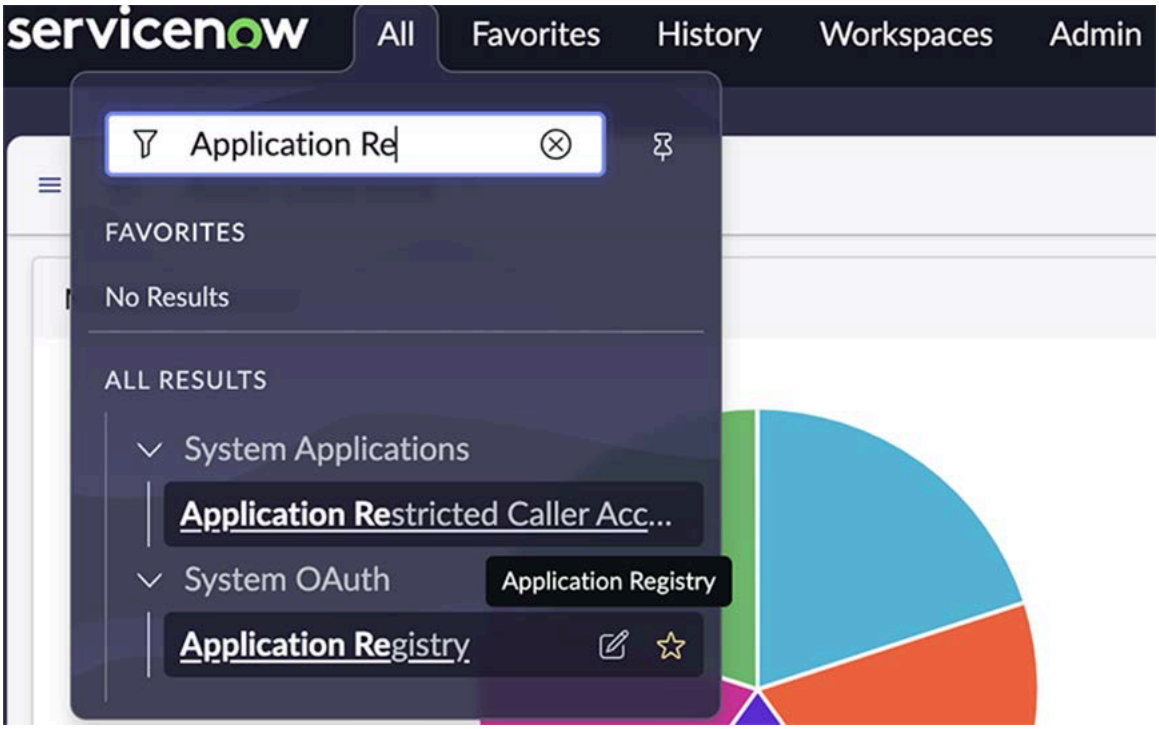
This requires a configuration change in AGNI and ServiceNow CMDB.

To configure ServiceNow for AGNI integration, perform the following steps:

1. Login to the ServiceNow CMDB portal.

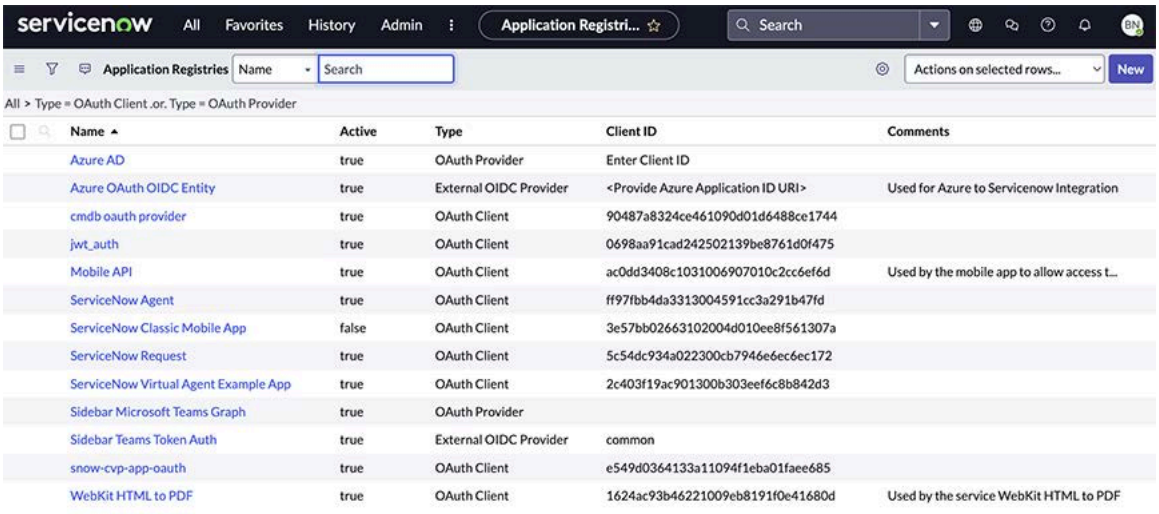
2. Click the **All** tab and search for **Application Registry Under the System OAuth** option.

Figure 3-7: 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.

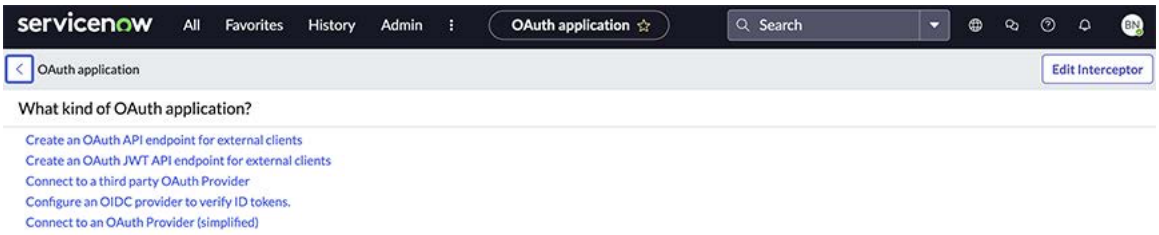
Figure 3-8: Create a new Application for AGNI



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 t...
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

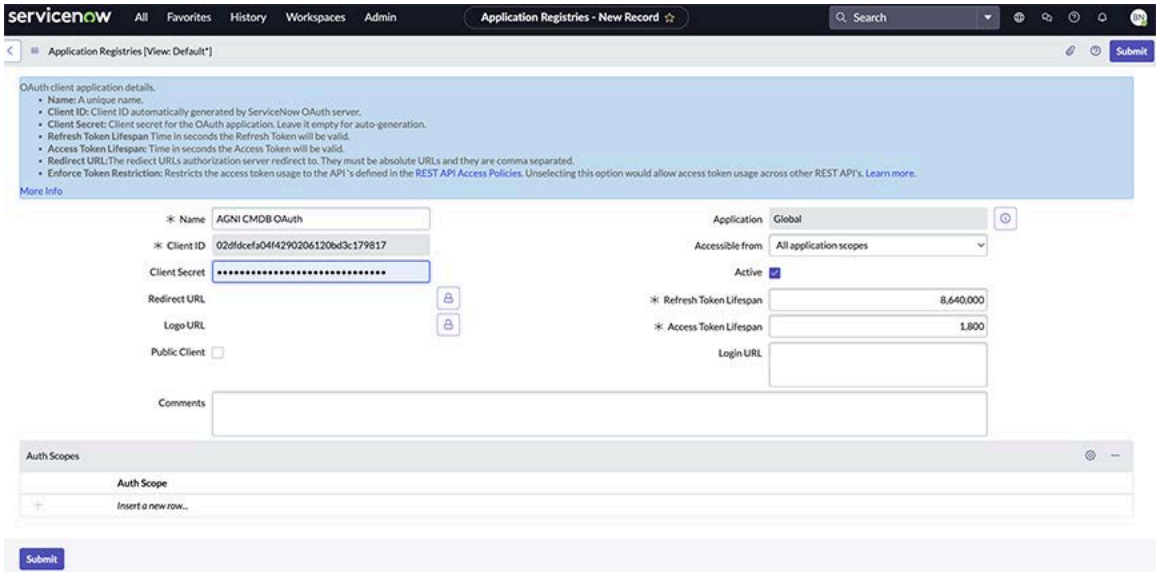
5. Select **Create an OAuth API endpoint for external clients** from the list of OAuth application types.

Figure 3-9: Select OAuth API Endpoint for External Clients



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

Figure 3-10: Provide CMDB OAuth details for AGNI



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

3.6 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.

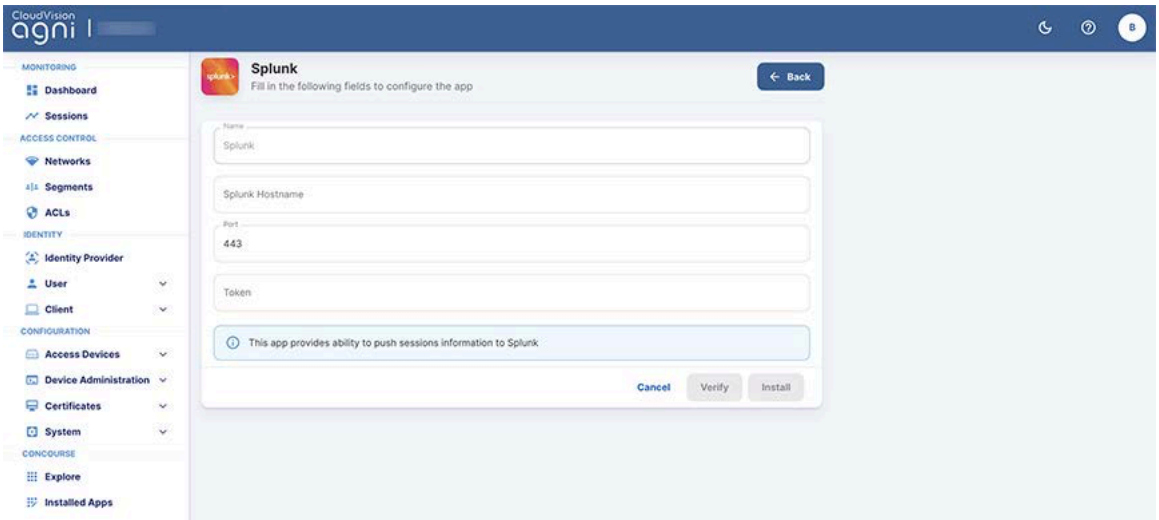
Prerequisites: The integration requires Splunk SIEM credentials to be configured as part of the concourse application configuration. Refer to vendor documentation for details on configuring these parameters.

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

1. Navigate to **Concourse** > **Explore** .

2. Install the **Splunk** application (see image below).

Figure 3-11: 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.

3.7 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.

Prerequisites: 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.

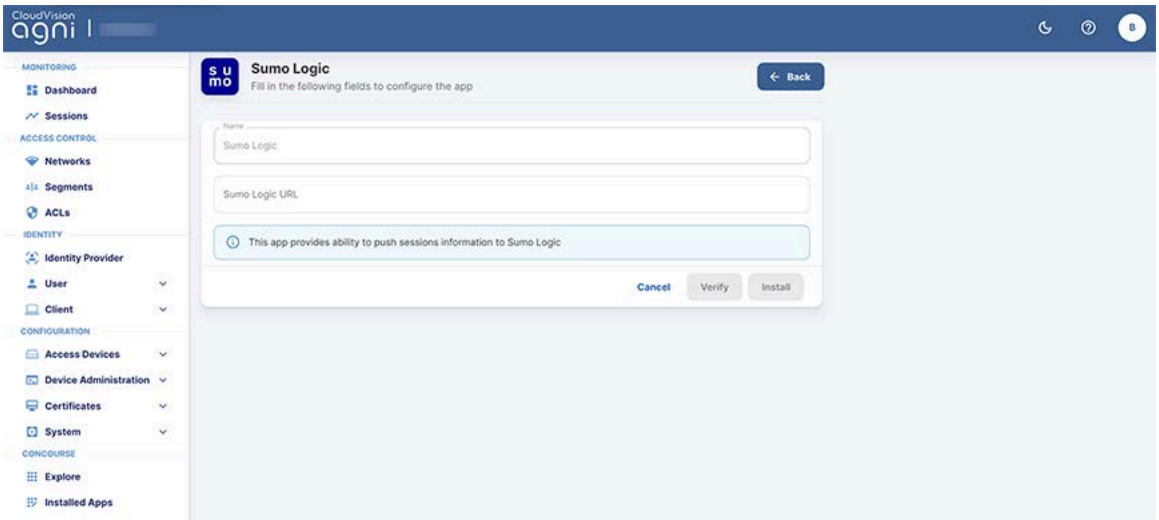
Integration is achieved through installing this concourse application to facilitate session log updates from AGNI.

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

1. Navigate to **Concourse** > **Explore**.

2. Install the **Sumo Logic** application (see image below).

   Figure 3-12: 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.

3.8 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.

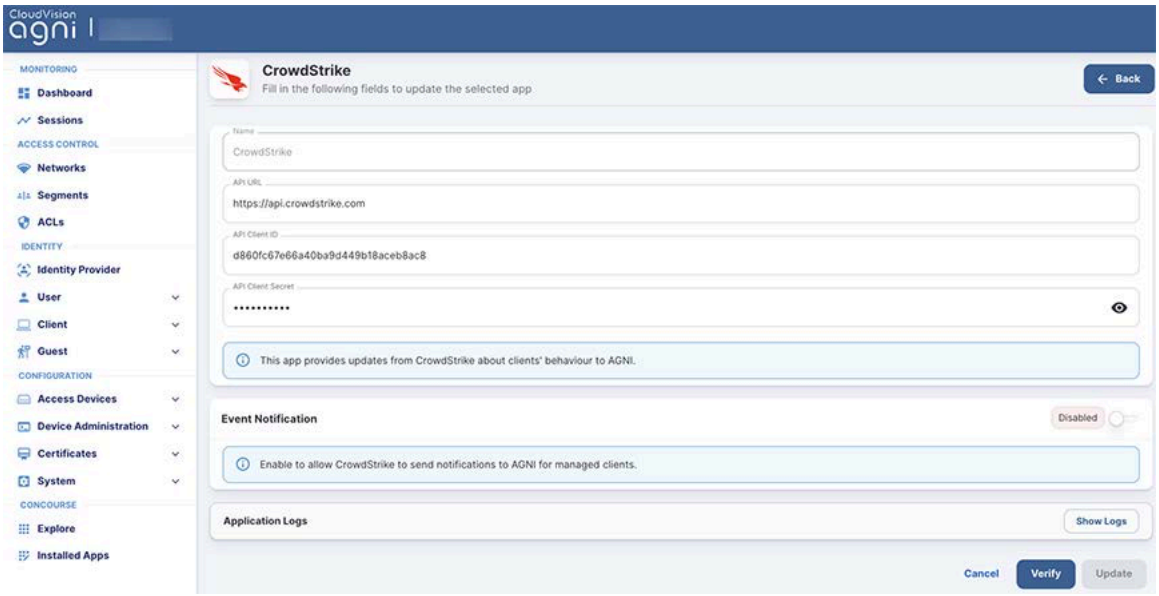
For details on CrowdStrike, see the vendor documentation.

To install CrowdStrike on AGNI, perform the following steps:

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.

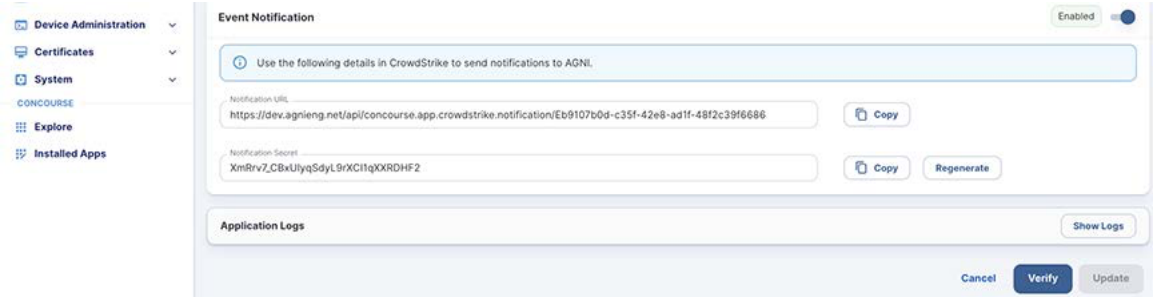
Figure 3-13: Installing CrowdStrike Concourse Application



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 3-14: Event Notification Configuration for CrowdStrike



3.9 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.

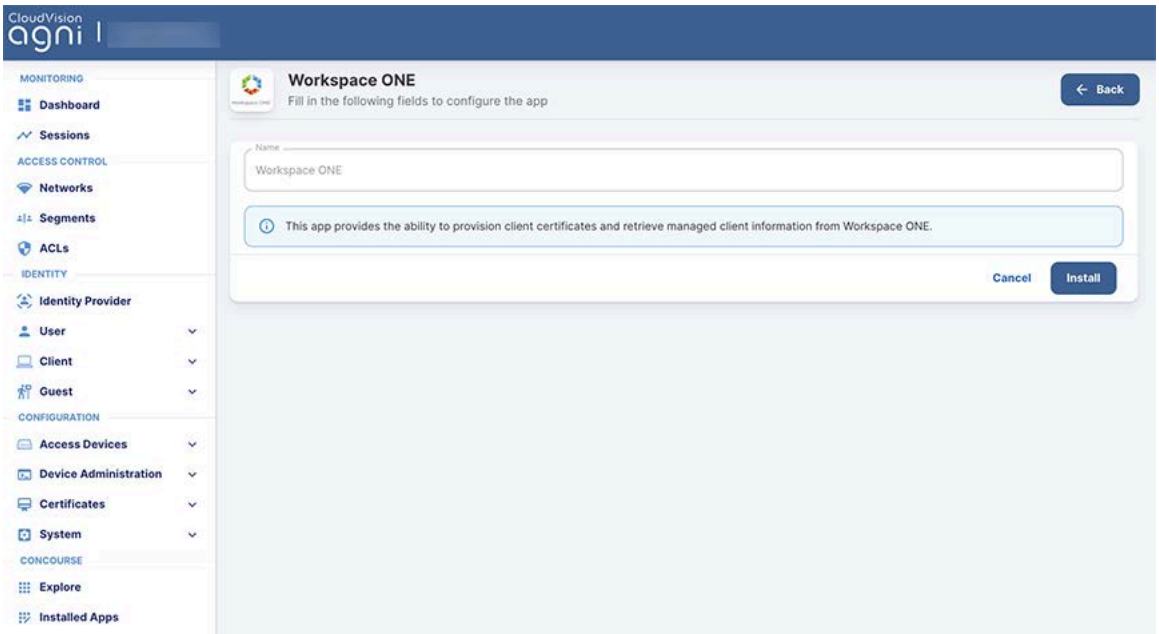
The integration of Workspace ONE with AGNI provisions the certificates and Wi-Fi profiles of the managed clients for connecting to an EAP-TLS network.

Prerequisite: 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, perform the following steps:

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 3-15: Installing Workspace ONE

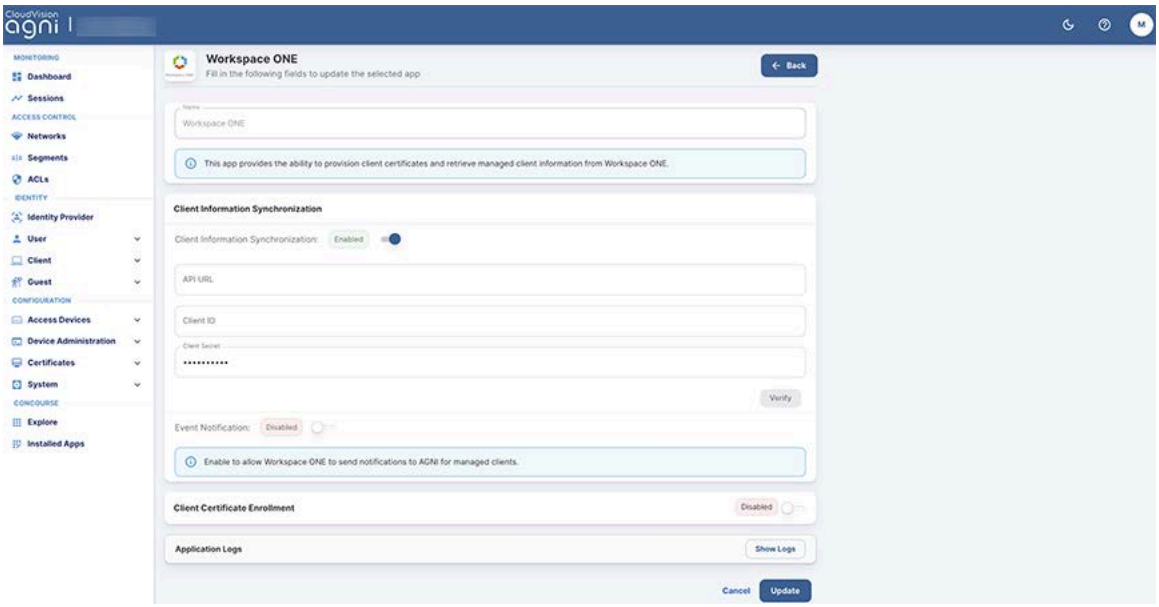


4. Enable the **Client Information Synchronization** if you use compliance policies with Workspace ONE.

   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.

   Figure 3-16: Configuring Workspace ONE Parameters



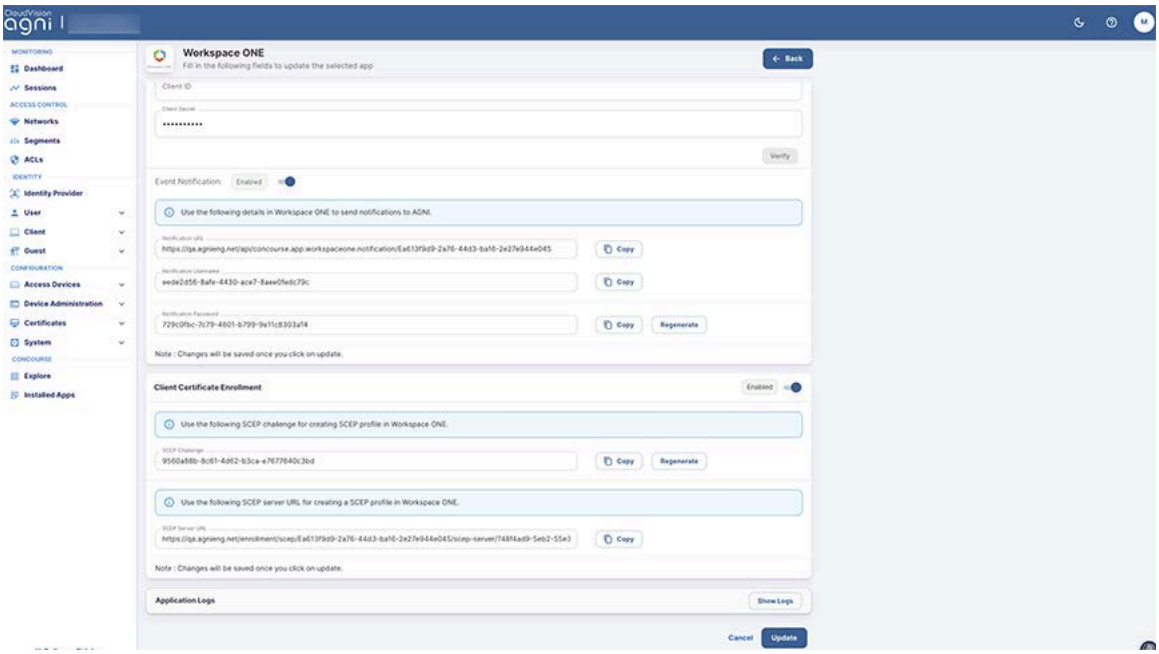
6. Within the Client Information Synchronization settings, enable **Event Notification**.

This enables AGNI to receive compliance status & Compromised status from Workspace ONE whenever the device details change.

> **Note:** Save the **Notification URL**, **Notification Username**, and **Notification Password**, which is configured on Workspace ONE Settings.

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

Figure 3-17: Configuring Workspace ONE Parameters



Chapter 4

Configuring Identity Providers

AGNI interacts with Identity Providers (IDPs) through OIDC and OAuth2.0 protocols. AGNI supports the following IDPs:

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

AGNI integration with IDPs requires:

- Authentication of user onboarding work flows to on-board the client devices through UPSK, EAP-TLS, and Captive Portal.
- Authentication of Admin login to the user interface.
- Authentication of Admin login to the UPSK client portal.
- Authentication of user login to the UPSK client portal.
- Authentication of 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.

4.1 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.

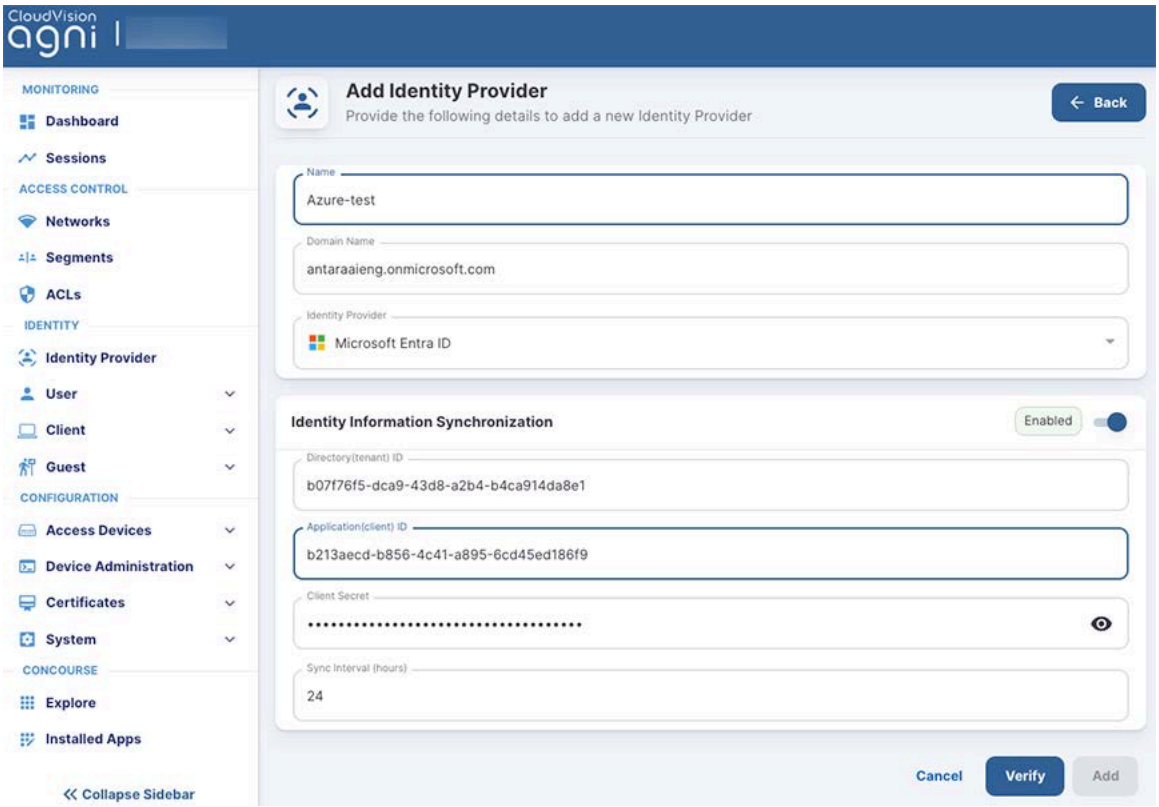
About authorization, you can skip the below steps, if you are not performing any user authorization or if you are not using any of the identity provider attributes in network policies.

If you provide user authorization, perform the following 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**.

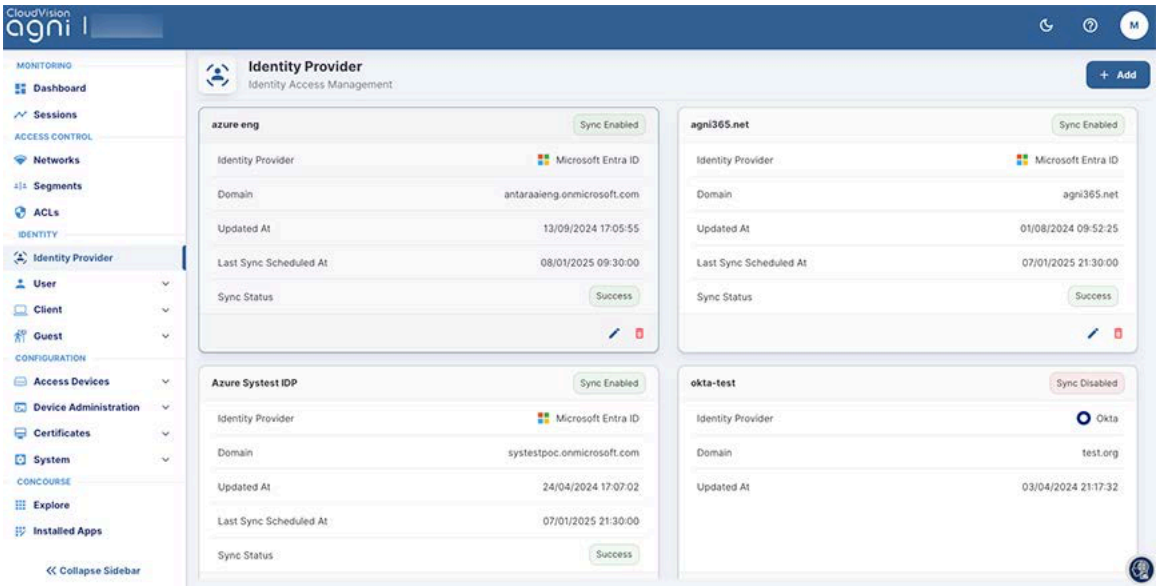
5. Provide the identity provider details.
   (Refer to Appendix section on how to configure the details in Microsoft Azure AD):
   a. **Directory (tenant) ID**
   b. **Application (client) ID**
   c. **Client Secret**
   d. **Sync Interval (hours)**
6. Click the **Verify** button. Once the operation is successful, the system fetches the list of groups from the IDP, which can be used in the policy creation.

Figure 4-1: Adding Identity Provider



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

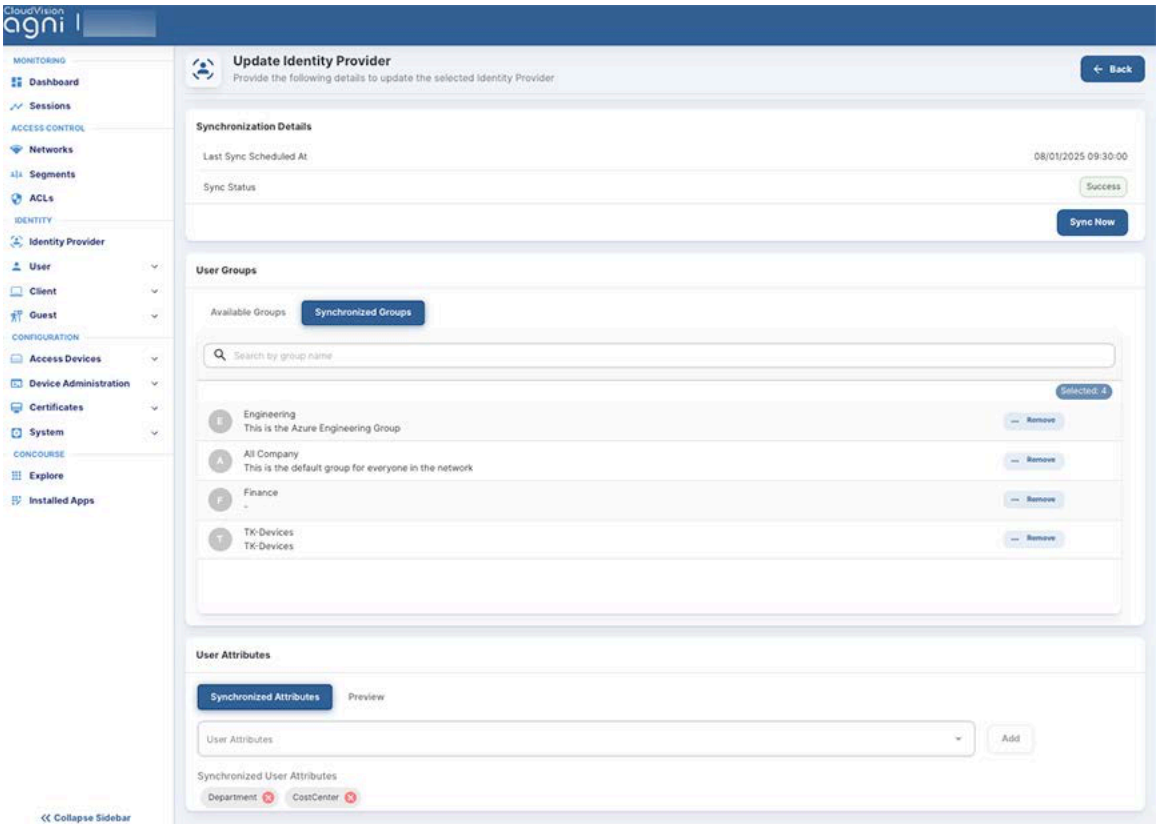
   Figure 4-2: Edit or Update Identity Provider



8. Select the groups from the **Available Groups** (see image below).

   The selected groups are visible in the **Synchronized Groups** tab and can be used in the network access policies.

   Figure 4-3: Identity Provider Available Groups

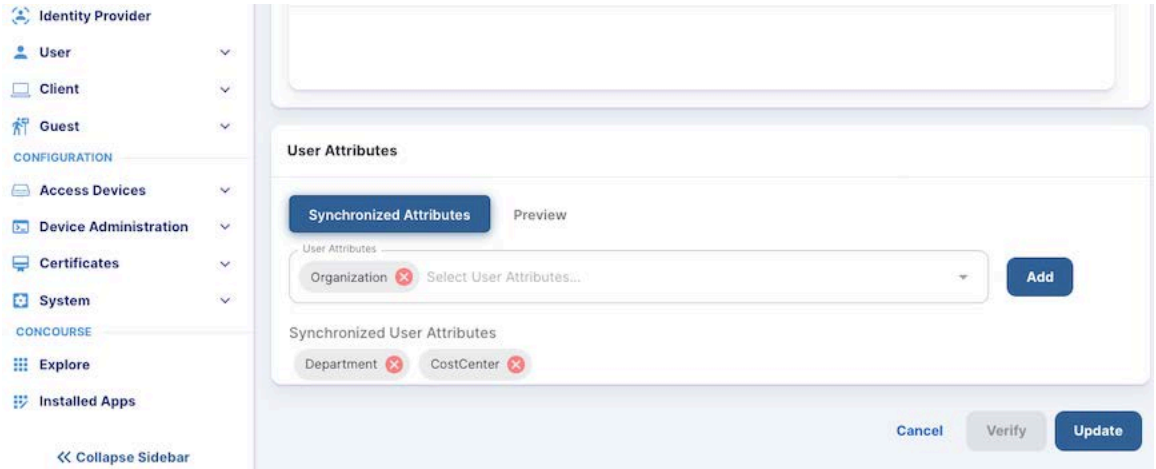


9. Click on the **Add** button to save the changes.

The details include:

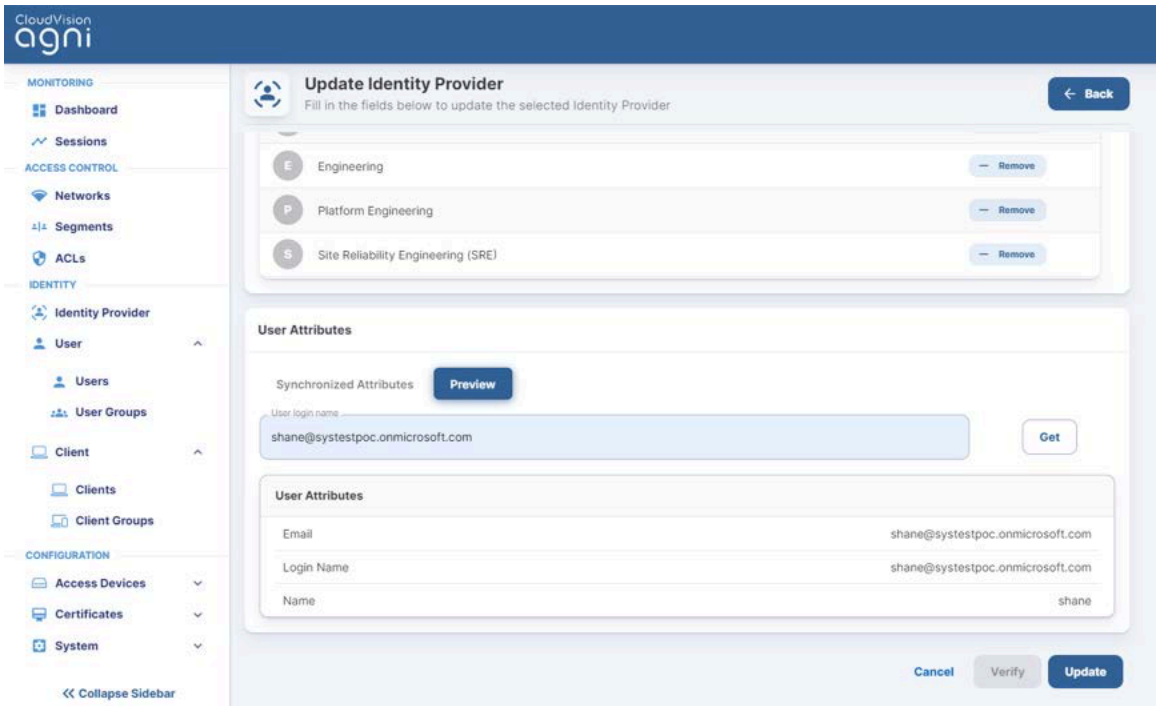
- **Sync Interval** - This parameter dictates when the system must synchronize user attributes from the IDP. To perform an on-demand synchronization, click on the **Sync now** button. Alternatively, the system synchronizes once every Sync Interval duration that was specified.
- **User Attributes** - 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 4-4: 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 4-5: Identity Provider and User Preview



4.2 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.

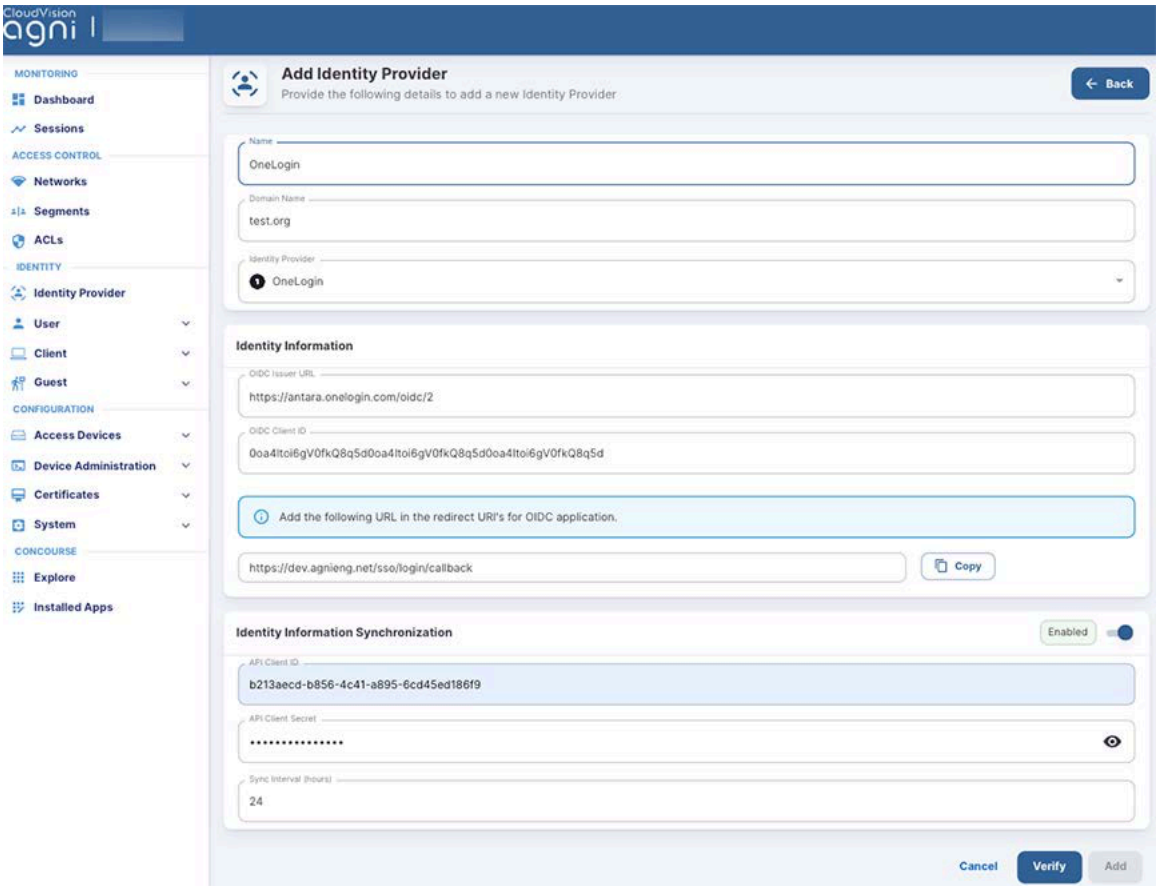
Authorization is performed by setting up API access under the Developers section in OneLogin administration. Create new API credentials in OneLogin for AGNI that have read permission for user fields, roles, and groups. Once set up, save the Client ID and Client Secret for later use.

Enter these values in AGNI by adding a new Identity Provider for OneLogin, performing the following steps:

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

b. **OIDC Client ID**

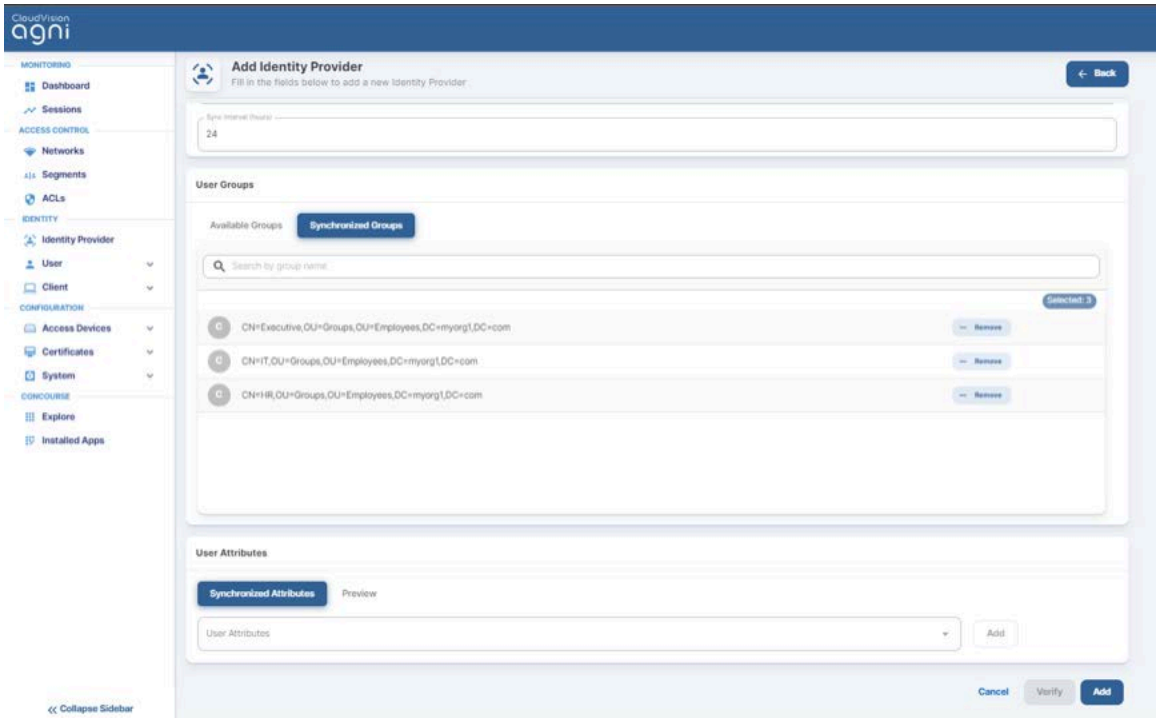
Figure 4-6: OneLogin and Identity Provider



5. Enable **Identity information Synchronization**.
6. Provide the **Identity Information Synchronization** details.
   (Refer to Appendix section on how to configure the details in OneLogin or the vendor documentation).
   a. **API Client ID**
   b. **API Client Secret**
7. 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.
8. 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 4-7: OneLogin Identity Provider Synchronization



4.3 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.

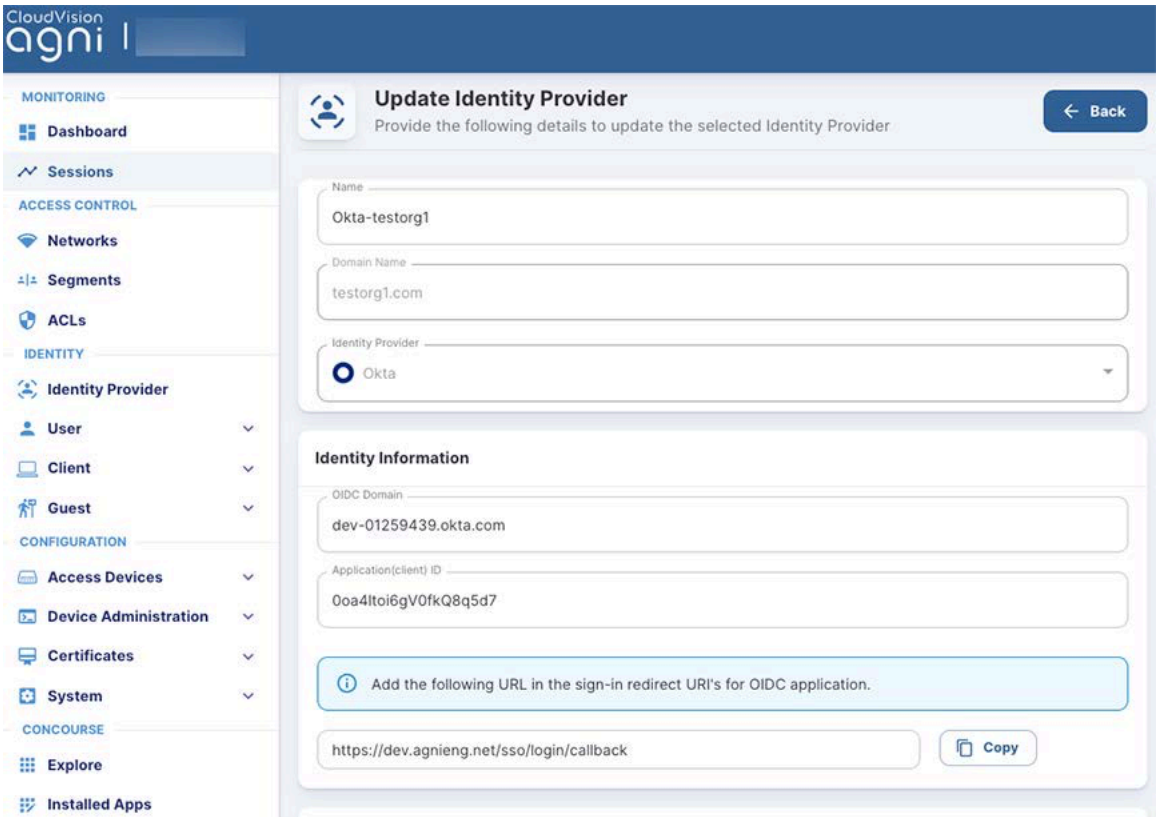
Authorization is performed through setting up API access under the Security section in Okta administration. Create a new **API Token** in Okta for AGNI.

Enter these values in AGNI by adding a new Identity Provider for Okta, performing the following steps:

1. Navigate to **Identity** > **Identity Provider**.
2. **Edit Identity Provider** (or **Add a new identity provider**).
3. Provide the details for:
   a. **Name** - Name of the identity provider.
   b. **Domain Name** - Domain name of the organization.
4. Provide the details for **Identity Information**.
   The details are used for authentication and is described in the authentication section above.
   a. **OIDC Domain**

b. **Application (client) Client ID**

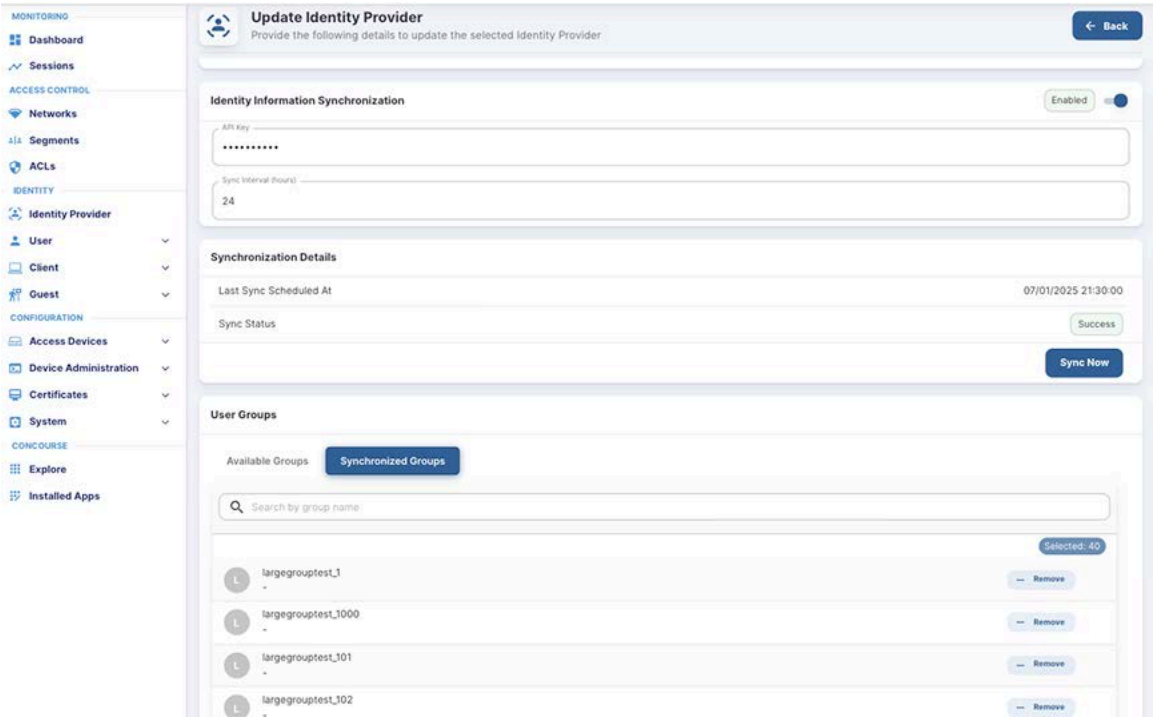
Figure 4-8: Okta Identity Provider Configuration



5. Enable **Identity information Synchronization**.
6. Provide the **Identity Information Synchronization** details.
   (Refer to the Appendix section on how to configure the details in Okta or the vendor documentation).
   a. **API Key**
7. 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.
8. 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 4-9: Okta Identity Provider Synchronization



4.4 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, performing the following steps:

1. Navigate to **Identity** > **Identity Provider**.
2. **Edit Identity Provider** (or **Add a new identity provider**).
3. Provide the details for:
   a. **Name** - Name of the identity provider.
   b. **Domain Name** - Domain name of the organization.
4. Provide the details for **Identity Information**.
5. Enable **Identity Information Synchronization**.
6. Provide the **Identity Information Synchronization** details.
   a. **Customer ID**
   b. **Account Email**

c. **Upload Service Account** Credentials.

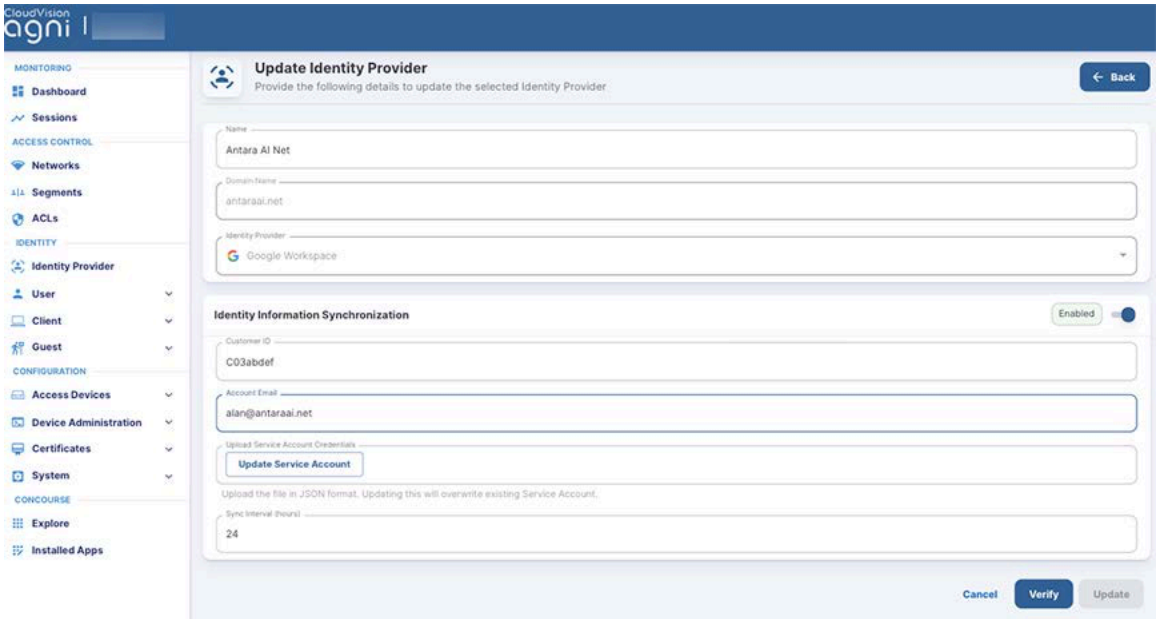
7. Click the **Verify** button.

   Once the operation is successful, you can add the group information as it appears in Google Workspace and use it in the authorization policies.

8. 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).

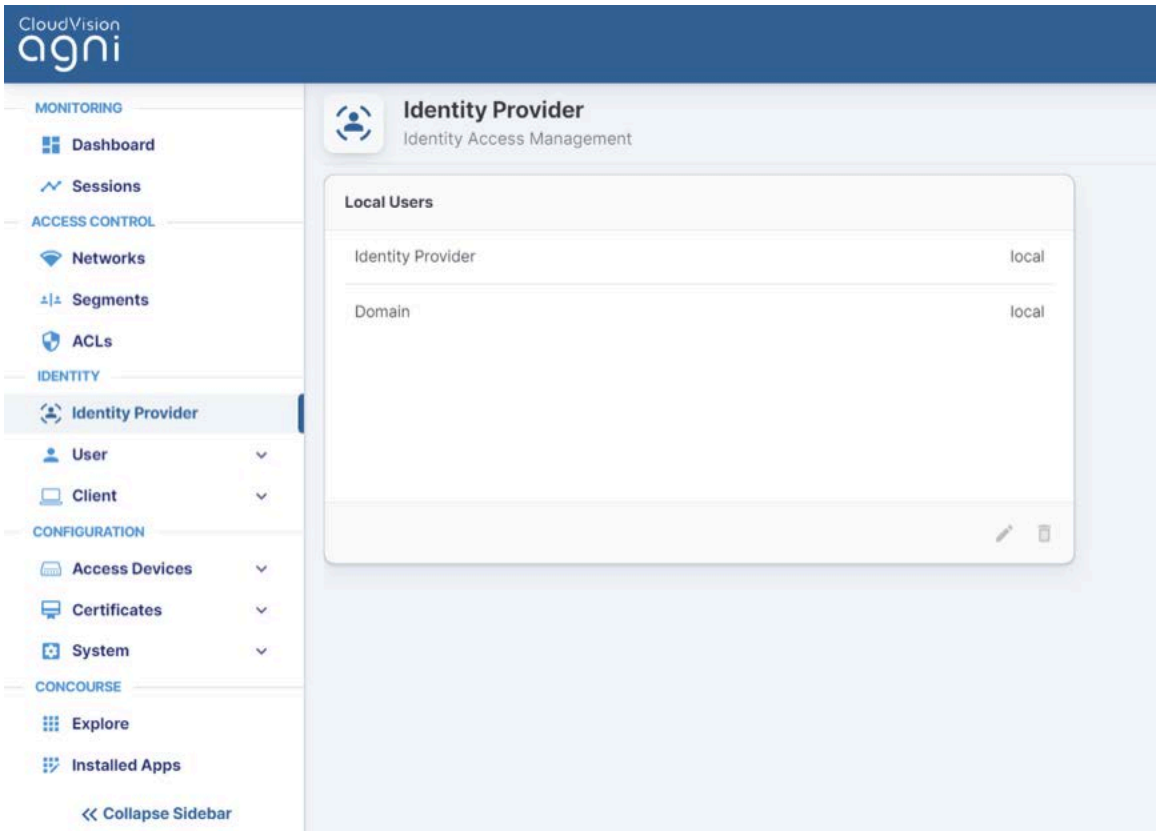
Figure 4-10: Google Workspace



4.5 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 4-11: Local IDP Configurations



Chapter 5

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.

5.1 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

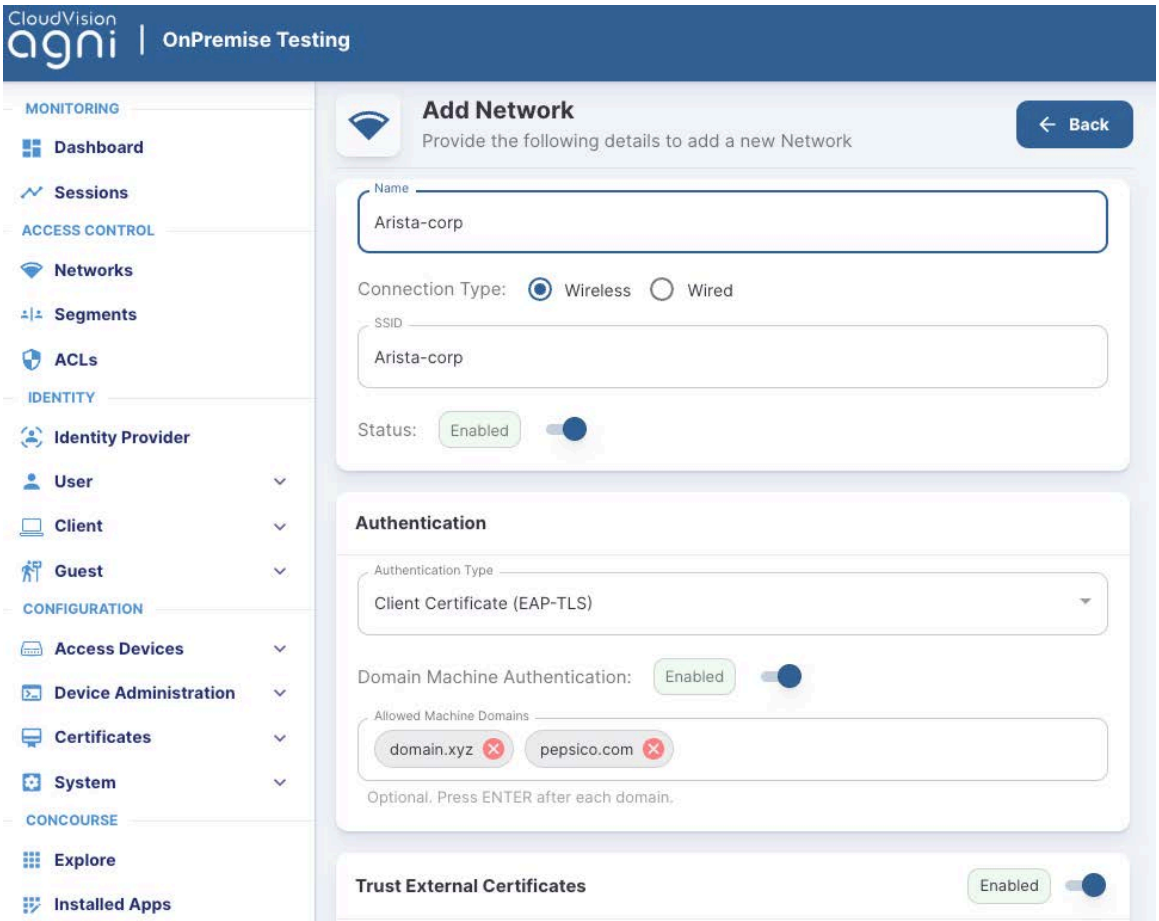
- Wireless SSID should be configured on the APs to perform 802.1X authentication.
- Clients are onboarded with credentials and configured to perform 802.1X authentication either using native PKI or external PKI.
- For external PKIs, the PKI **root** and **issuer certificates** are imported into AGNI

5.1.1 Configuration Steps

To configure Networks, perform the following steps:

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

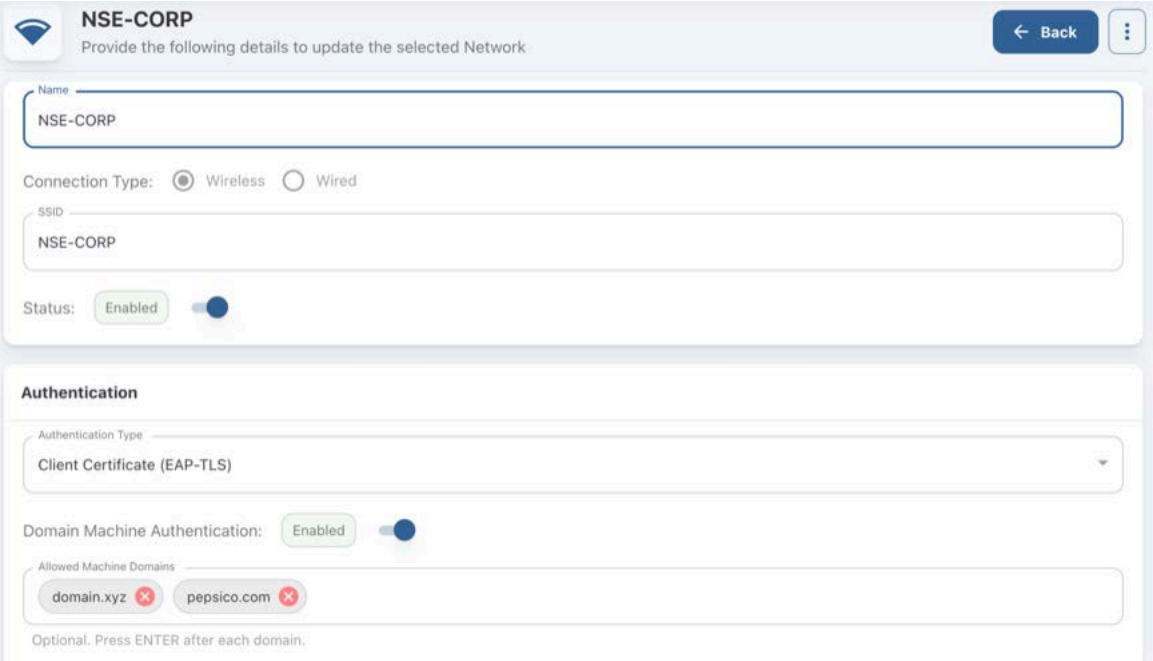
   Figure 5-1: Wireless EAP-TLS Network



2. Enter the network **Name** and choose **Connection Type** as **Wireless**.
3. Enter the **SSID** name. Ensure that the name matches the SSID configured in wireless access points.
4. Set the **Status** value.
   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).

Figure 5-2: Domain Machine Authentication



7. **Trusted External Certificates**
   a. If external PKI is being used and if you require AGNI to honor the external certificates, enable the setting with an option to check against **CRL** and **OCSP URLs** for certificate revocations.
   b. The setting assumes external PKI root and issuer certificates are imported into AGNI.
   c. **User Identity Binding**
      1. **Required** - When set, the certificate has a valid query-able user identity for request authorizations.
      2. **Optional** - When set, the certificate contains any identity that is optionally bound or not bound to the user. For example, this option can be set to honor appliance authentication where the certificates are not bound to any user but set to machine identity.
8. **Onboarding**
   a. **Enable** this setting if using AGNI PKI.
   b. **Enable Allow Email Code Login for IDP User**.
      This configuration is applicable for UPSK and EAP-TLS network authorization types. Users onboarding the device to AGNI through Self-Service portal have the option to login through Email Code (OTP). AGNI Self-Service Portal onboards the user after OTP verification (sent to your registered email account). Optionally, if IDP synchronization is enabled, then the user attributes and group information gets updated. For details, see the Authenticating Users with Email Codes (as against IDP) section.
   c. **Allow Local User Self Registration**:
      1. **Disabled** - Disallows local users to self-register into the system as part of the user onboarding process.
      2. **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.

3. **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 Wi-Fi configuration of your AP. Clients are redirected to this URL during the onboarding process.

Figure 5-3: Onboarding

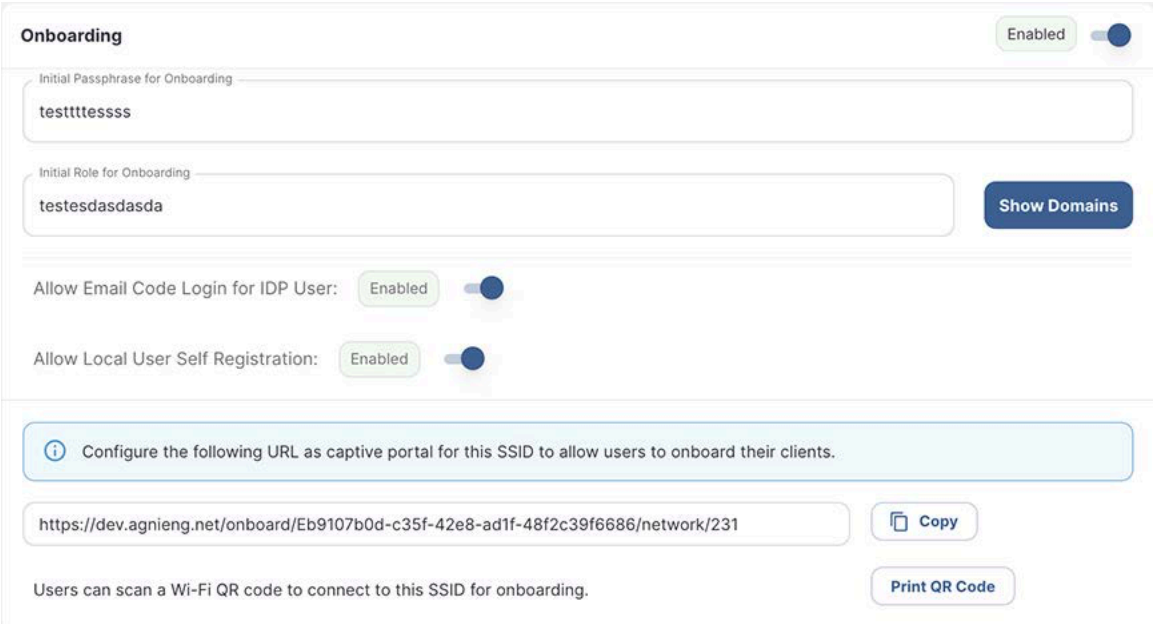


Figure 5-4: Wireless EAP-TLS Network User Onboarding

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.

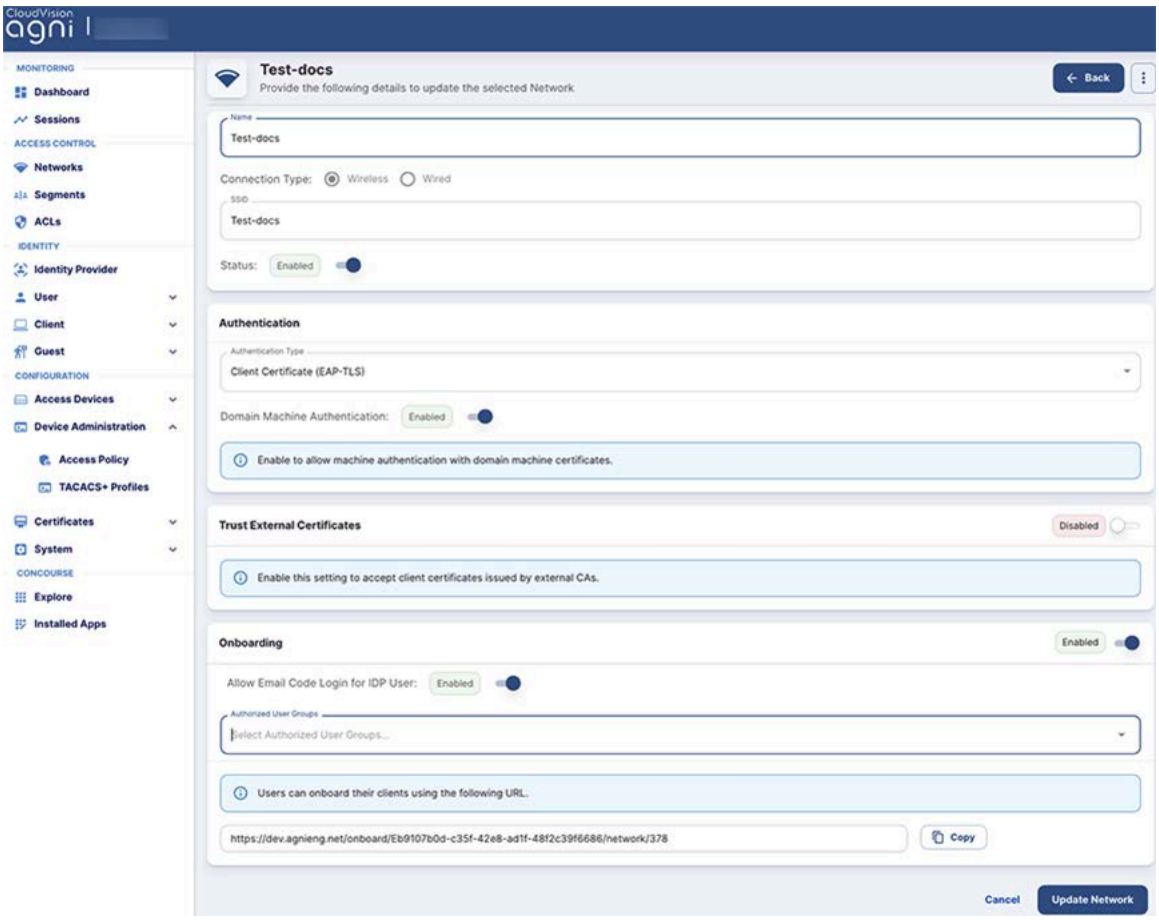
5.1.2 Authenticating Users with Email Codes (as against IDP)

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, perform the following steps:

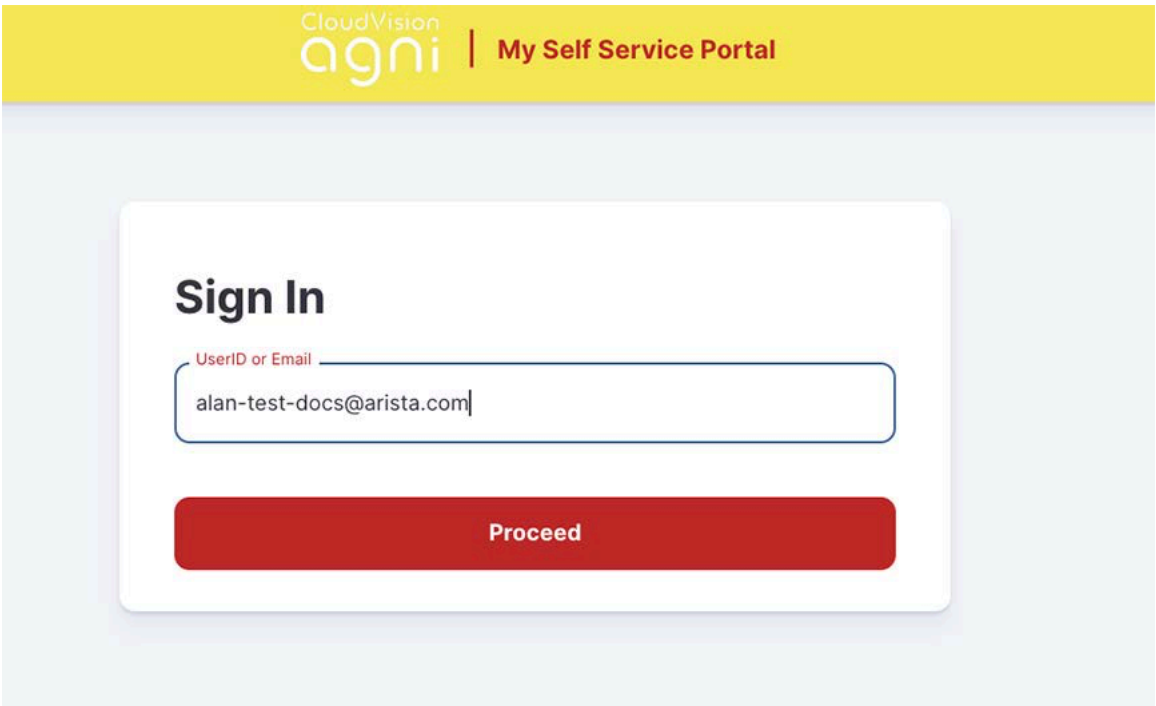
1. Navigate to **Access Control** > **Networks** and select your network.
2. Enable the **Allow Email Code Login for IDP Users** in the Onboarding section.
3. Click the **Update Network** to enable the feature.

Figure 5-5: Updating the Network Details



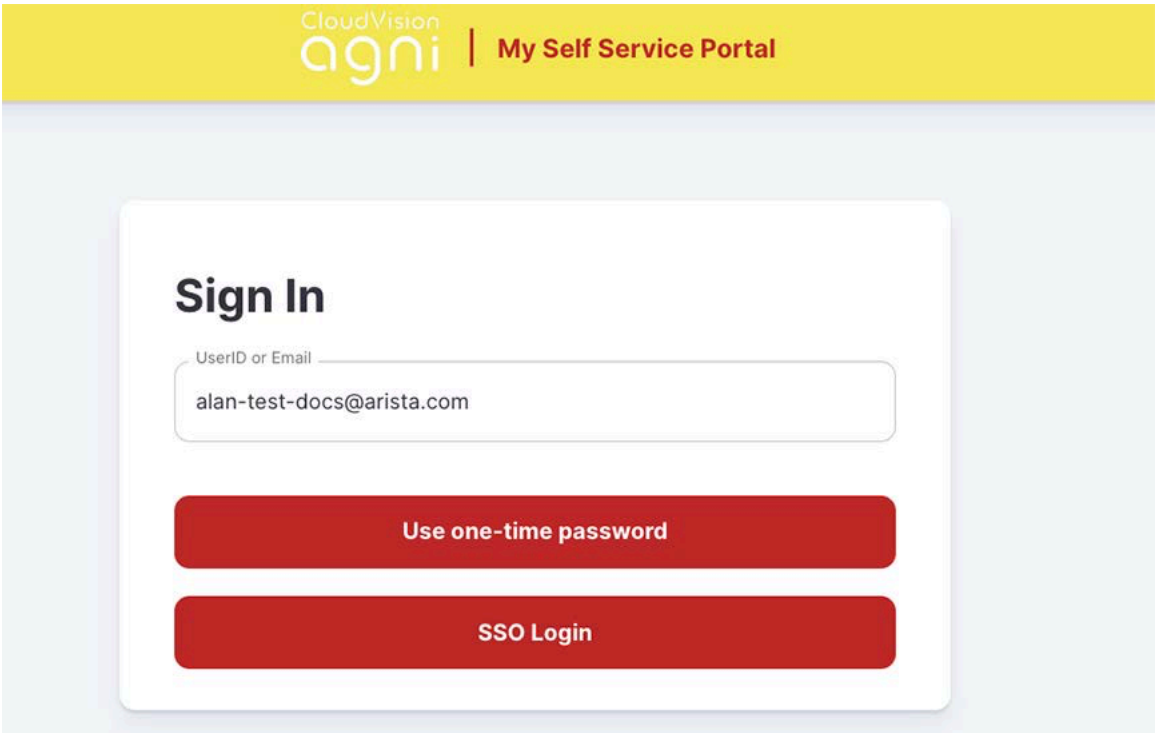
4. Once enabled, **Copy** the onboarding URL and open it from the computer you want to onboard and log in to.

   Figure 5-6: Self Service Portal Login



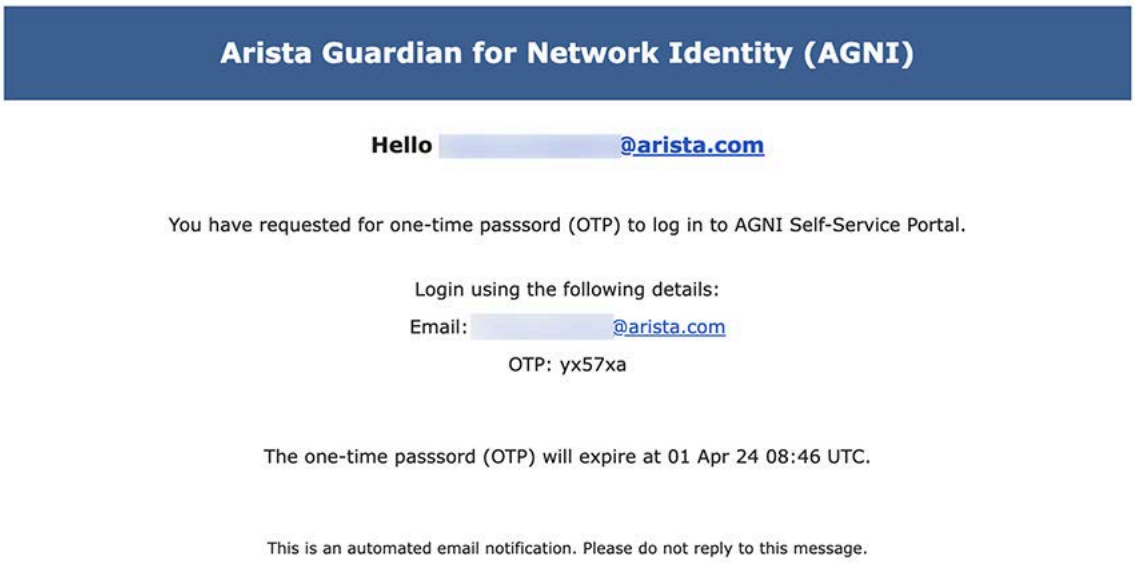
5. Click the **Proceed** button and click the **Use one-time password** option.

   Figure 5-7: Use One-Time Password Option



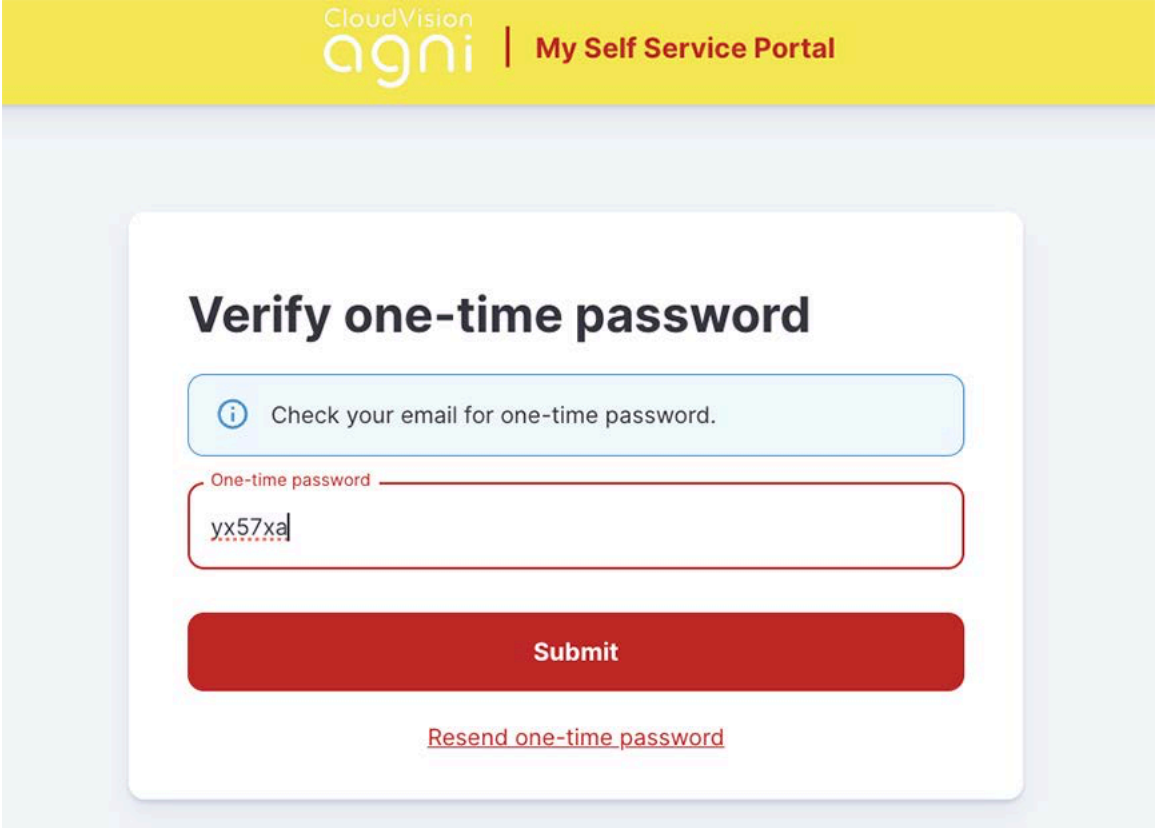
6. Check your registered email for OTP details:

Figure 5-8: AGNI Login



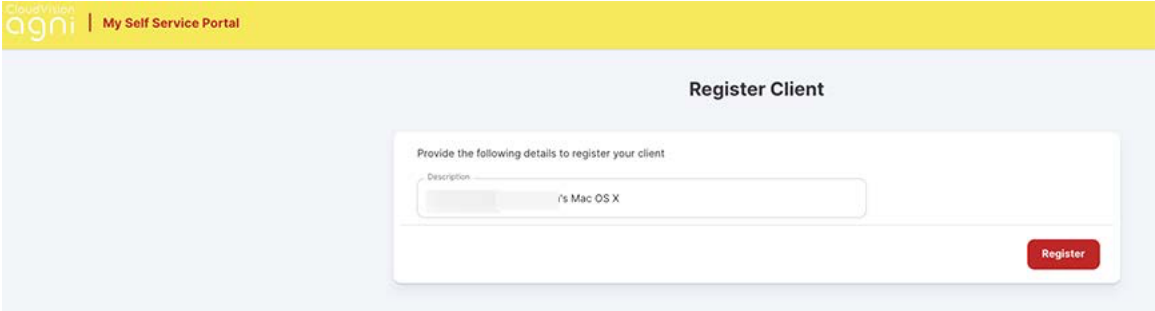
7. Copy the OTP, paste that for the authentication against IDP, and click the **Submit** button.

Figure 5-9: Verify OTP



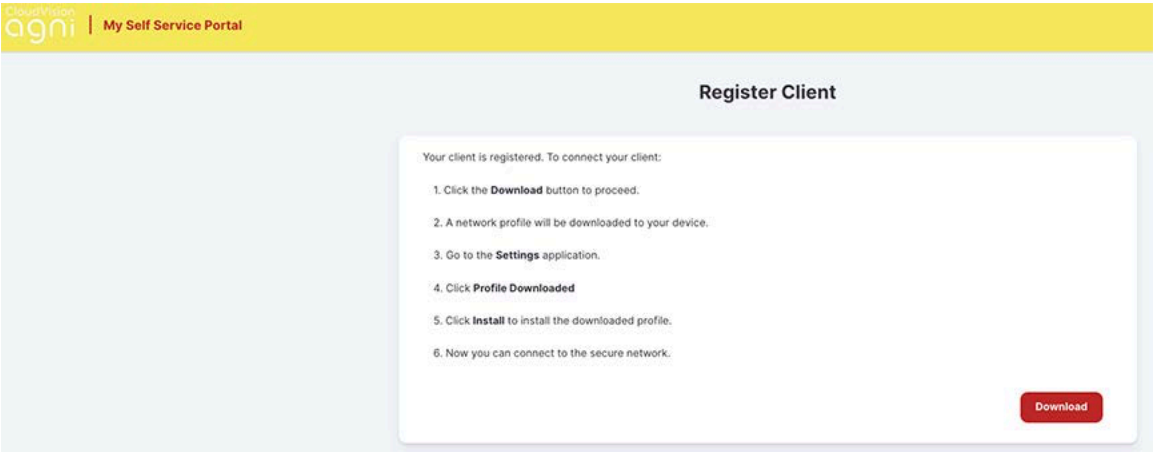
8. After successfully logging into the Self-Service portal, click the **Register** button to complete the onboarding process.

Figure 5-10: Register Client



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.

Figure 5-11: Download & Connect to AGNI Network



5.1.3 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 Wi-Fi 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:

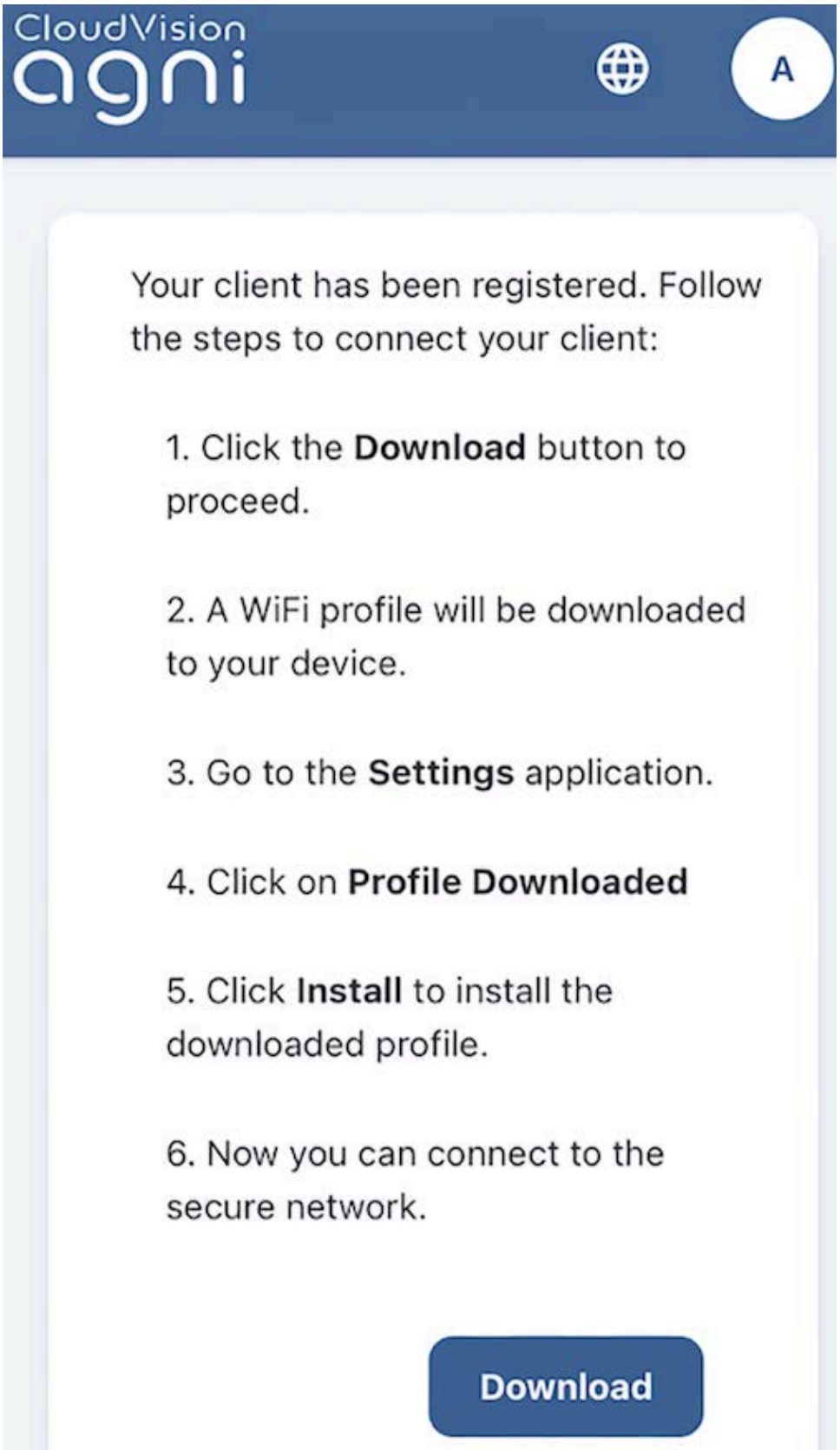
- iPhone
- MacBook
- Android
- Windows
- Chromebook

5.1.3.1 iPhone Configuration

To configure AGNI on an iPhone, perform the following steps:

1. Click the **Register** button to redirect to the page to download the Wireless configuration profile.

Figure 5-12: Download Wireless Profile



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

Figure 5-13: Profile Downloaded

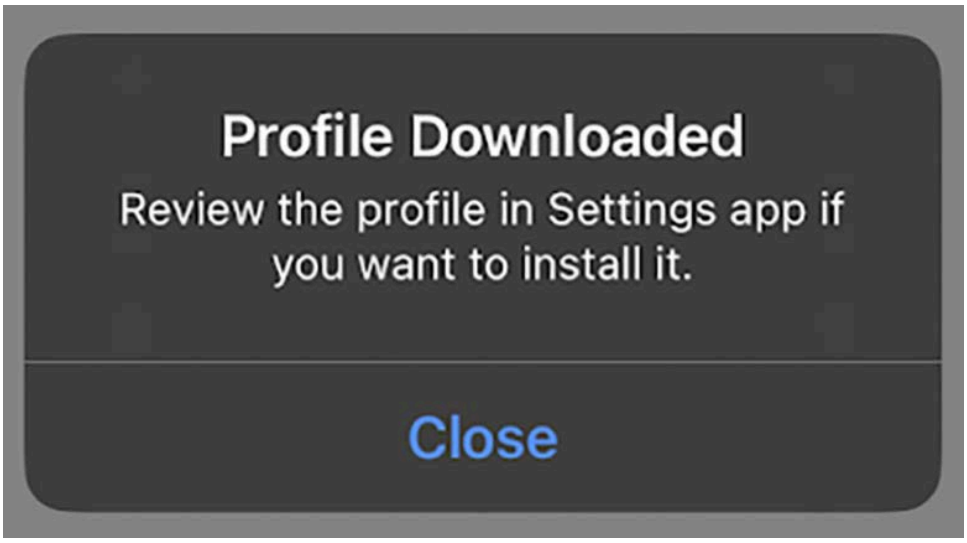


Figure 5-14: Profile Downloaded

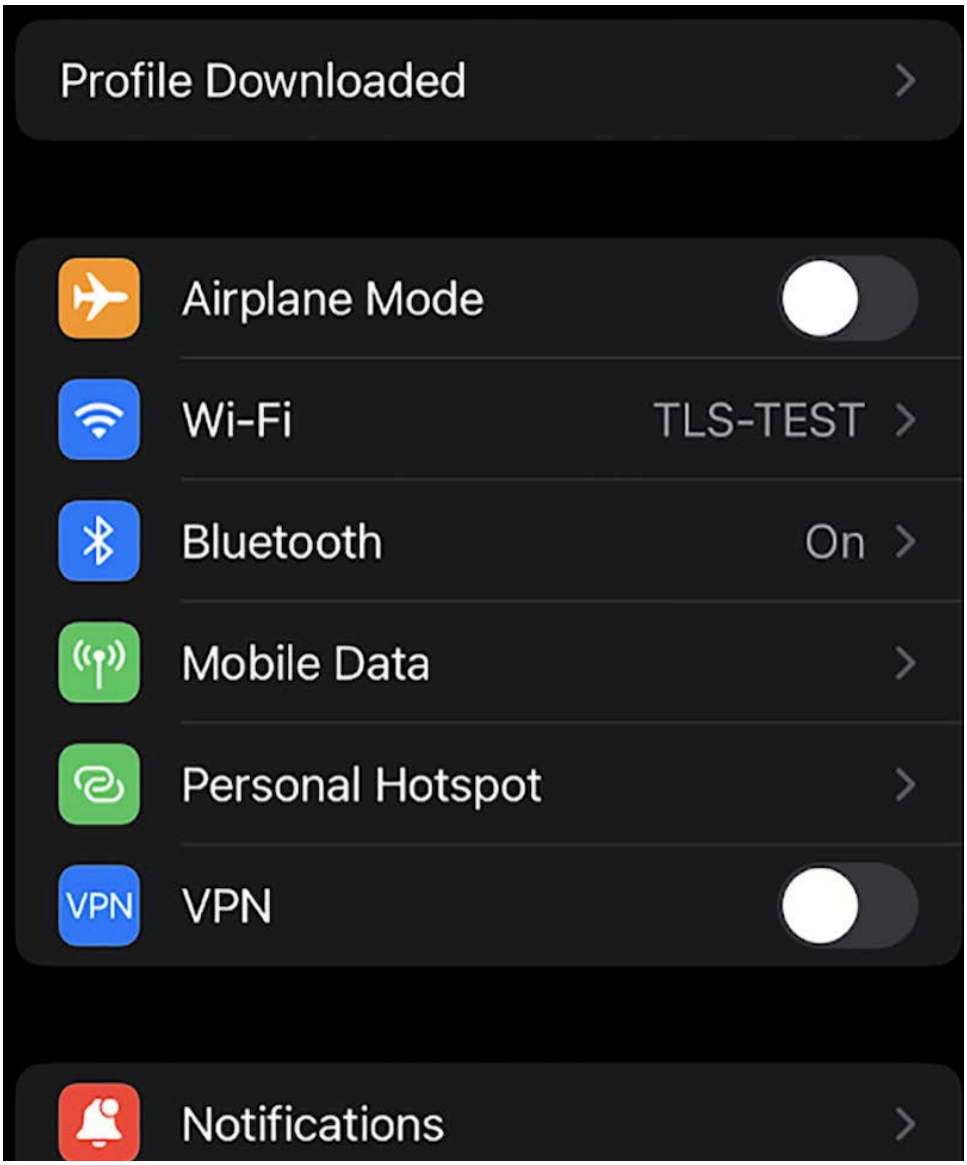
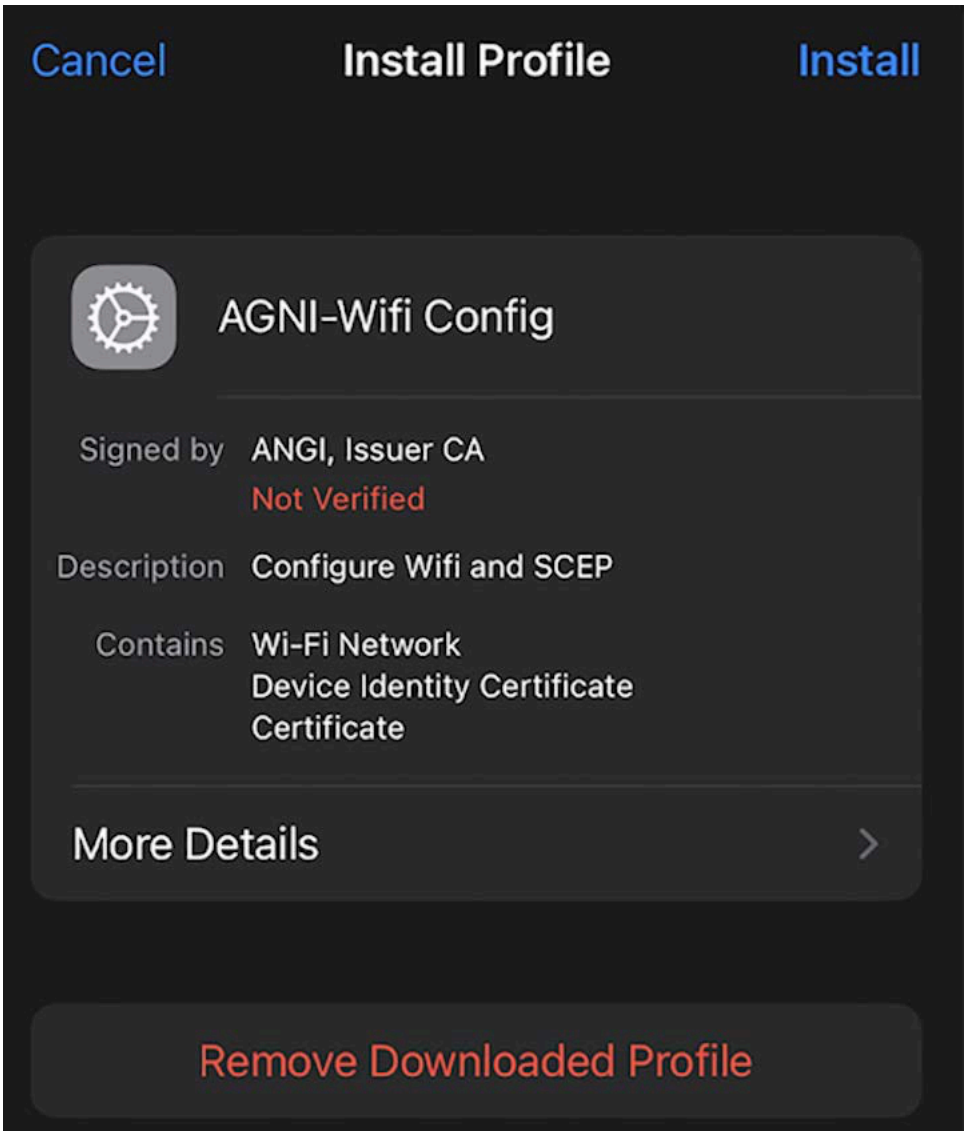


Figure 5-15: Profile Installed



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

5.1.3.2 MacBook Configuration

The configuration process on the MacBook is similar to the iPhone. To configure, perform the following steps:

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.

Figure 5-16: AGNI-Wifi Config

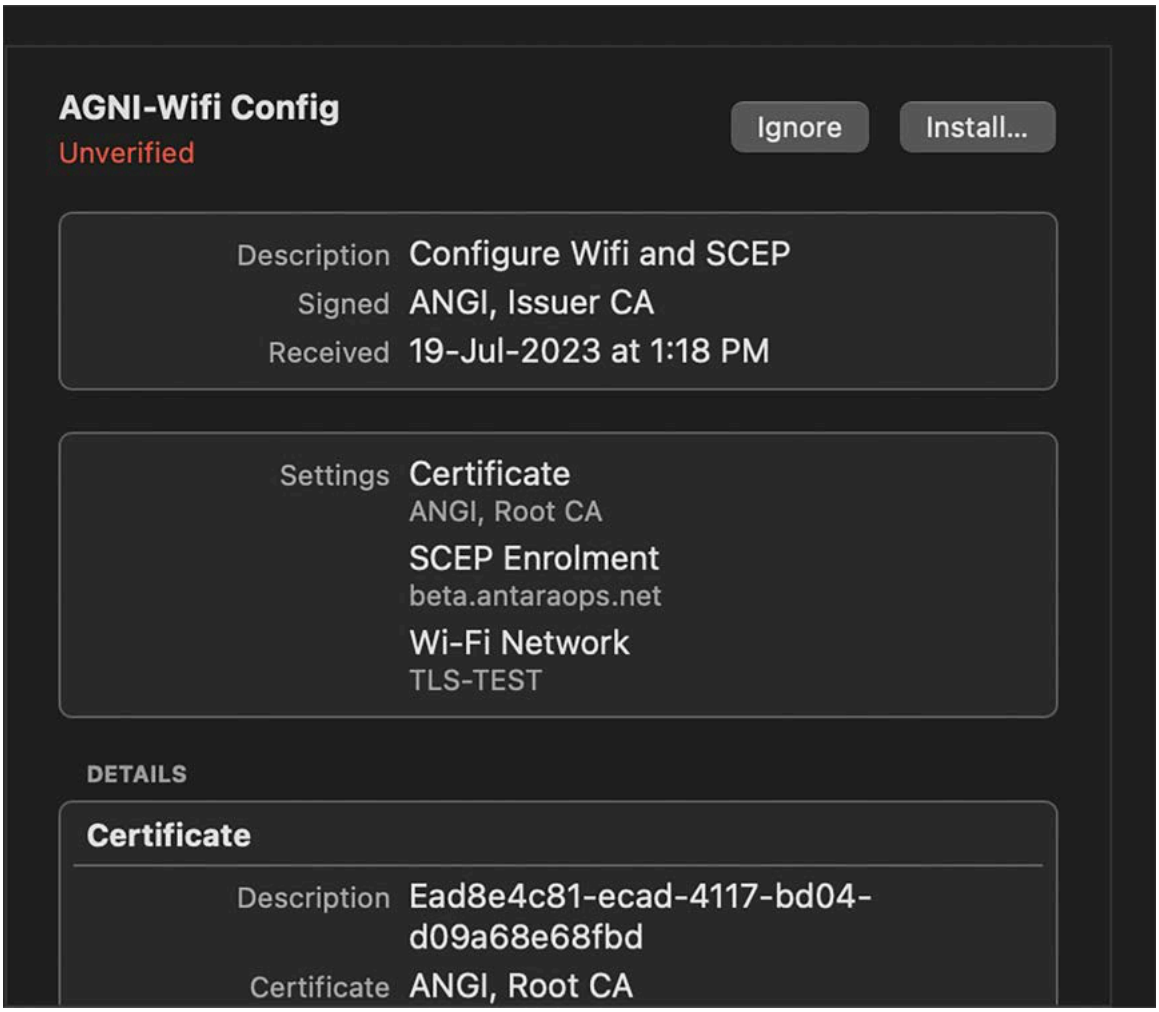
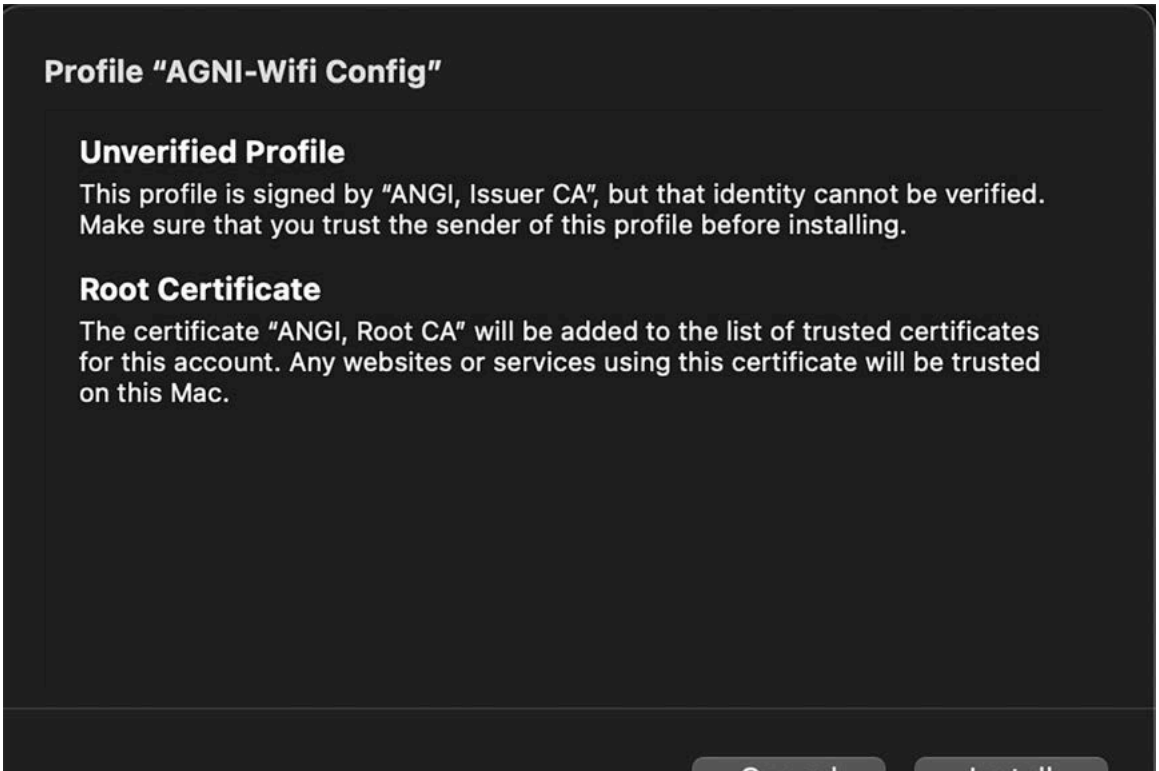


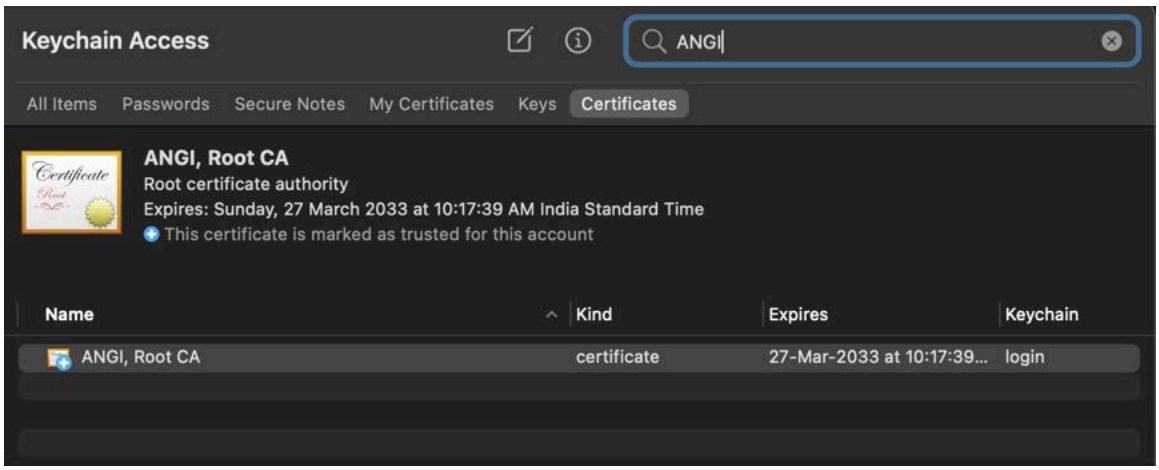
Figure 5-17: Unverified Profile



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

For further verification on the Root CA installation, use the **Keychain Access** application.

Figure 5-19: Keychain Verification

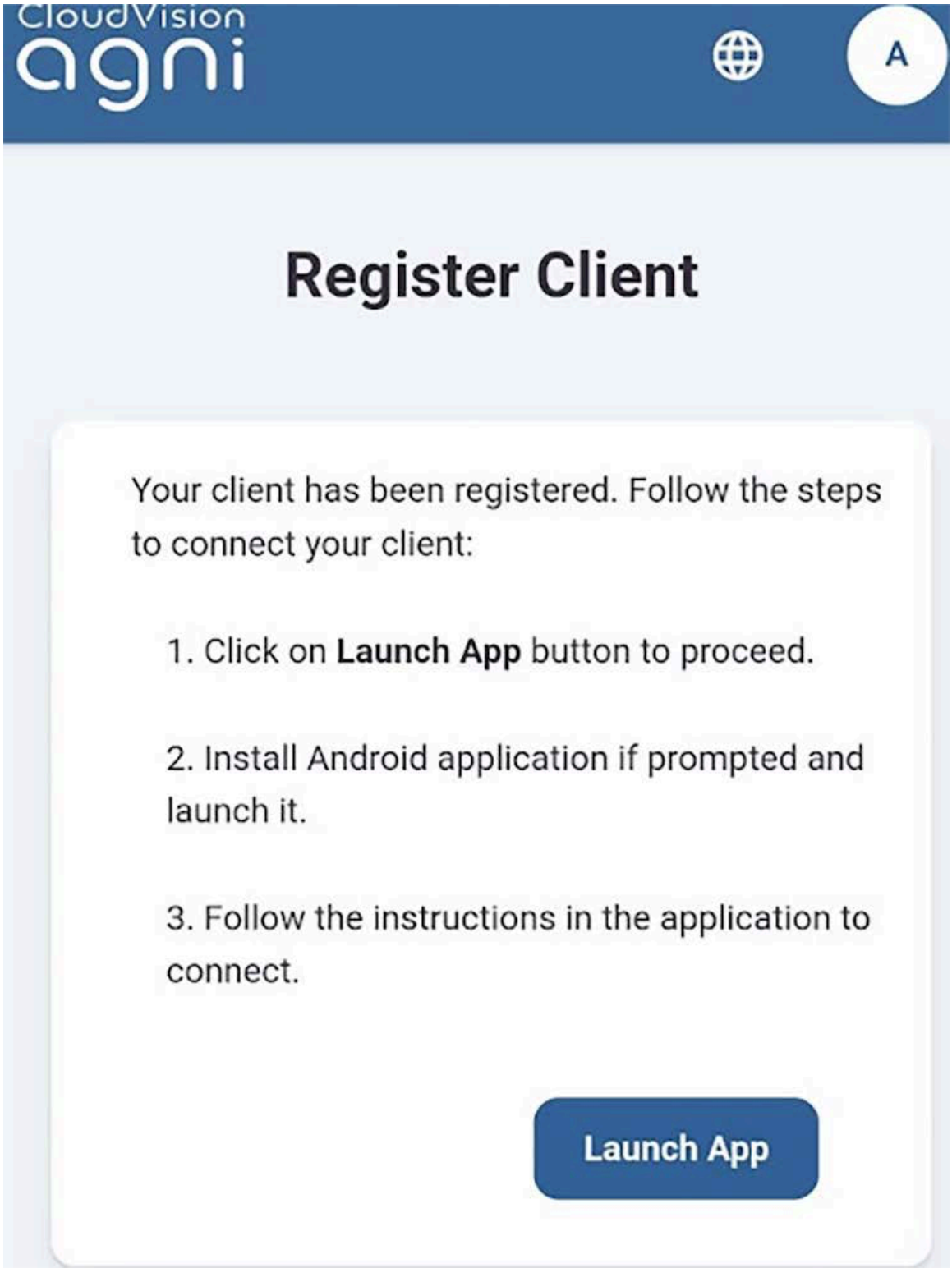


5.1.3.3 Android Configuration

For android devices, the wireless configuration profile is pushed via the AGNI Onboard application, which is available on Google Play Store.

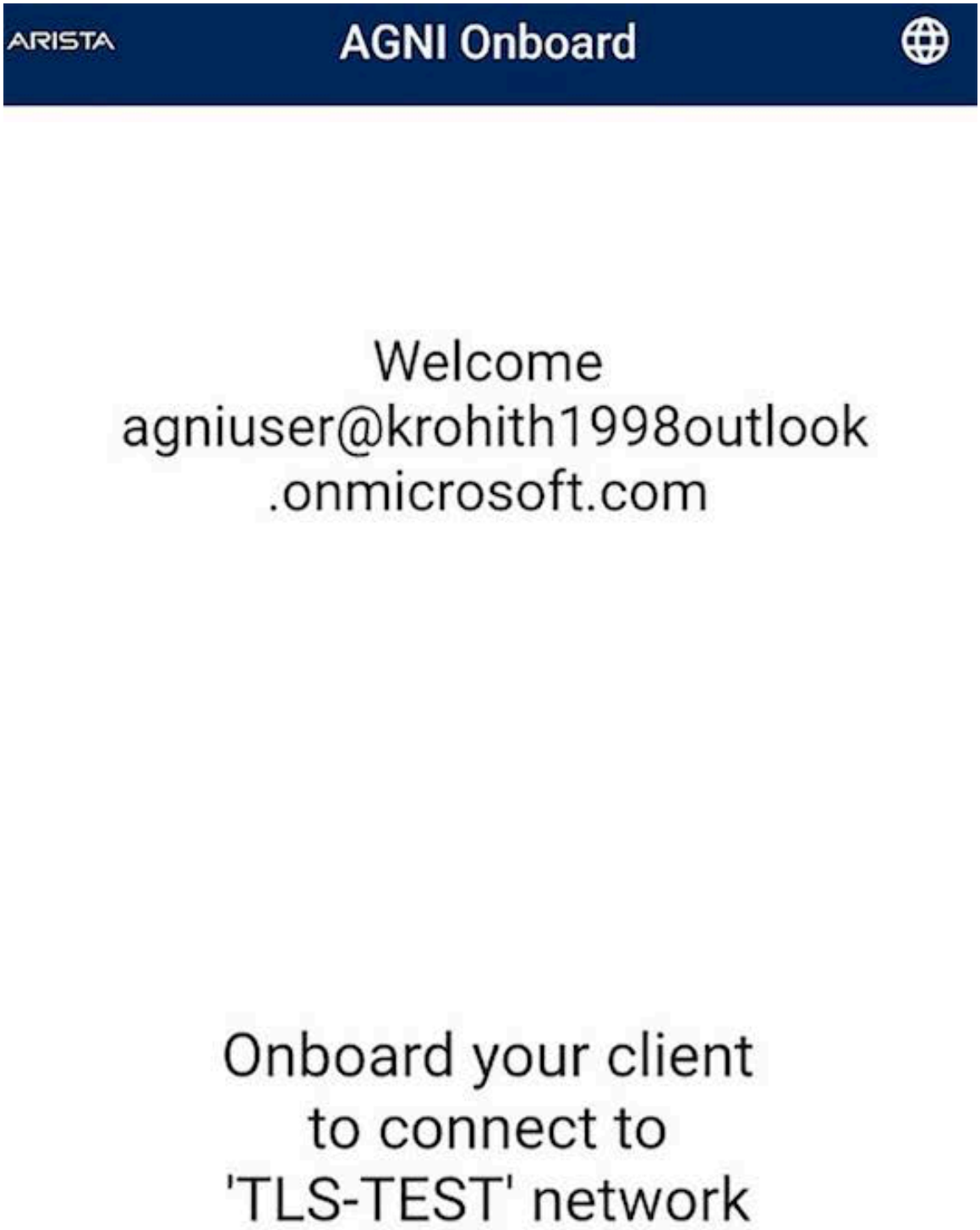
After client registers, the user is prompted to launch the application:

Figure 5-20: Register Client



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.

Figure 5-21: AGNI Onboard



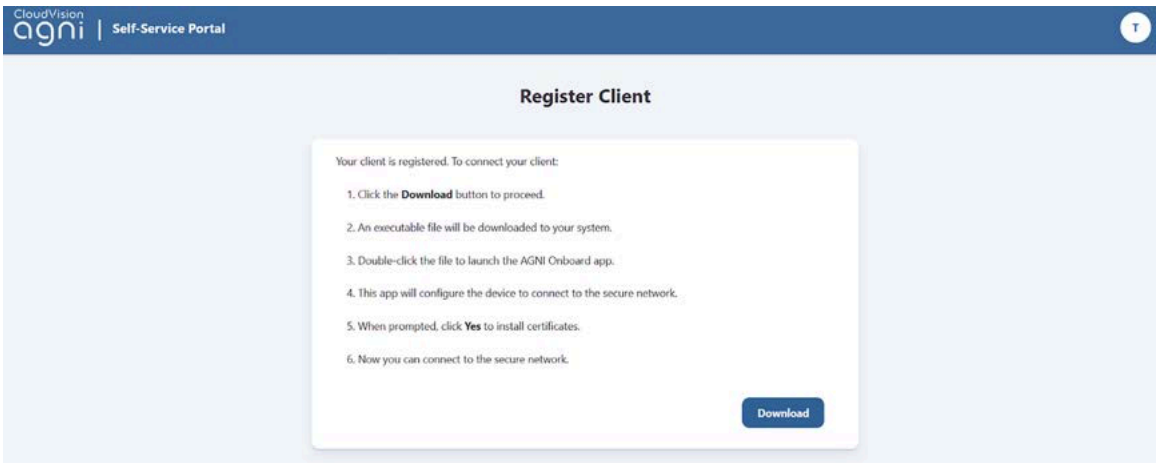
After the application is allowed to suggest networks, the device automatically connects to the network in range.

5.1.3.4 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.

1. Download the `.exe` file once the client is registered on the self service portal.

   Figure 5-24: Register Client



2. After running the `.exe` file as an administrator, click the **Start** button to install the profile.

During the profile installation, the AGNI Root CA certificate is installed in the device's trusted certificate store.

Figure 5-25: Onboard Client

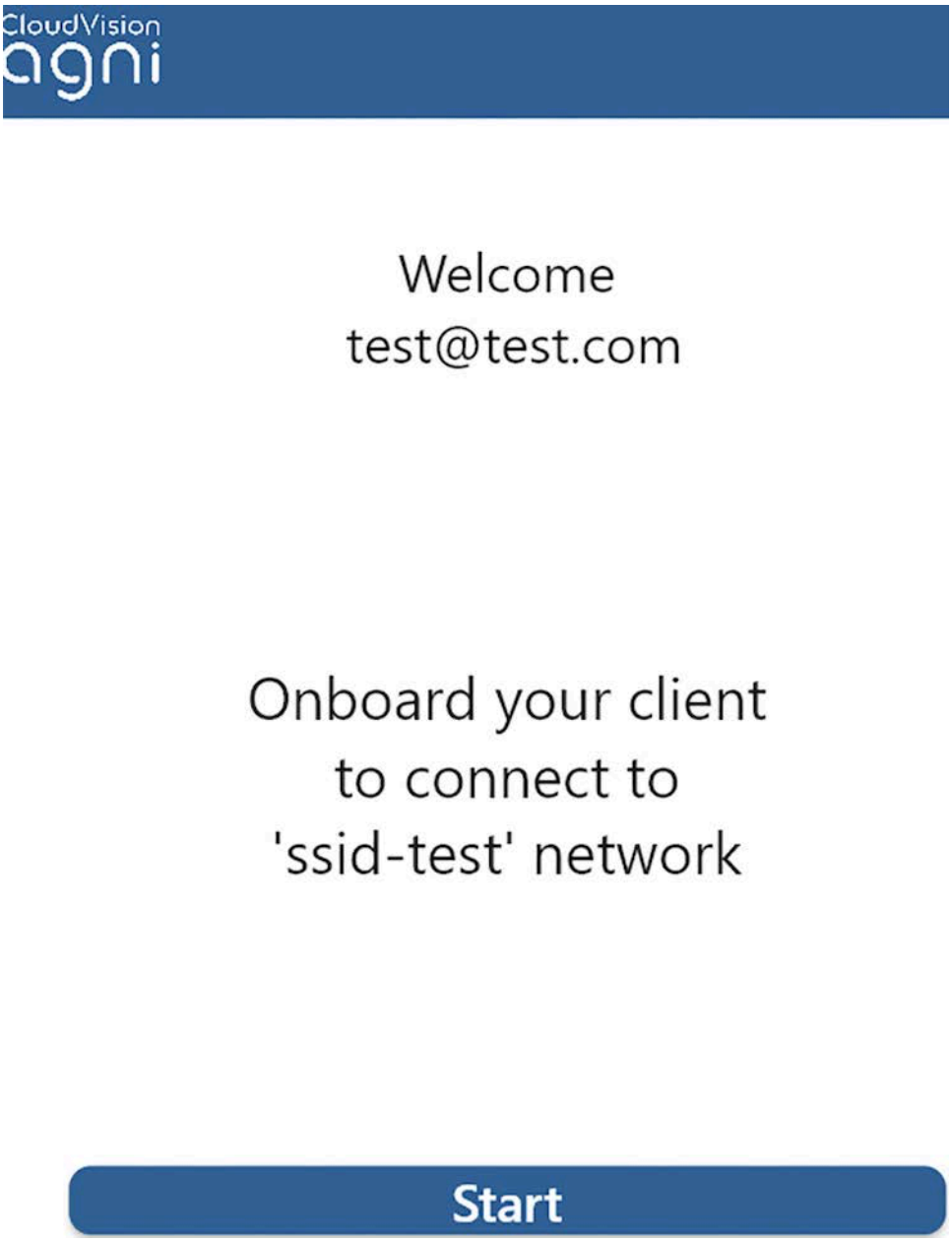
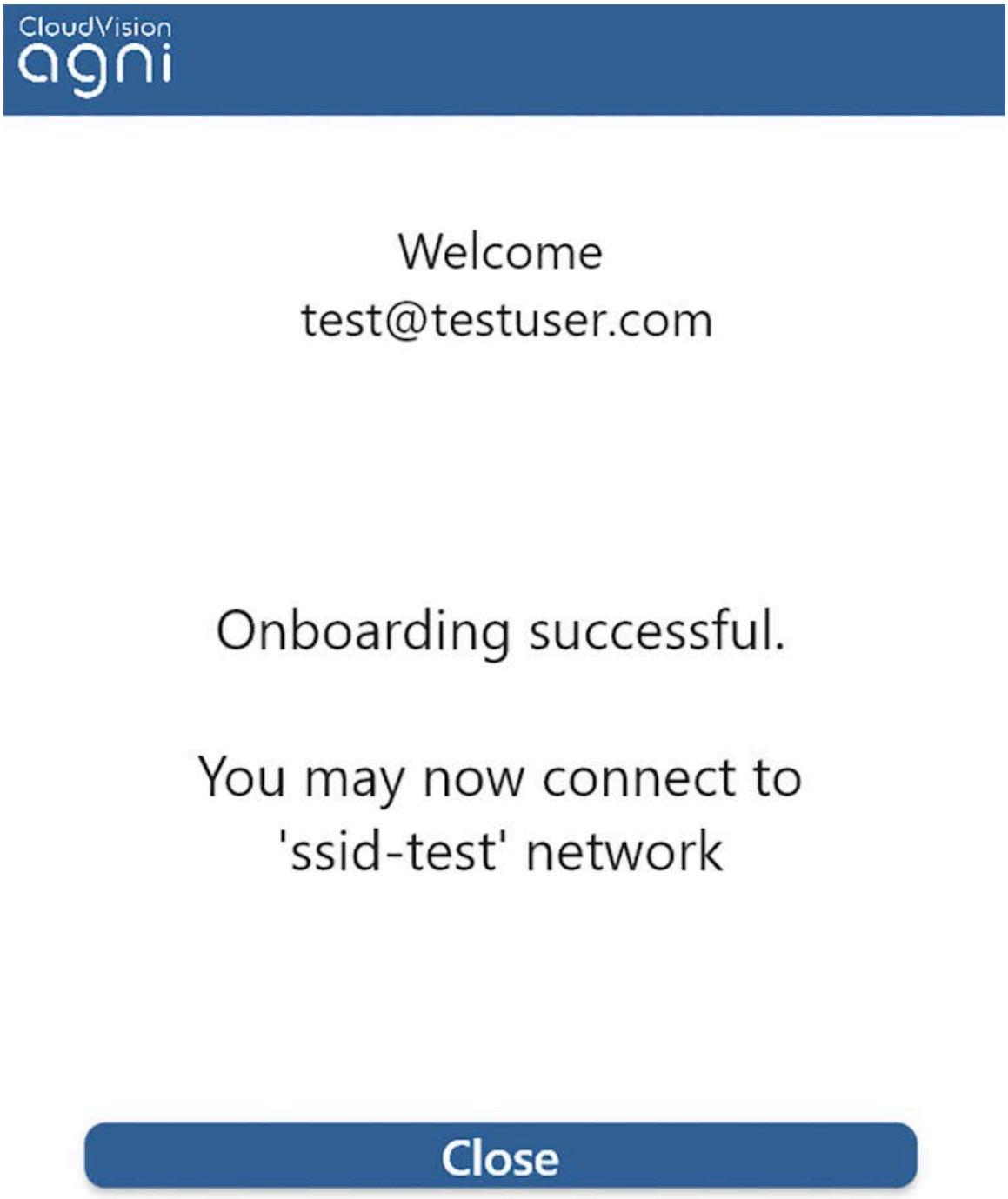


Figure 5-26: Security Warning

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

Figure 5-27: Onboarding Success



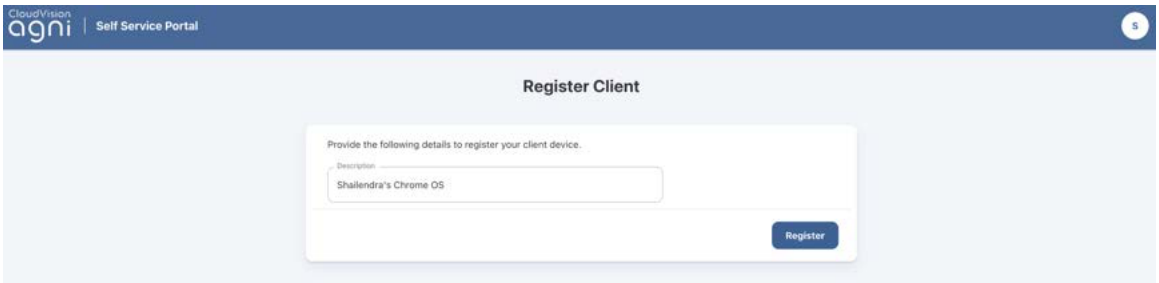
5.1.3.5 Chromebook Configuration

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

To configure Chromebook, perform the following steps:

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

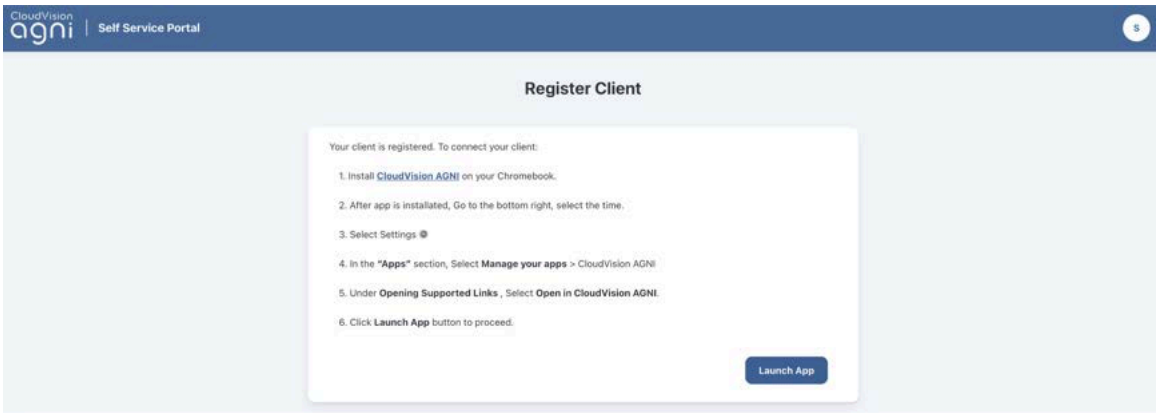
   Figure 5-28: Register Client



3. Click the **Register** button.

   After successful login, the user receives a set of instructions to download the Cloud Vision AGNI application. Follow the instructions.

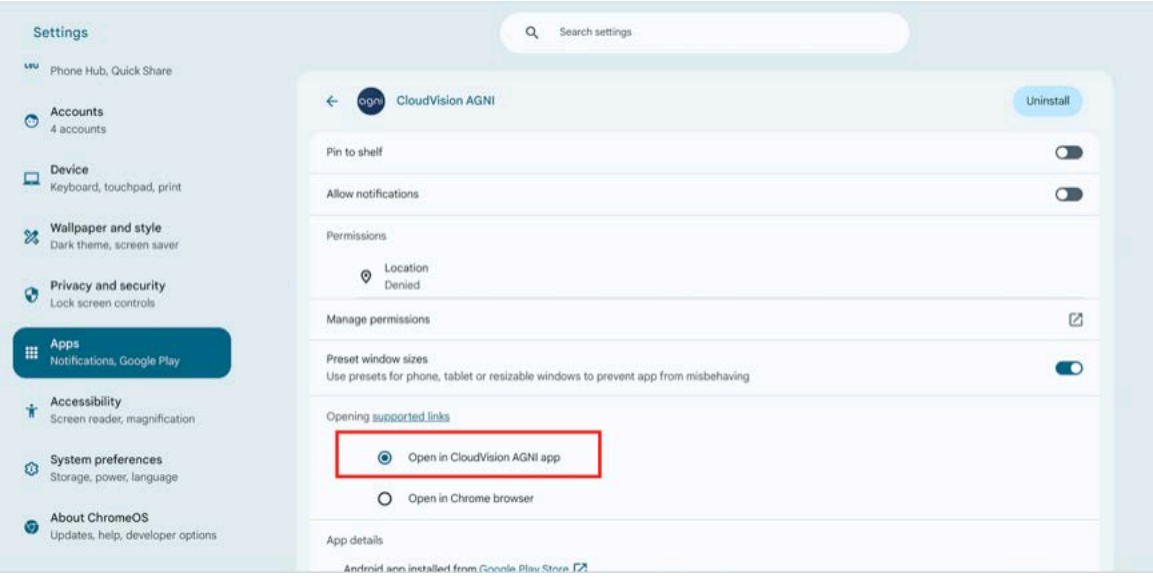
   Figure 5-29: Register Client Steps



4. Download the AGNI Onboarding application from the play store.
5. Click the **Settings** from the bottom right options and navigate to **Apps** > **Manage Apps**.
6. Select the **AGNI** application and open the settings.

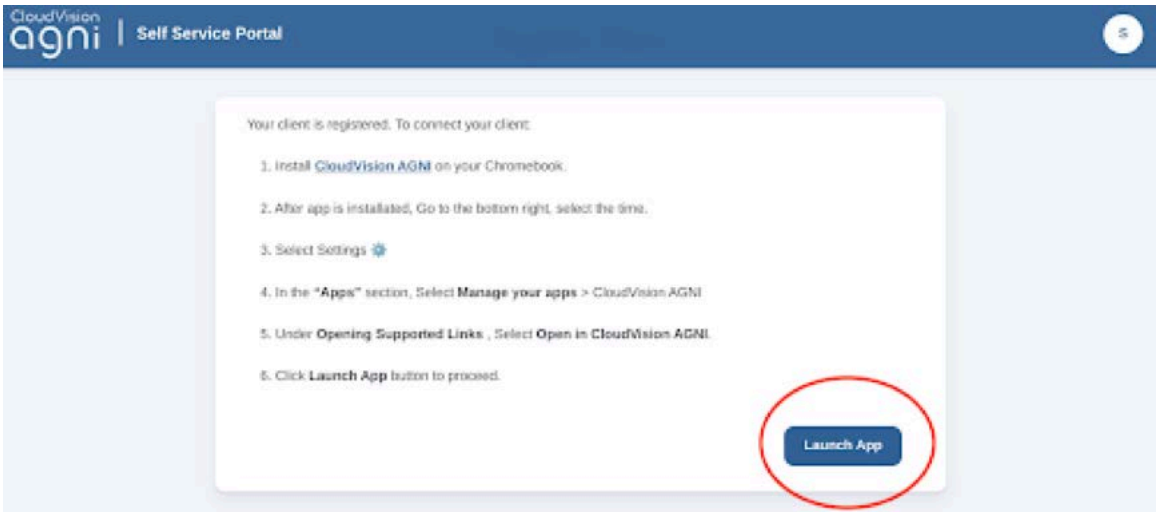
7. Select the **Open in CloudVision AGNI app** from the Opening supported links.

Figure 5-30: CloudVision AGNI App



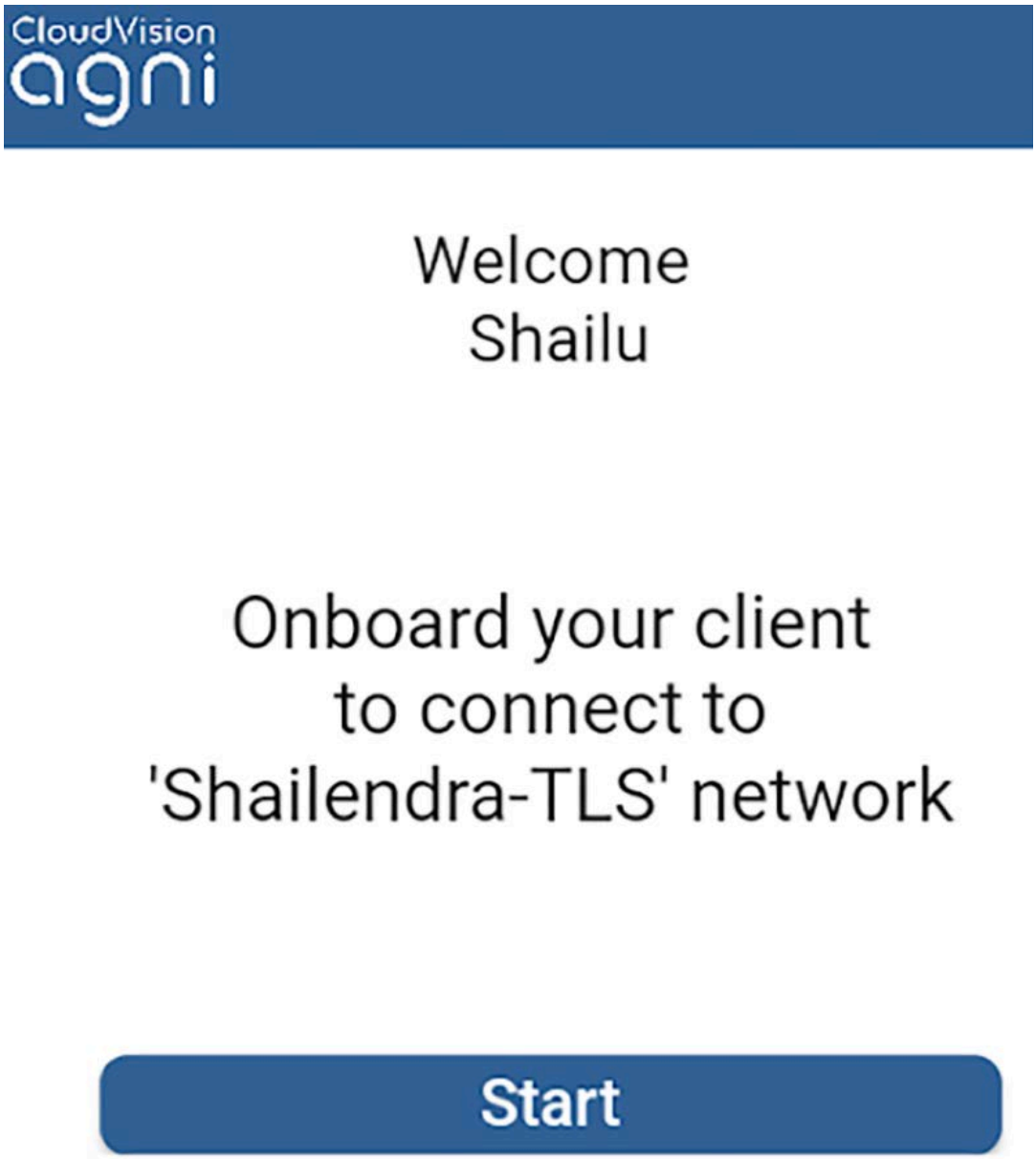
8. Click the **Launch App** button from the Self Service Portal.

Figure 5-31: Launch App



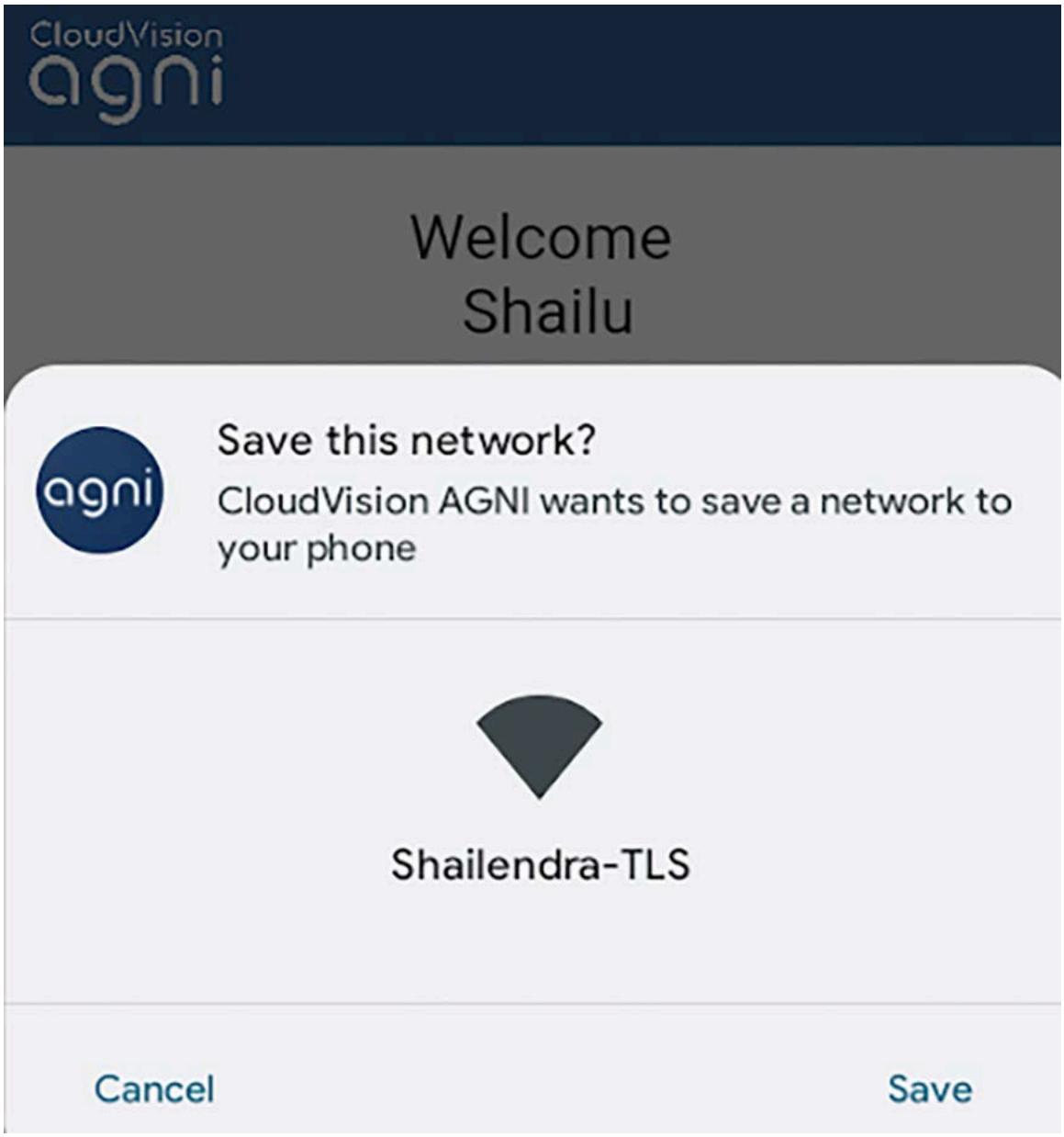
The CloudVision AGNI application is displayed and proceeds with the rest of the configuration.

Figure 5-32: Onboarded Client



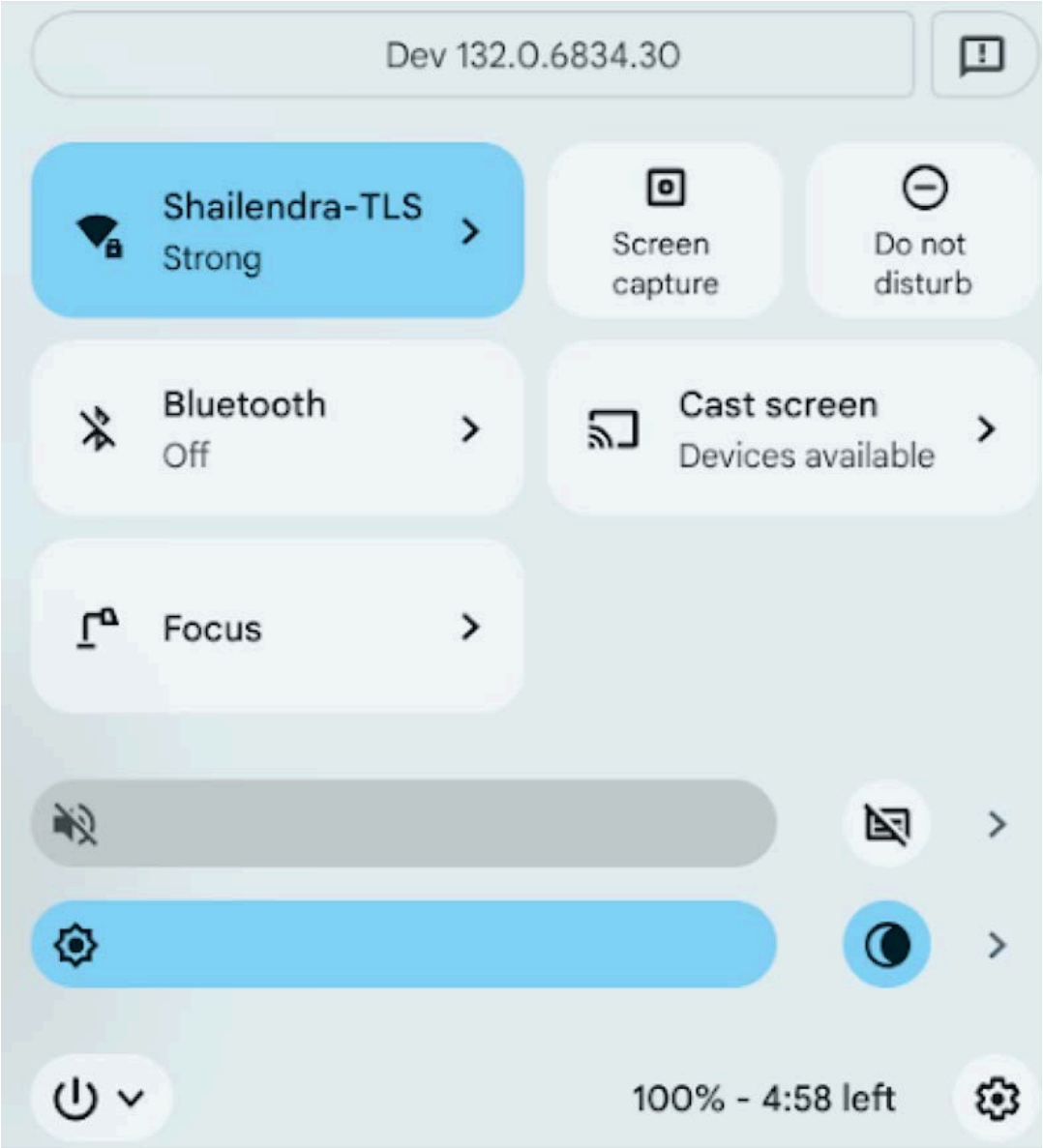
Allow the application to configure the wireless profile and install certificates.

Figure 5-33: Save Network



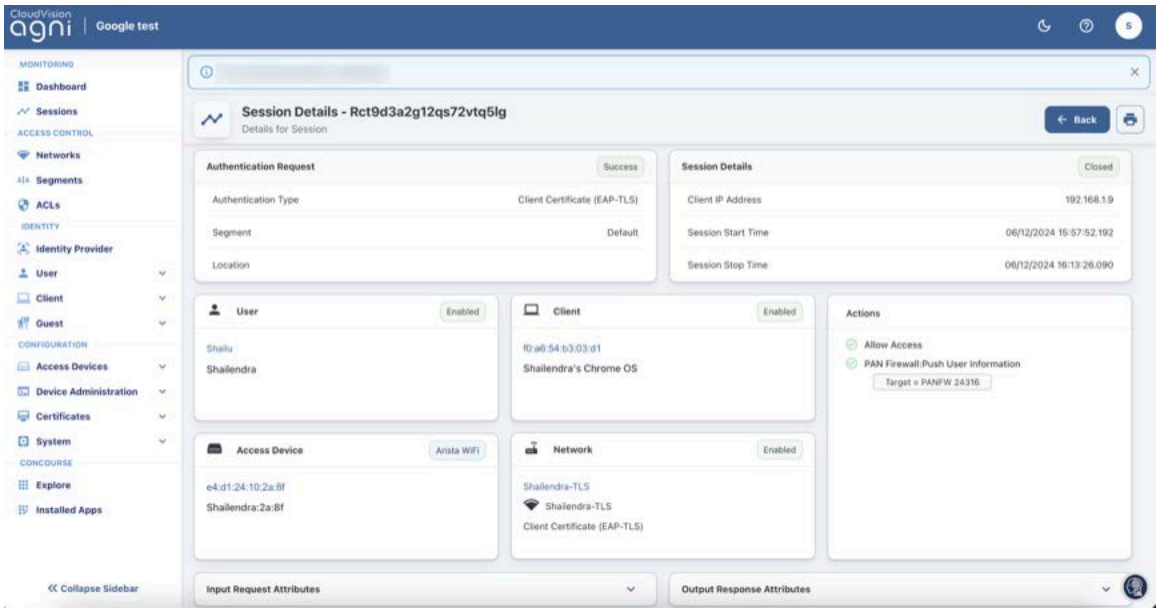
The network profile gets installed with the required certificates.

Figure 5-34: Installed Profile



The client is displayed in the session list in AGNI.

Figure 5-35: Session Details



5.2 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).

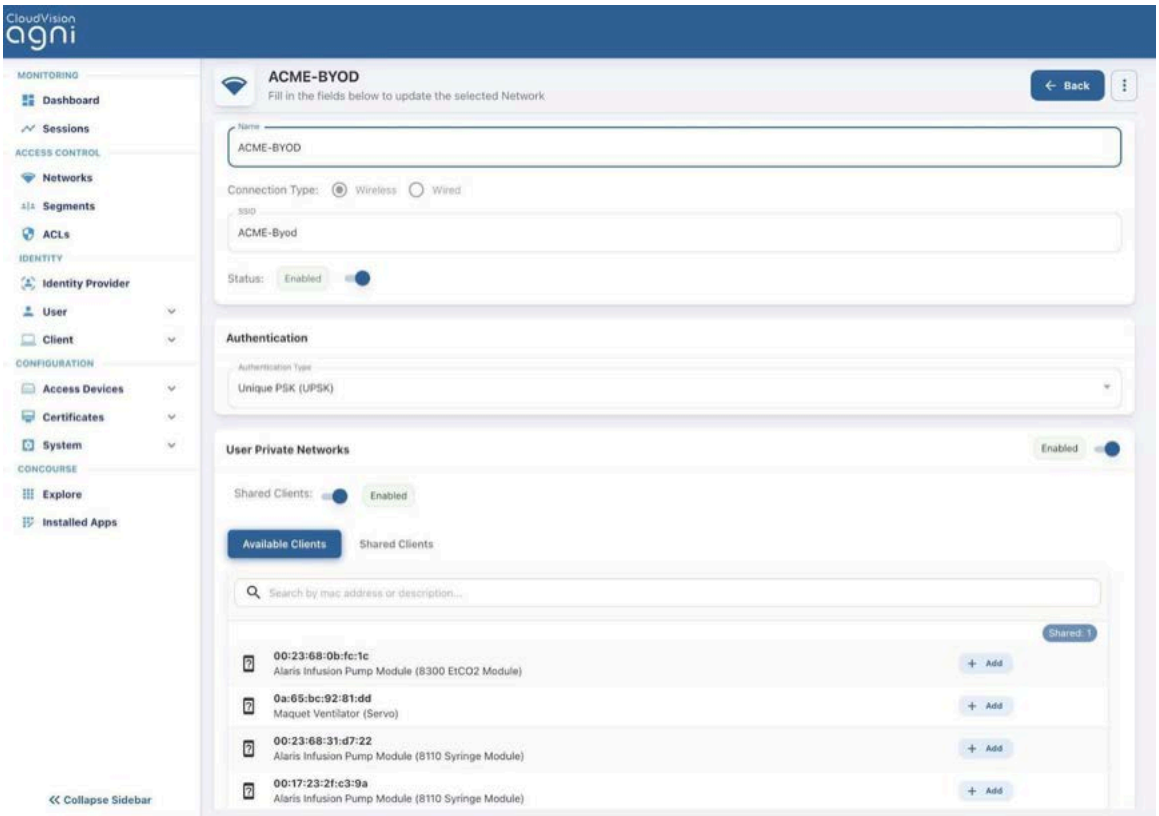
5.2.1 Configuring the UPSK Settings

To configure the UPSK settings, perform the following steps:

1. Navigate to **Access Control** > **Networks**.

2. Click on the **Add Networks** button.

Figure 5-36: Configuring Wireless UPSK Network



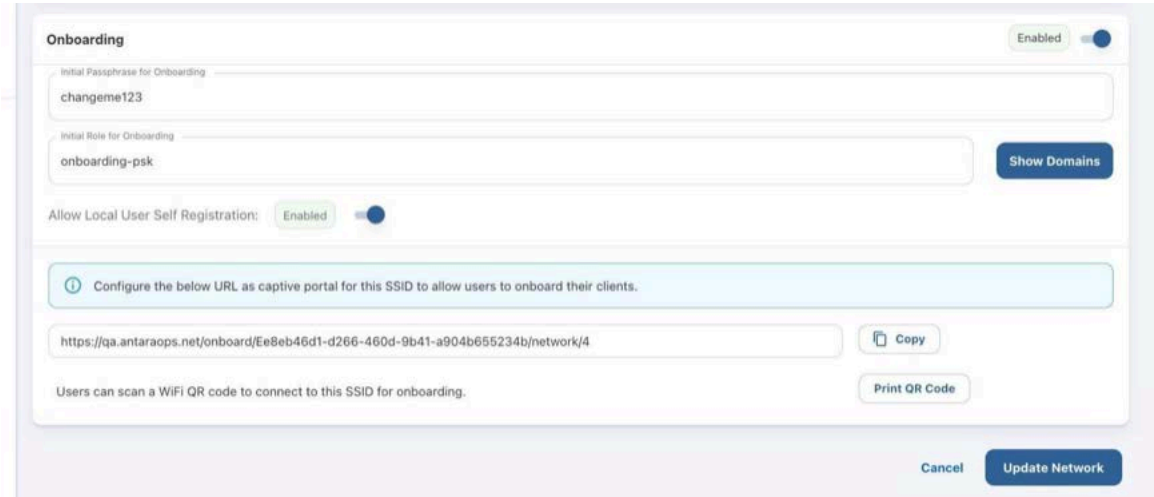
3. Enter the **Network Name** and choose **Connection Type** as **Wireless**.
4. Provide the **SSID** name. Ensure that the name matches the SSID configured in wireless APs.
5. Set the **Status** value:
   a. **Enabled** - Enables this network to honor incoming requests.
   b. **Disabled** - Disables this network.
6. **Authentication** – The type of authentication should be set to Unique PSK (UPSK). This enables the system to honor UPSK authentication requests.
7. **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.
8. **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**:

1. **Disabled** - Disallows local users to self-register into the system as part of the user onboarding process.
2. **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.
3. **Enabled** - Users can self-register into the system as part of the user onboarding process.

Figure 5-37: Wireless UPSK Network User Onboarding



9. 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 Wi-Fi 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.

5.2.2 Configuring the Device Count Limit for Authentication

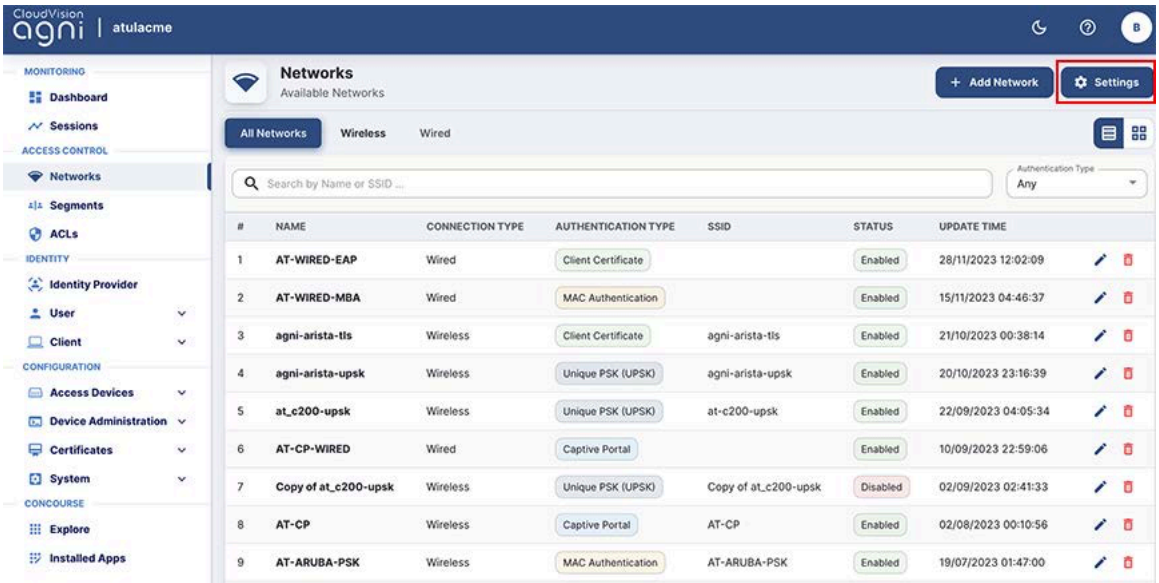
This section describes the steps to configure the maximum device count limit for authentication using Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and UPSK in AGNI.

To configure the EAP-TLS maximum count, perform the following steps:

1. Log in to AGNI and navigate to **Access Control** > **Networks** .

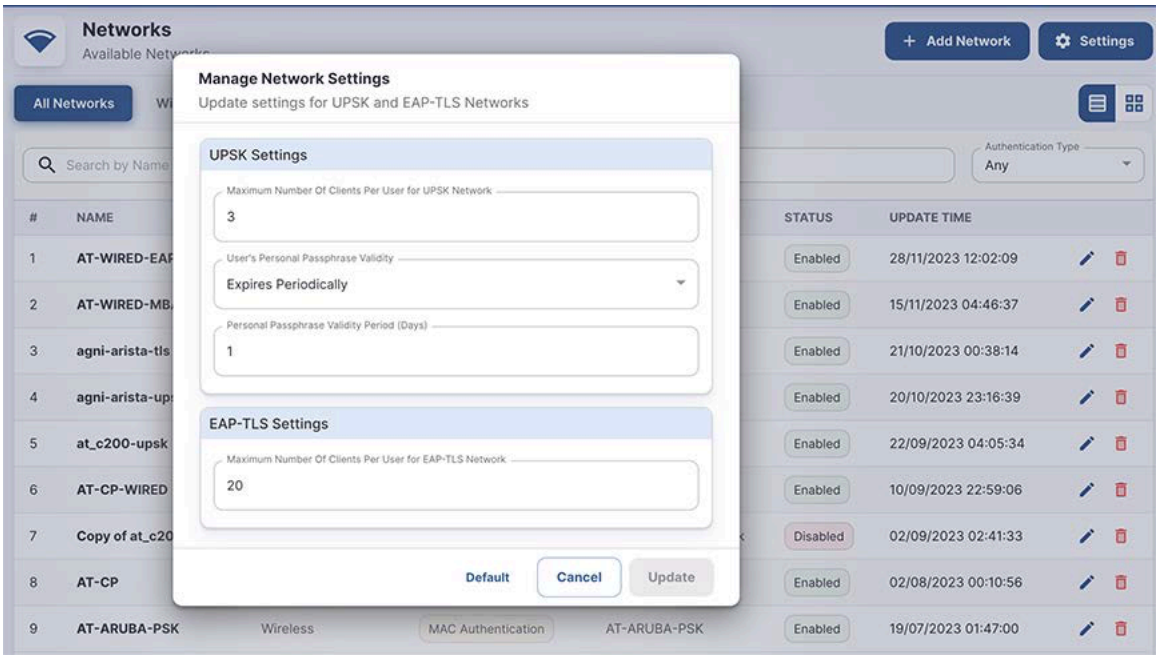
2. Click **Settings** on the top right corner of the dashboard (see image below).

Figure 5-38: List of Networks Page



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

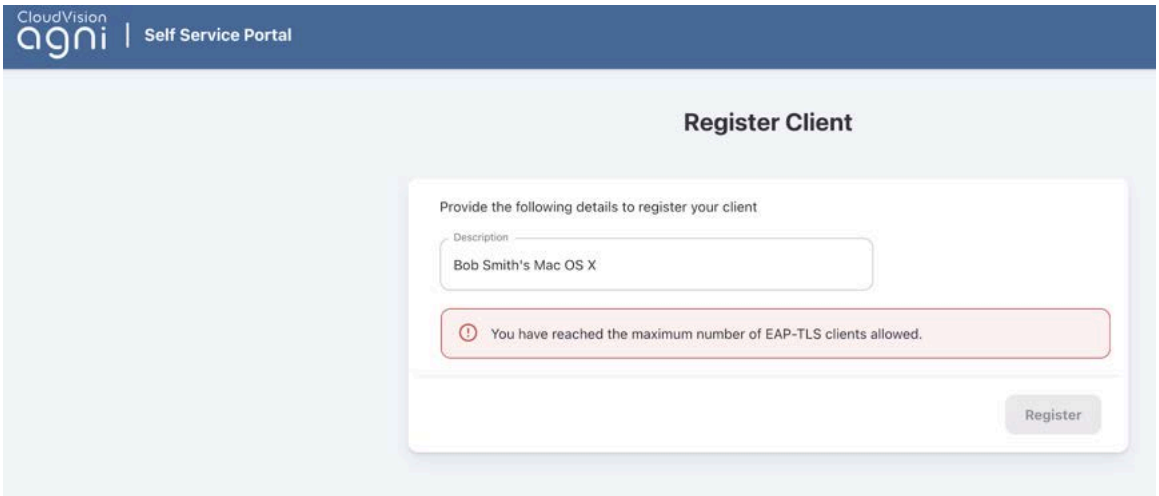
Figure 5-39: Manage Network Settings



3. Enter a value between **1-20** to set the maximum number of clients per user for the EAP-TLS Network.

The maximum number of clients you can add is 20. If you enter a value higher than 20, an error message is displayed as in the image below:

Figure 5-40: 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.

5.3 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).

5.3.1 Configuration Steps

Perform the following steps:

1. Navigate to **Access Control** > **Networks** and select the **Add Networks** button.
2. Enter the **Network Name** and choose **Connection Type** as **Wireless**.
3. Enter the **SSID** name. Ensure the name matches the SSID configured in the wireless APs
4. Set the **Status** value:
   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: 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.
      1. **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.
      2. **Always** - When set, the clients are re-authenticated whenever connected to the captive portal network.
8. **Authorized User Group** - This setting is optional and applicable when the User Type is set to Organizational user. Choose the names of the User Groups, if you need to allow onboarding to be permitted for the users belonging to these groups. When this setting is not provided the system honors onboarding requests from all the users of the organization.
9. **Re-authenticate Registered Clients** - This setting is applicable when the user type is set to Organizational user.
   a. **Periodic** - When set, the clients are re-authenticated once in every Re-authentication Period (days) configured. Re-authentication Period (days) specifies the frequency of re-authentication in days.
   b. **Always** - When set, the clients are re-authenticated whenever connected to the captive portal network.

c. **Not Required** - When set, the user is permitted always into the network after the first captive portal authentication.

Figure 5-41: Wireless Captive Portal Network Page One

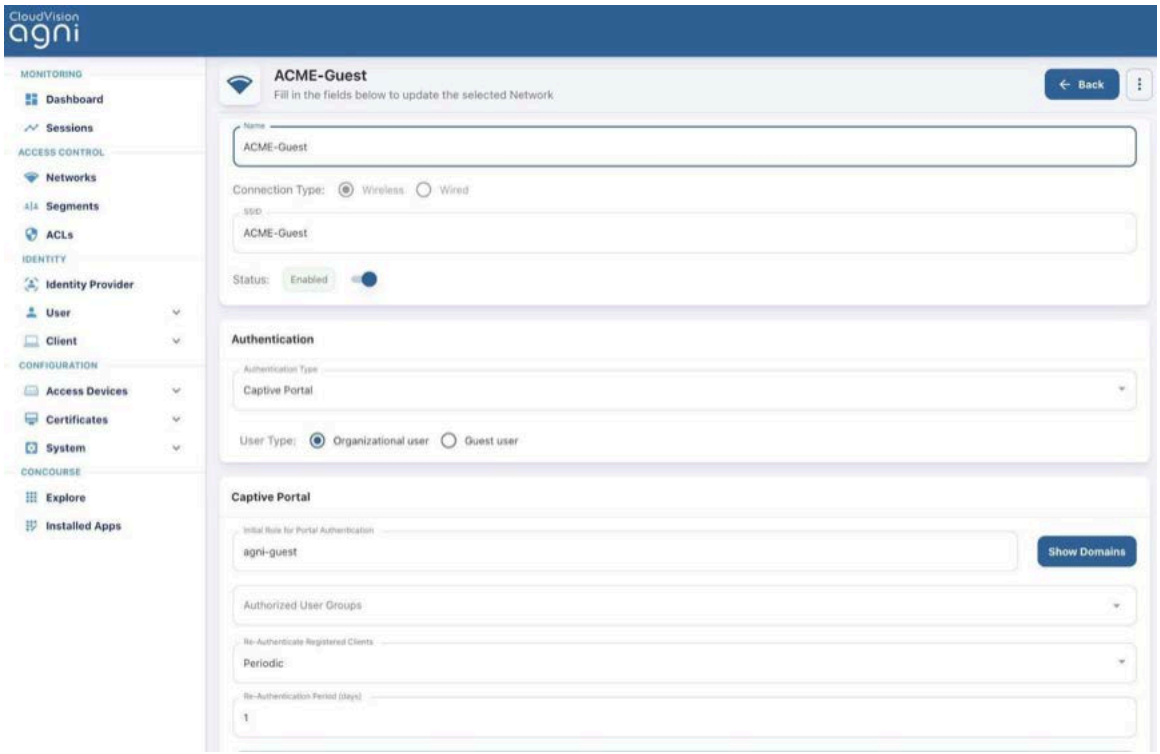
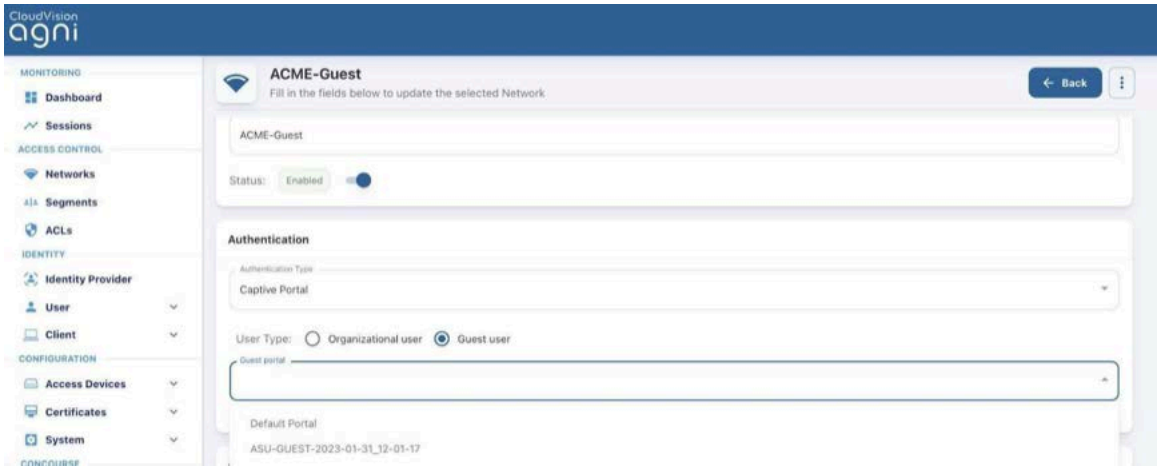


Figure 5-42: Wireless Captive Portal Network Page Two



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 Wi-Fi configuration of your AP. Clients are redirected to this URL for onboarding.

Figure 5-43: Wireless Captive Portal Network Onboarding

5.4 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.

5.4.1 Configuration Steps

To configure a Wireless MAC Authentication Network, perform the following steps:

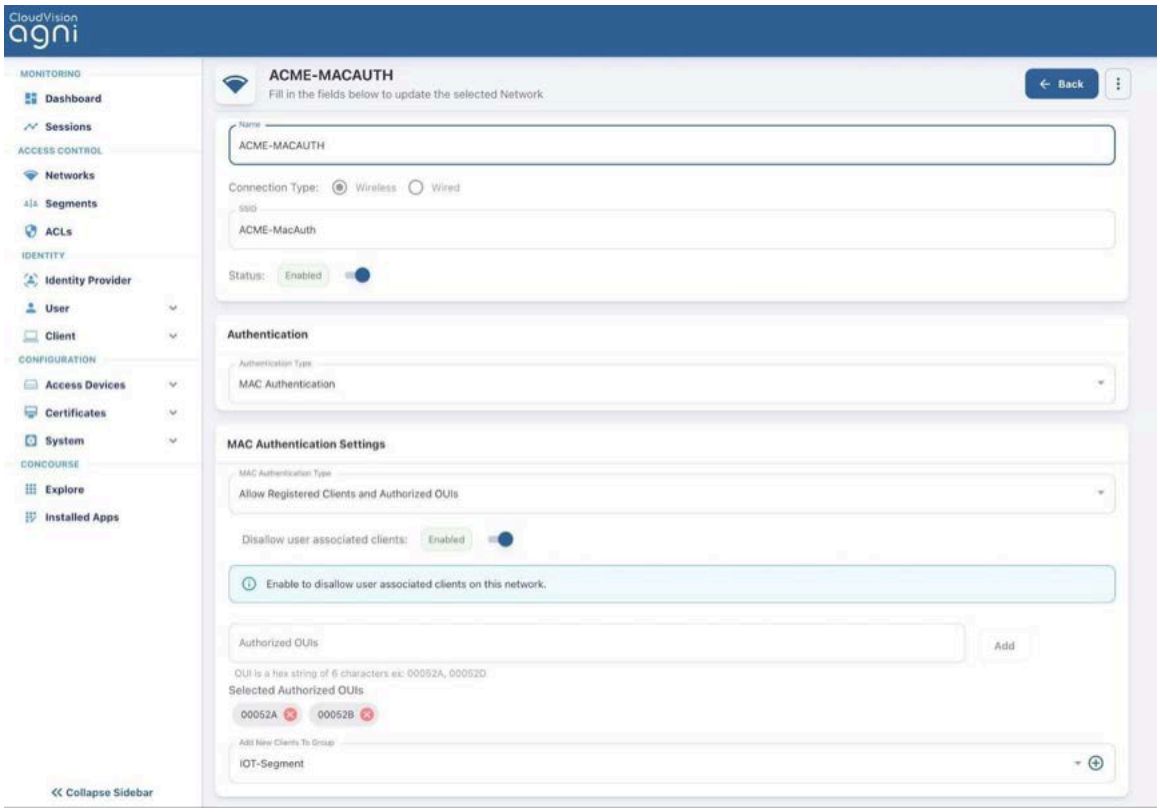
1. Navigate to **Access Control** > **Networks** and select the **Add Networks** button.
2. Enter the **Network Name** and choose **Connection Type** as **Wireless**.
3. Enter the **SSID** name. Ensure the name matches the SSID configured in the wireless APs
4. Set the **Status** value:
   a. **Enabled - 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.
      - **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.

- **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.

1. **Allow New Clients to Group** - Specify the client group to persist the newly authenticated MAC addresses.
2. **Allow Registered Clients and Authorized OUIs** - This option behaves similarly to Allow Registered Clients Only and Authorized OUIs Only combined.

Figure 5-44: Wireless MAC Authentication Network



Chapter 6

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.

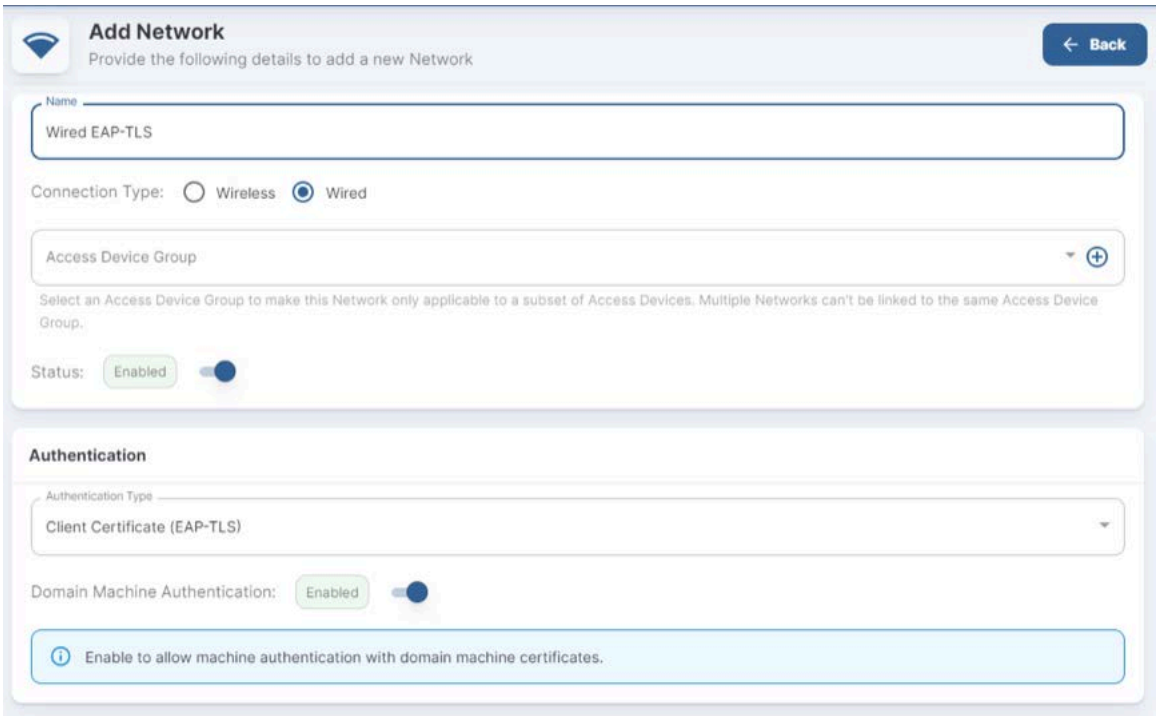
6.1 Configuration Steps

To configure a wired 802.1X network, perform the following steps:

1. Navigate to **Access Control** > **Networks**. Click the **Add Networks** button.
2. Enter the **Network Name** and choose **Connection Type** 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.

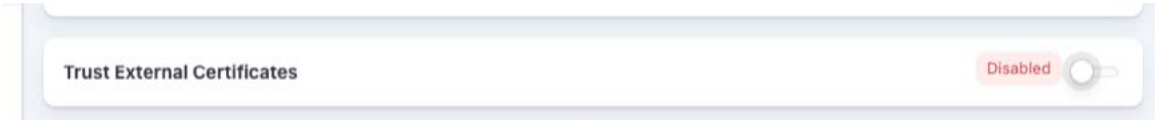
   Figure 6-1: Add Network (Authentication)



6. **Trust External Certificates**:

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

      Figure 6-2: Trust External Certificates

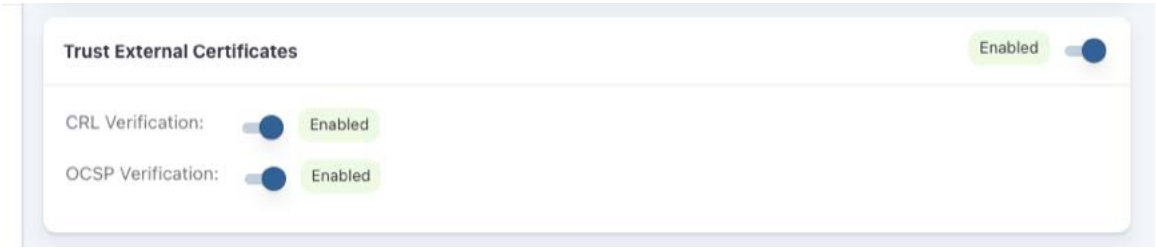


   b. **Enabled** - This option is applicable while using external PKI. You must import the Root and Issuer CAs into the system.

   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.

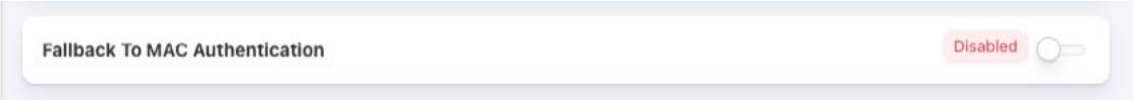
      Figure 6-3: Add Network (Trusted External Certificates)



7. **Fallback to MAC Authentication**

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

Figure 6-4: Add Network (Fallback To MAC Authentication)



b. **Enabled** - When 802.1X authentication fails, the system falls back to MAC authentication.

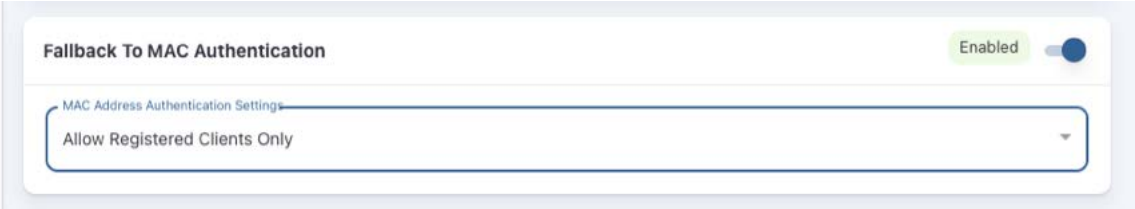
1. **MAC Authentication Type** - Lists the available authentication settings and chooses the one applicable to the network.

   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 enables to build an inventory of the client devices.

   Figure 6-5: Add Network (MAC Address Authentication Settings)

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

   Figure 6-6: Add Network (Fallback to MAC Authentication)



   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 enables to create an inventory of the client devices.

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

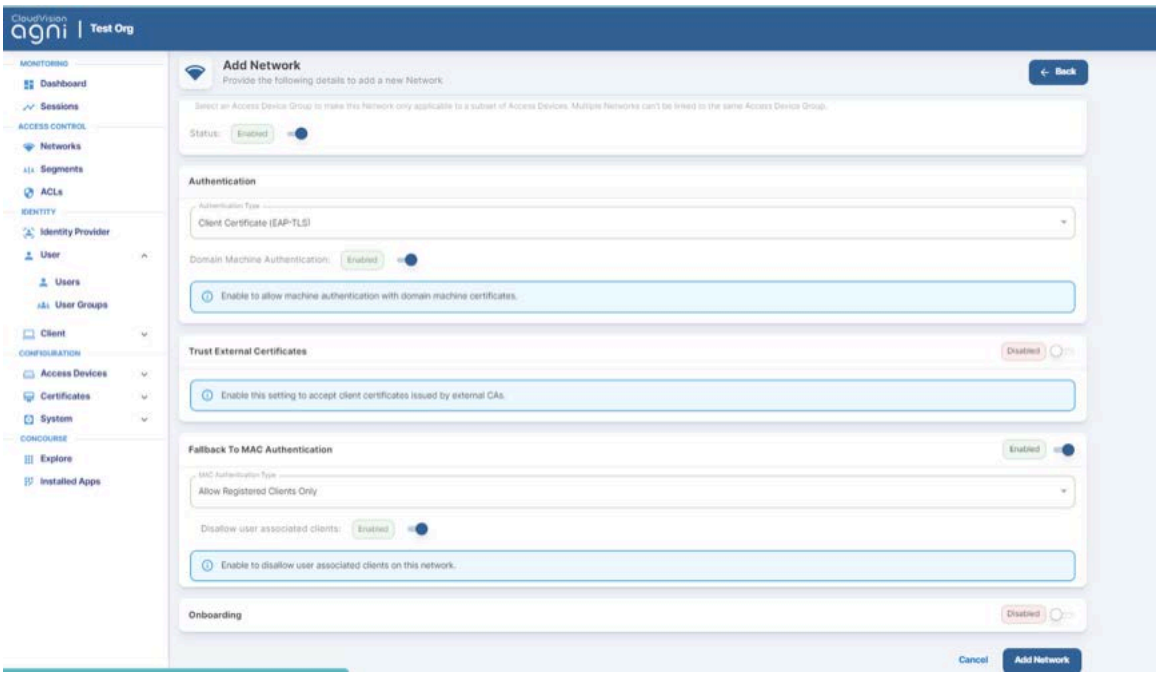
   Figure 6-7: Allow Authorized OUIs Only

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 6-8: Onboarding

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

Figure 6-9: Sample Wired 802.1X configuration



6.2 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.

6.2.1 Configuration Steps

To configure a wired MAC authentication network, perform the following steps:

1. Navigate to **Access Control** > **Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **Connection Type** as **Wired**.
3. **Access Device Group** - (Optional setting) If the network authentication is only applicable to a subset of Access Devices, then choose the **Access Device Group**. Otherwise, the network applies to all the network access devices.
4. **Authentication** - Choose the Authentication Type as **MAC Authentication**.

5. **MAC Authentication Settings** - Lists the available authentication settings, you can choose the one applicable to the network.

   a. **Allow All Clients** - When set, the MAC authentication admits all the clients that are attempting the wired authentication. Choose a client group to add the authenticated MAC addresses. This help to build an inventory of the client devices.

   Figure 6-10: 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.

   Figure 6-11: Add Network (MAC Address Authentication Settings)

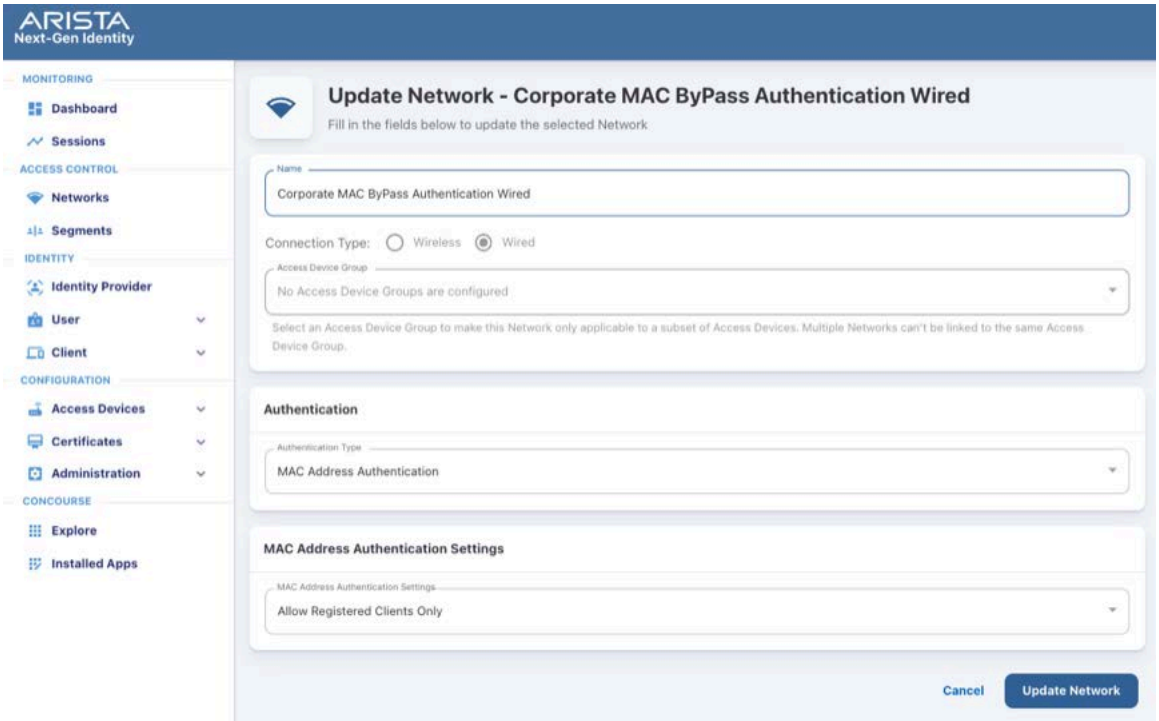
   c. **Allow Authorized OUIs Only** - When set, the system honors the MAC authentication attempts only from the clients matching the authorized OUI list. The Authorized OUI list should be specified for this setting. Choose a client group to add the authenticated MAC addresses. This helps to build an inventory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

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

Figure 6-12: Add Network (Authorized OUIs)

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

Figure 6-13: MAC ByPass Authentication Configuration



6.3 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.

6.3.1 Configuration Steps

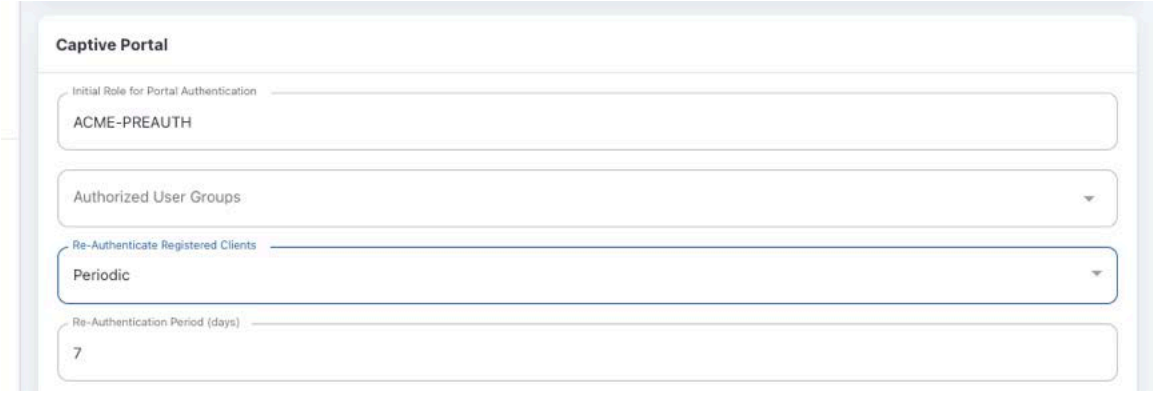
To configure a wired captive portal network, perform the following steps:

1. Navigate to **Access Control** > **Networks**. Click on the **Add Networks** button.
2. Enter the **Network Name** and choose **Connection Type** 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:** 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.

Figure 6-14: Figure: Captive Portal

Figure 6-15: 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 6-16: Captive Portal URL

6.4 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.

6.4.1 Configuring AGNI

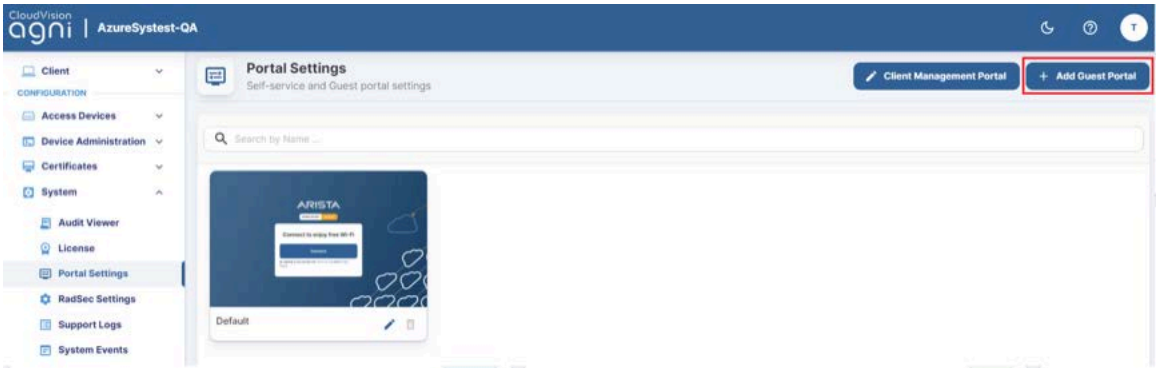
Perform the following steps to configure AGNI.

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

   Figure 6-17: Guest Portal

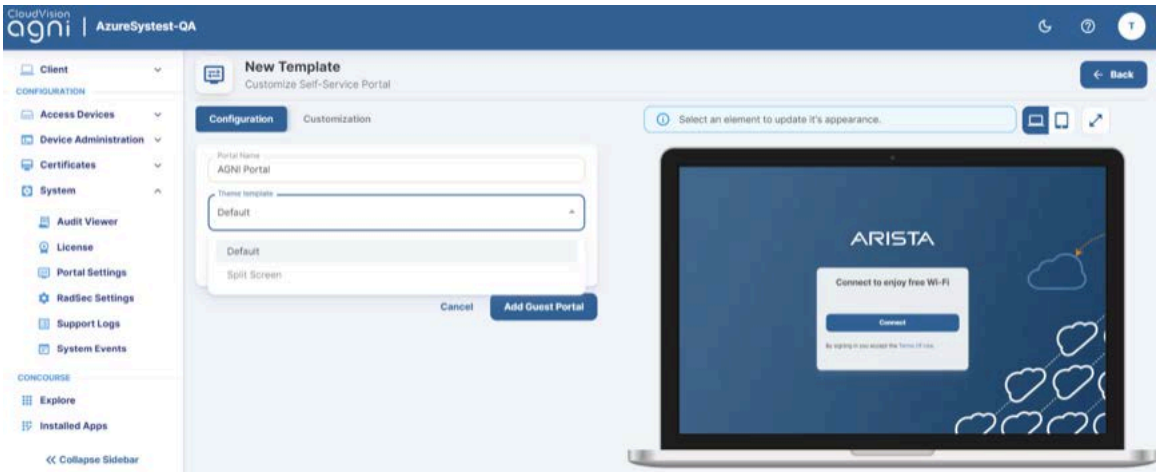
2. Click the **Add Guest Portal** button.

   Figure 6-18: Add Guest Portal



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**.

   Figure 6-19: Configure Portal



4. Select the **Authentication Type** as **Clickthrough**.
5. Click the **Customization** tab to customize the portal settings, including:
   a. **Page**

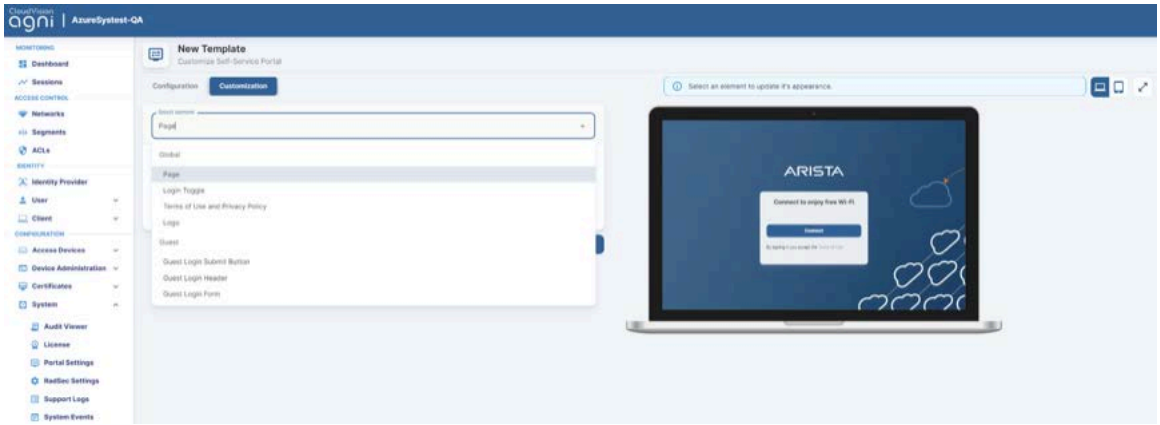
b. **Login Toggle**

c. **Terms of Use and Privacy Policy**

d. **Logo**

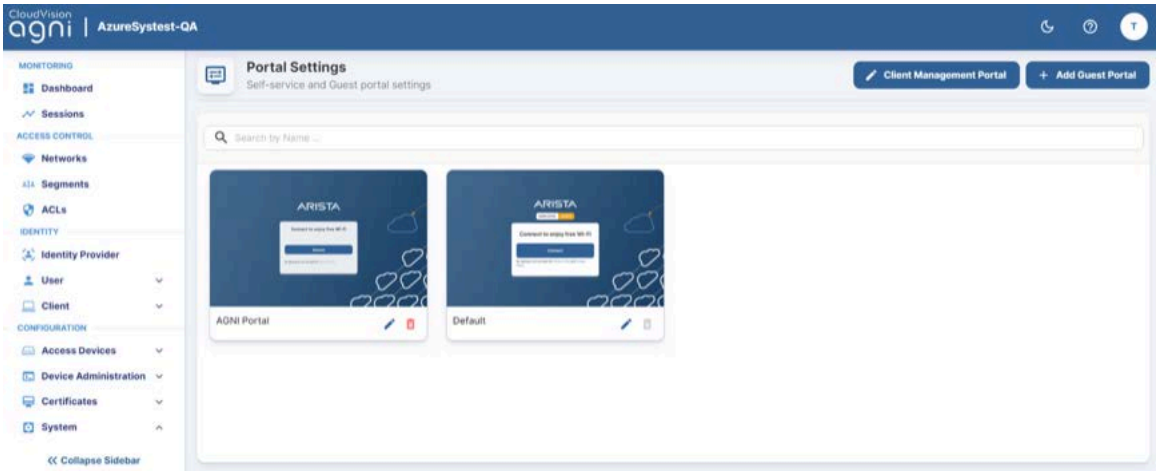
e. **Guest Login Submit Button**

Figure 6-20: Customize Portal



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

Figure 6-21: Added Guest Portal



7. Navigate to **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**

1. **Authentication Type - Captive Portal**
2. **Captive portal type - Internal** for AGNI Hosted Captive Portal.

e. **Captive Portal**

1. **Initial ACL** - ACL Name
2. **Authorized user group** - if applicable

3. **Re-Authentication Clients** - per requirement

Figure 6-22: Network Settings

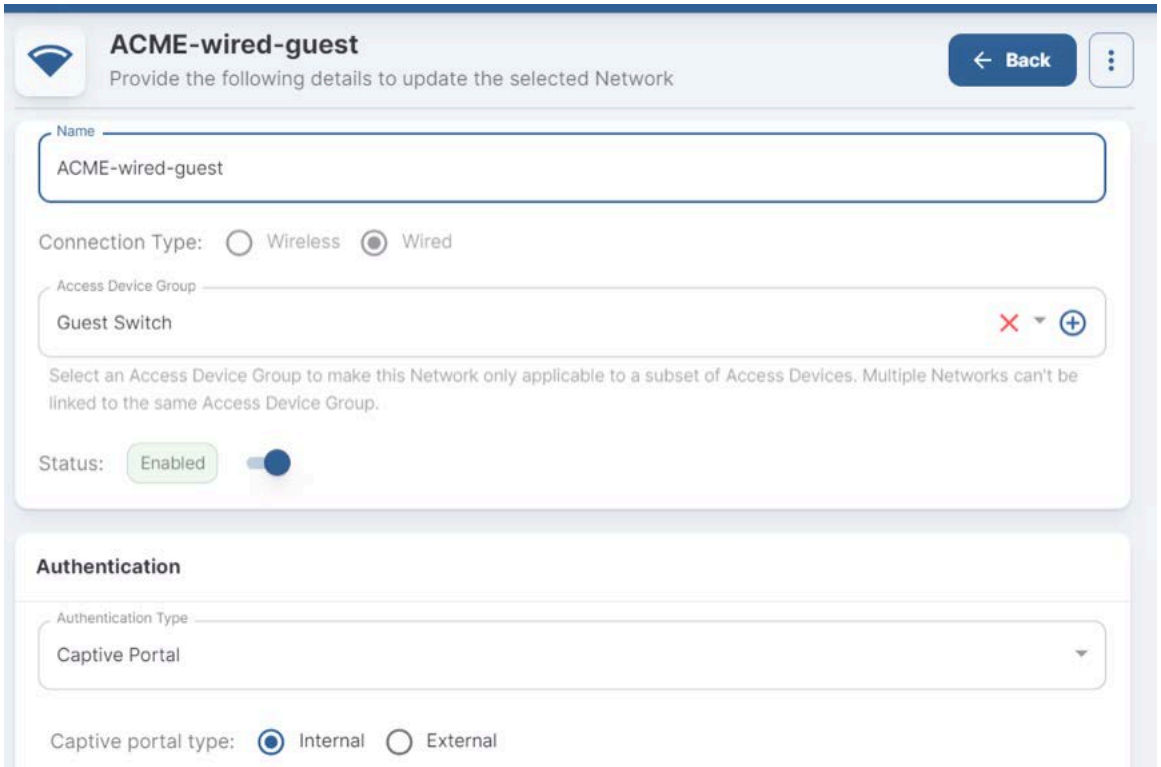
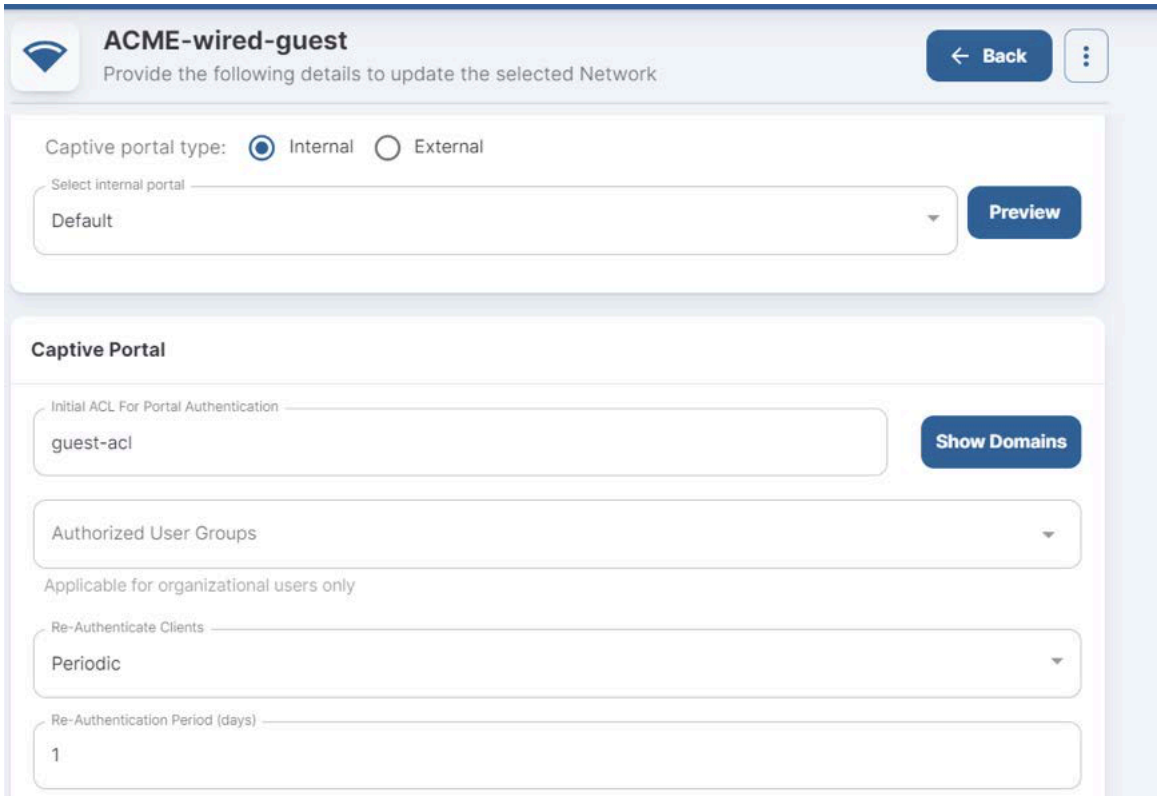
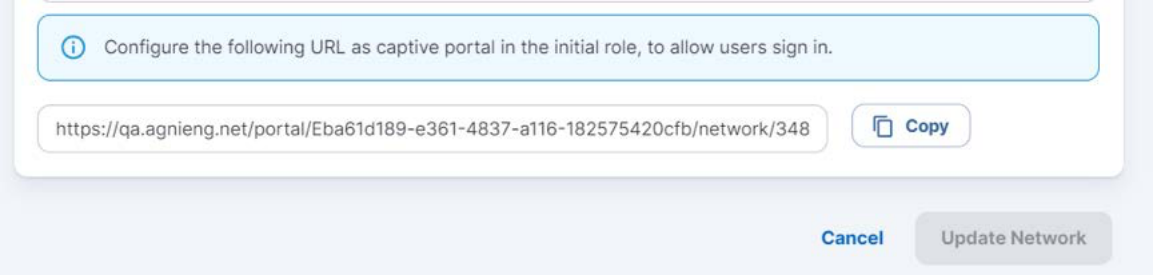


Figure 6-23: Network Settings



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

Figure 6-24: Portal URL



6.4.2 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
!
```

Chapter 7

Configuring Segmentation Policies

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

7.1 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.

7.2 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.

7.3 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

7.4 Configuration

Perform the following steps to configure segmentation policies:

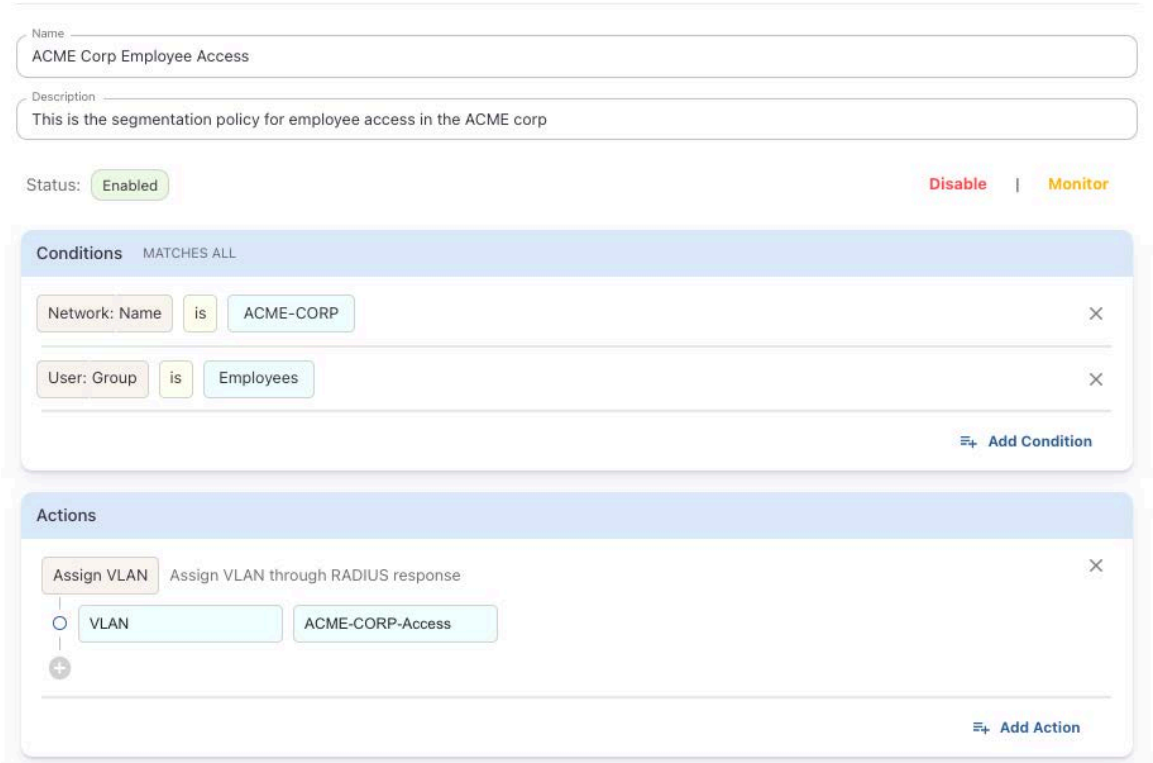
1. Navigate to **Access ControlSegments**. Click on the **Add Segment** button.
2. Enter **Name** and **Description**.
3. Add **Conditions**.
4. Add **Actions**.
5. Click **Add Segment** button to save the segment.

7.4.1 Sample Segments

The following samples are for reference.

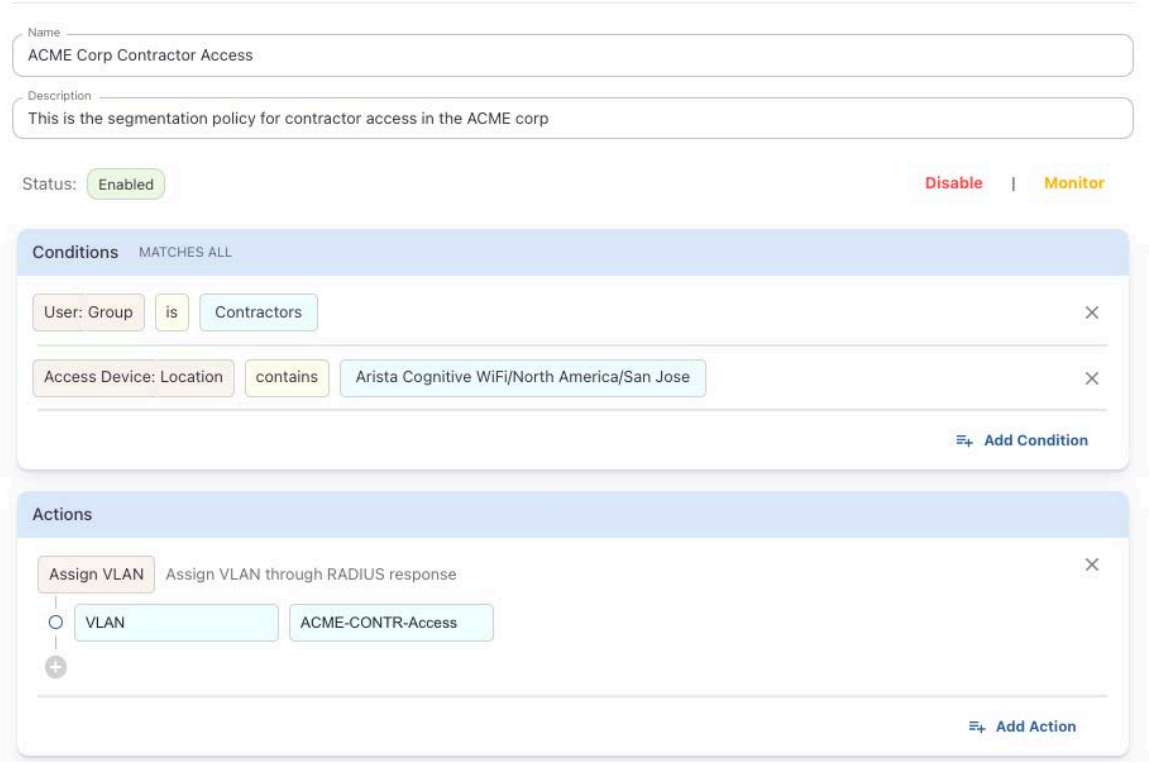
Sample Employee Access Segment:

Figure 7-1: Employee Access Segment Policy



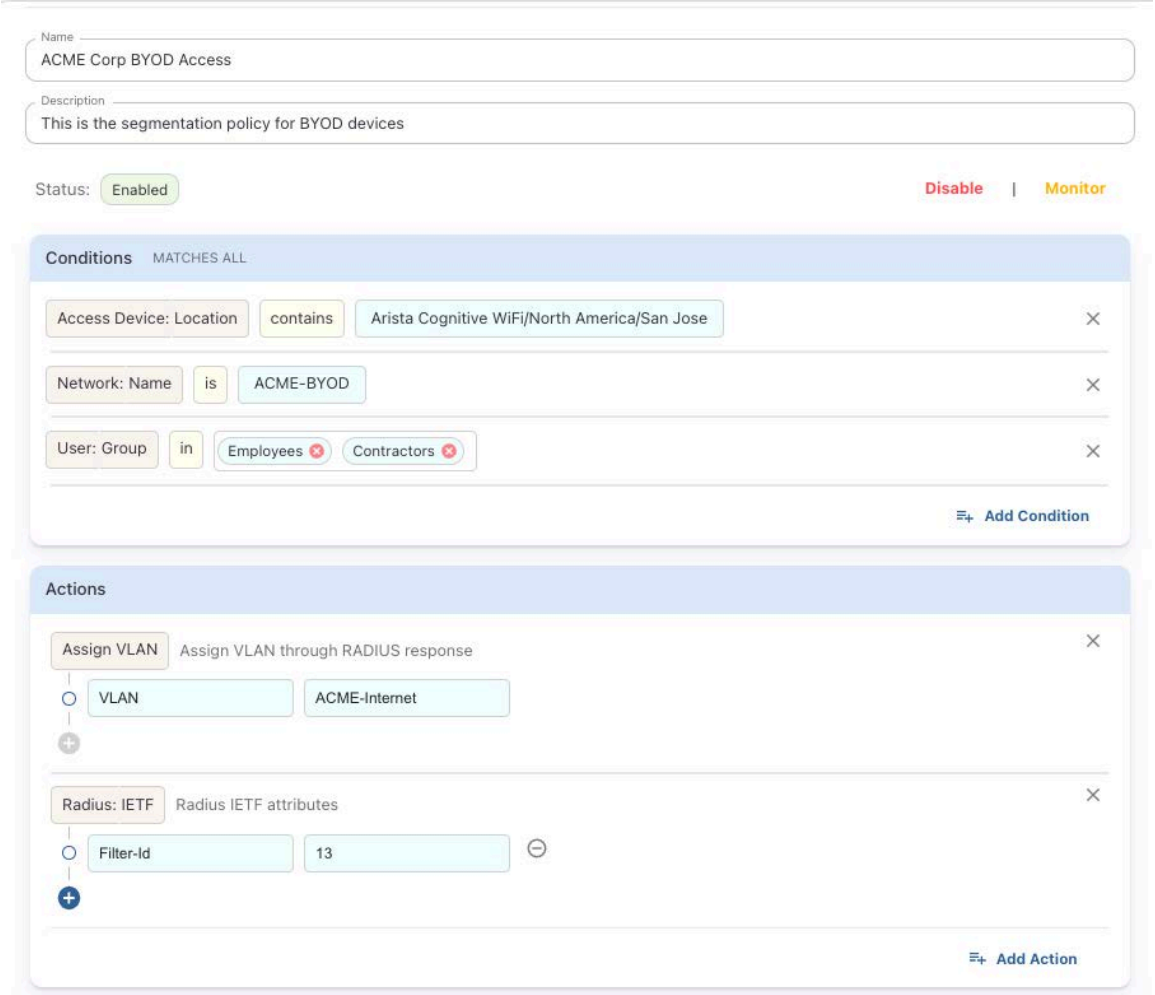
Sample Contractor Access Segment:

Figure 7-2: Contractor Access Segment Policy



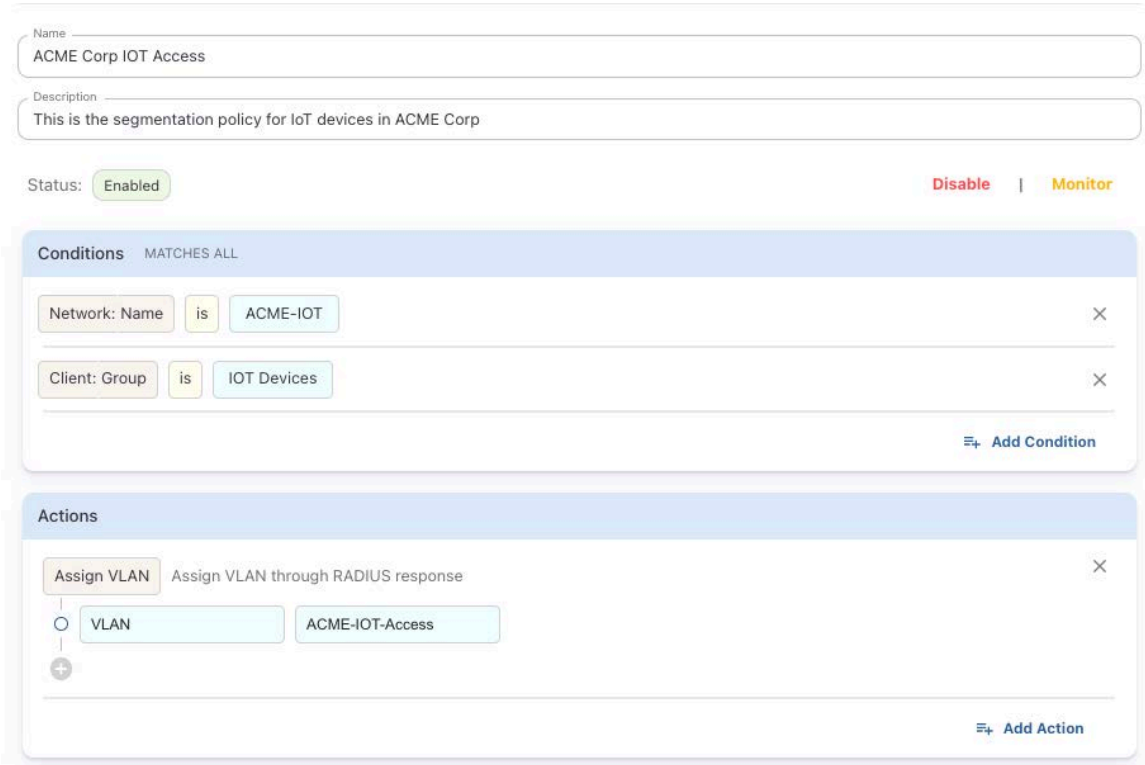
Sample BYOD Access Segment:

Figure 7-3: BYOD Access Segment Policy



Sample IOT Access Segment:

Figure 7-4: IOT Access Segment Policy



Chapter 8

Configuring the Devices in AGNI

Network Access Devices (NADs) connect with AGNI via RADIUS or 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 add the devices.
- Add a whole subnet
- Import the devices using CSV file

For details on the concourse plugin installation, see the Integrating with Concourse Applications section (above).

8.1 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 RADIUS and RadSec protocol. The vendor list includes:

- Arista Wi-Fi
- Arista Switch
- Aruba
- Cisco
- Cisco Meraki
- Generic
- Juniper

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

To add or import access devices, perform the following steps:

1. Navigate to **Configuration** > **Access Devices** > **Devices**
2. Select **Add Device** option and enter the following details:
   a. **Name** of the device.
   b. **IP Address** of the device.
   c. **MAC Address** of the device.
   d. Choose the **Vendor** from the list.
   e. Enter the **Serial Number** of the device. (This field is mandatory only for Cisco Meraki devices).

f. Enter the **RADIUS Shared Secret** for the device.

g. Enter the **TACACS+ Shared Secret** for the device.

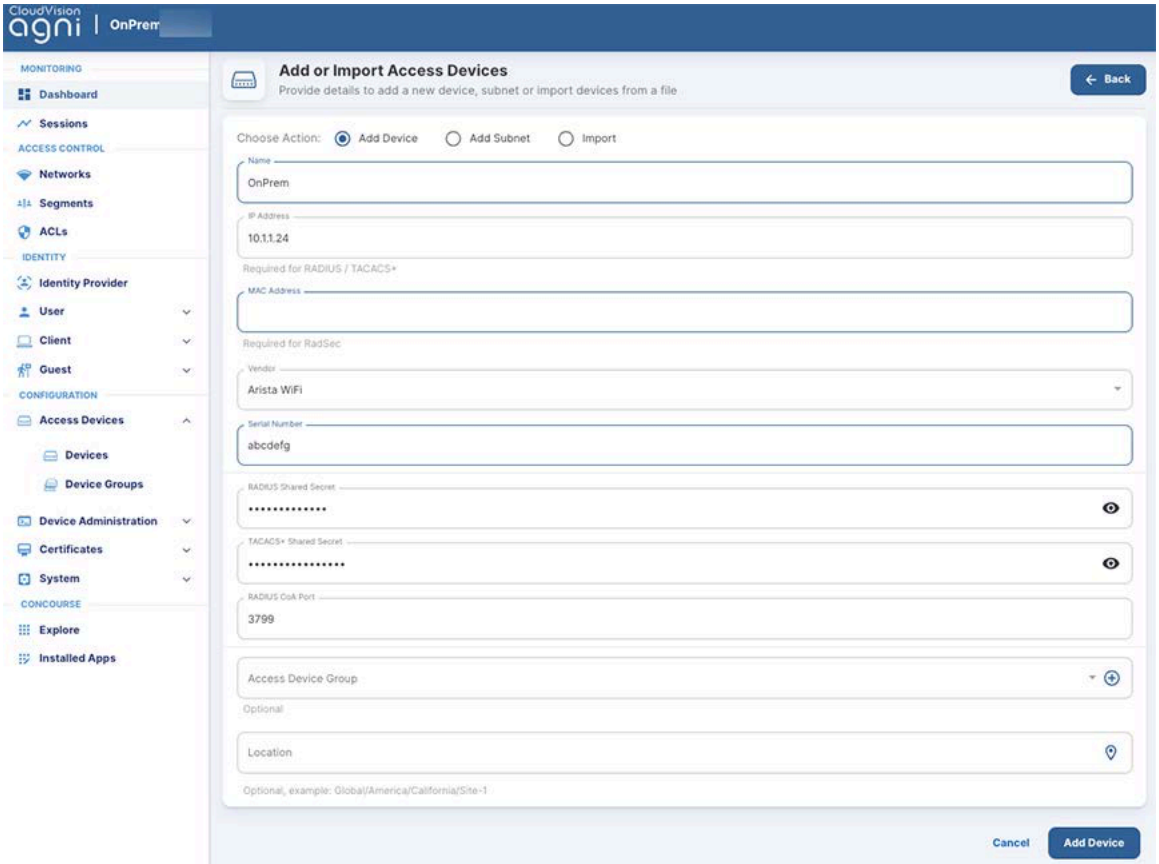
h. Enter the **RADIUS CoA Port** for the device. The default port is **3799**.

i. Enter the **Access Device Group** to which this new device is part of. You can also add a new device group by clicking the **+** icon.

j. Enter the **Location** of the device.

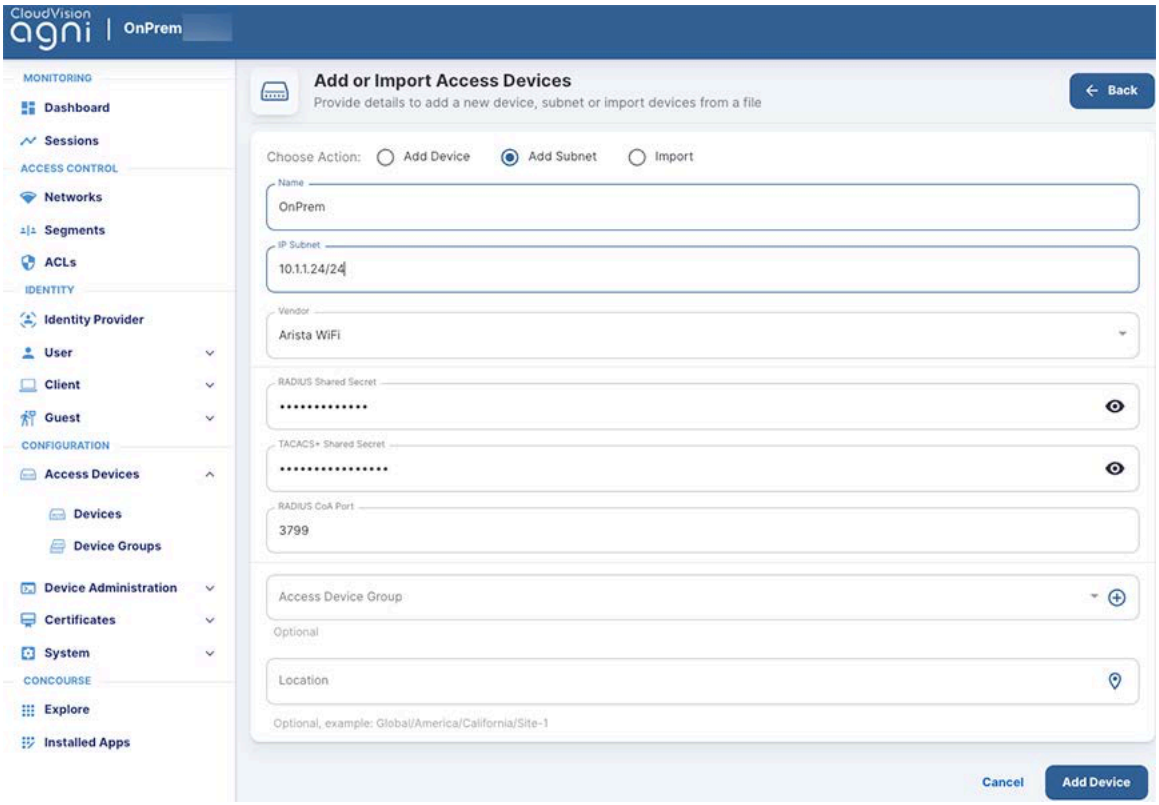
3. Click the **Add Device** button.

Figure 8-1: Adding or Importing a Device



4. To add a subnet, select the **Add Subnet** option and enter the details:

Figure 8-2: Adding a Subnet



To import a device group, see the Importing Devices in Bulk to AGNI section.

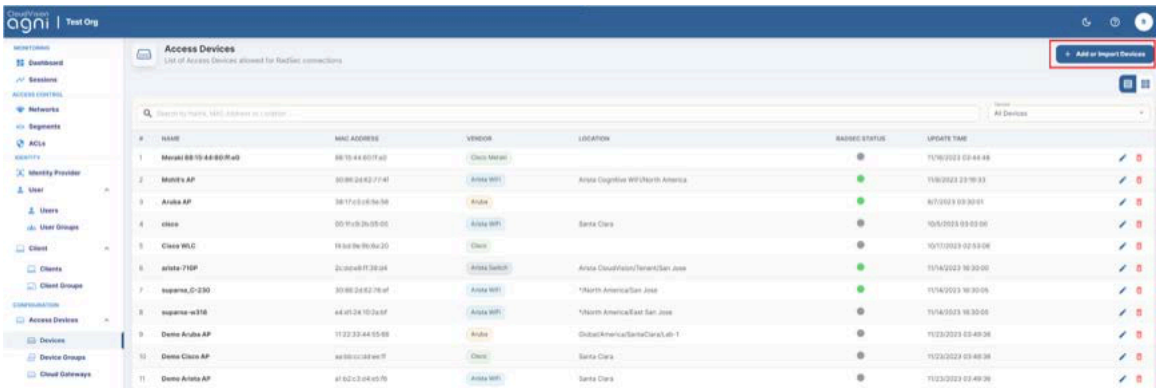
8.2 Importing Devices into AGNI

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, perform the following steps:

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

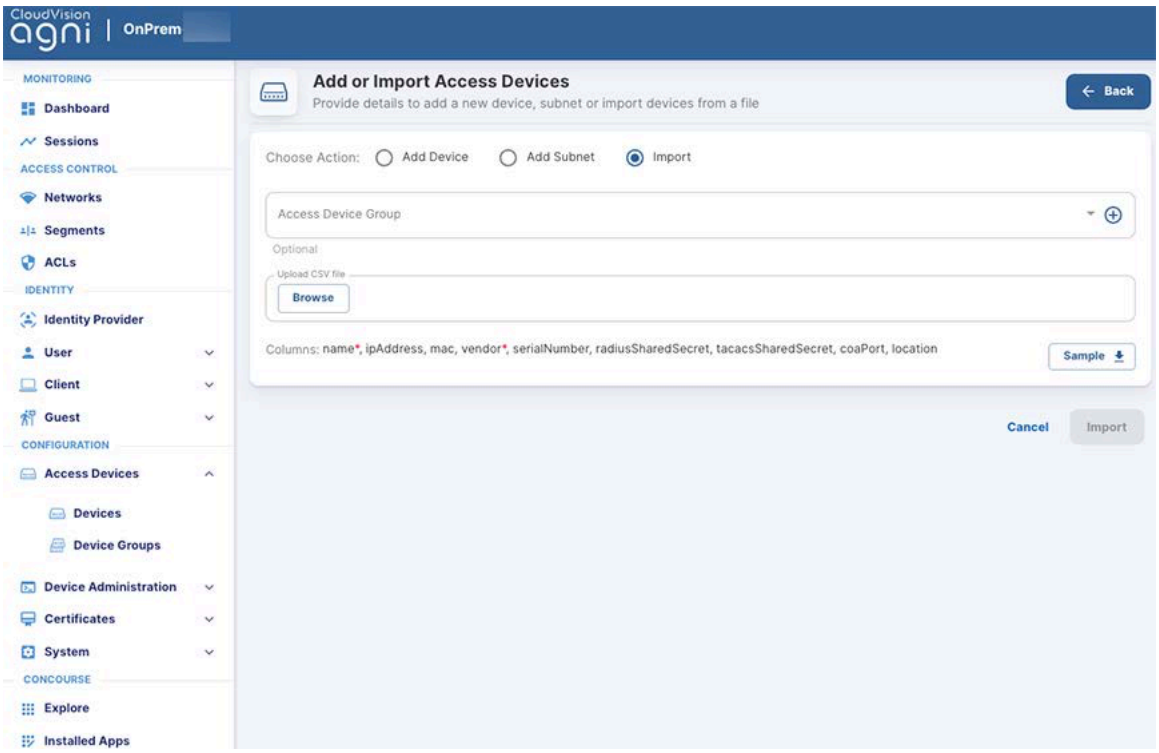
   Figure 8-3: Importing Access Devices



> **Note:** The Serial Number is a mandatory field for adding Cisco-Meraki devices using `.CSV` file format.

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

   Figure 8-4: Choosing Import option



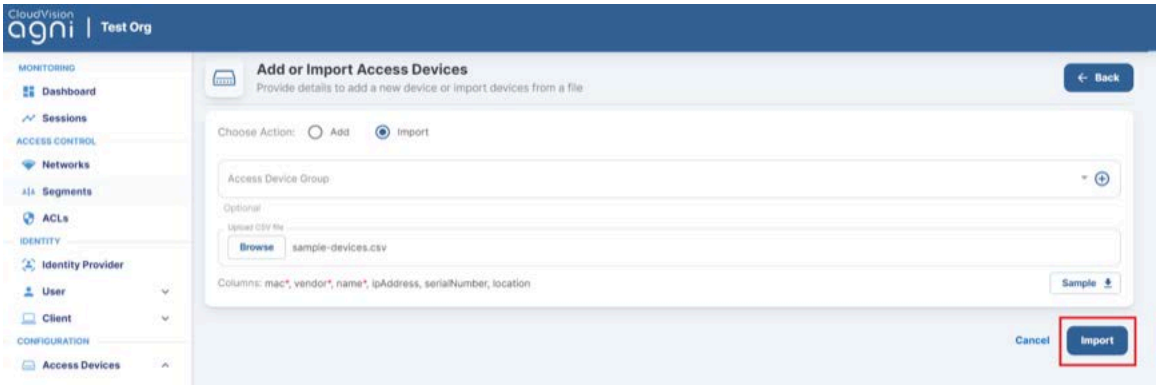
As an admin, you can download a sample `.CSV` file and create the desired `.CSV` file in the required format. The `.CSV` file includes the following columns:

- Name (mandatory)
- IP Address (optional)
- MAC Address (mandatory)
- Vendor (mandatory)
- Serial Number (mandatory for Cisco-Meraki devices only))

- Radius Shared Secret (optional)
- TACACS+ Shared Secret (optional)
- CoA Port (optional)
- Location (optional)

3. To download a sample `.CSV` file, click the **Sample** button.
4. 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 8-5: Add or Import Devices - Import Button



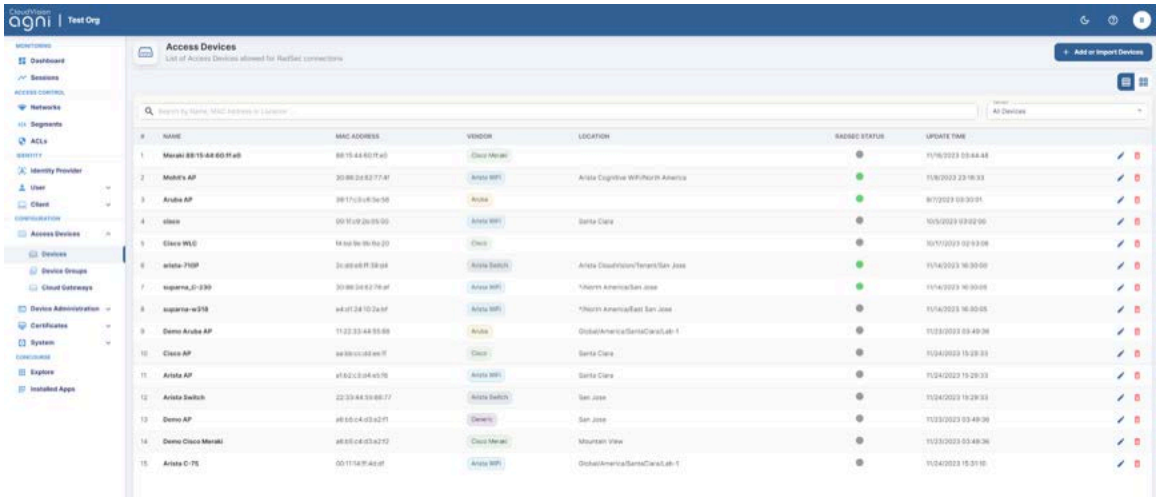
> **Note:** You can also assign a device group while importing the Network Access devices. Once the bulk device import is complete, all the devices get associated with the selected device group.

5. 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).

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

Figure 8-6: Access Devices List



Chapter 9

User Configurations

9.1 Users

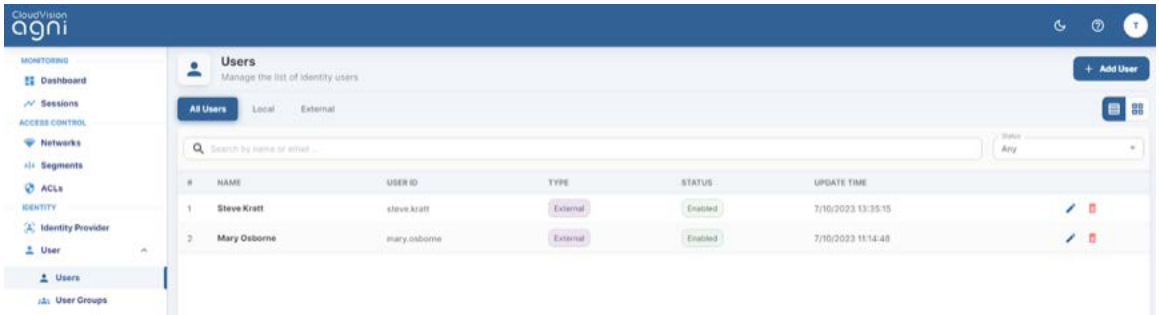
9.1.1 All Users

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.

9.1.2 External Users

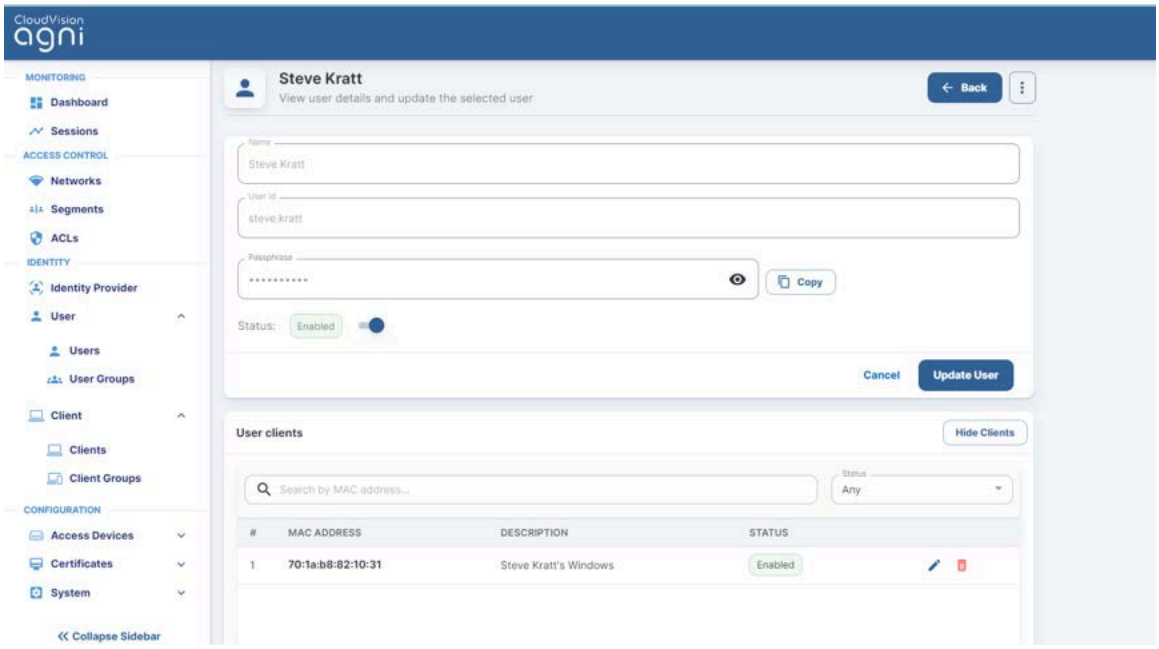
AGNI synchronizes the users in external IDPs (e.g.: Azure AD, Okta, OneLogin, and others) along with user attributes and group memberships. The users are marked external in the user's listing.

Figure 9-1: External Users



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

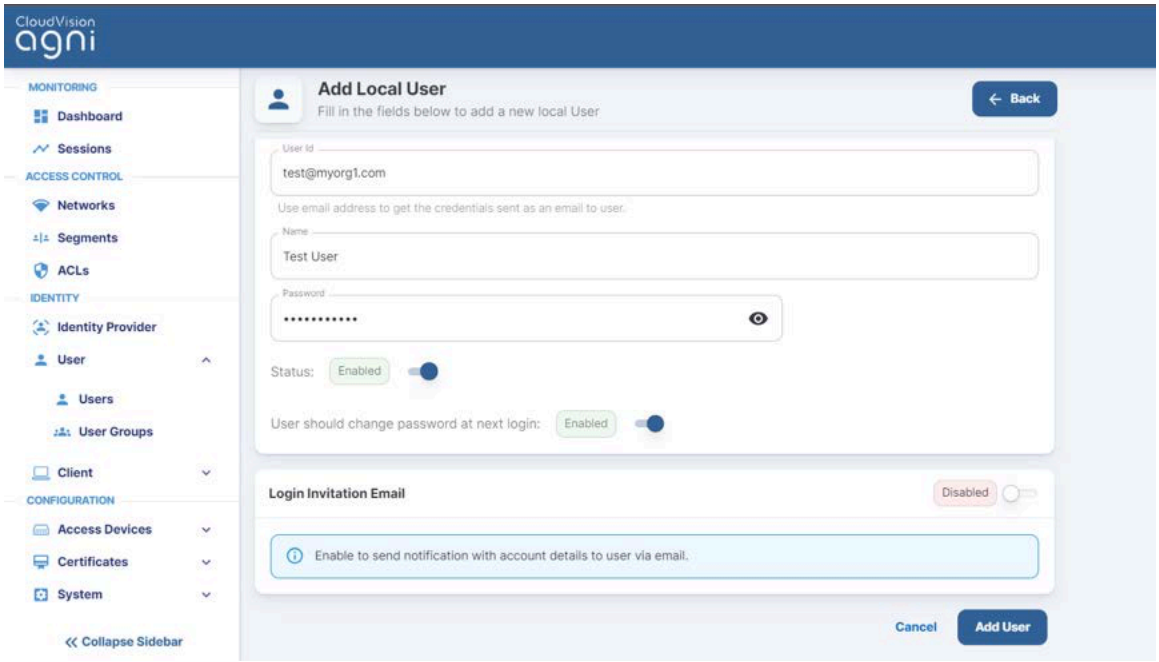
Figure 9-2: External User Updated Information



9.1.3 Local User

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

Figure 9-3: Add Local Users



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).

Figure 9-4: Local User with Read-only Access (part of Restricted User Group)

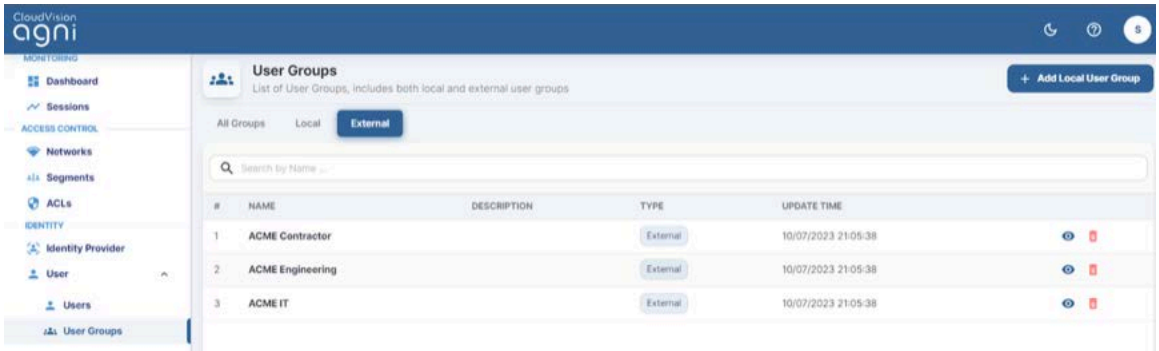
9.2 User Groups

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

External User Groups are synchronized with the configured IDPs. These are managed externally. AGNI provides visibility of the group details in this interface. If an external user group needs to be deleted then

Admin should remove it from the Available Groups in the IDP config. The changes are local to the system and not reflected in the external IDPs.

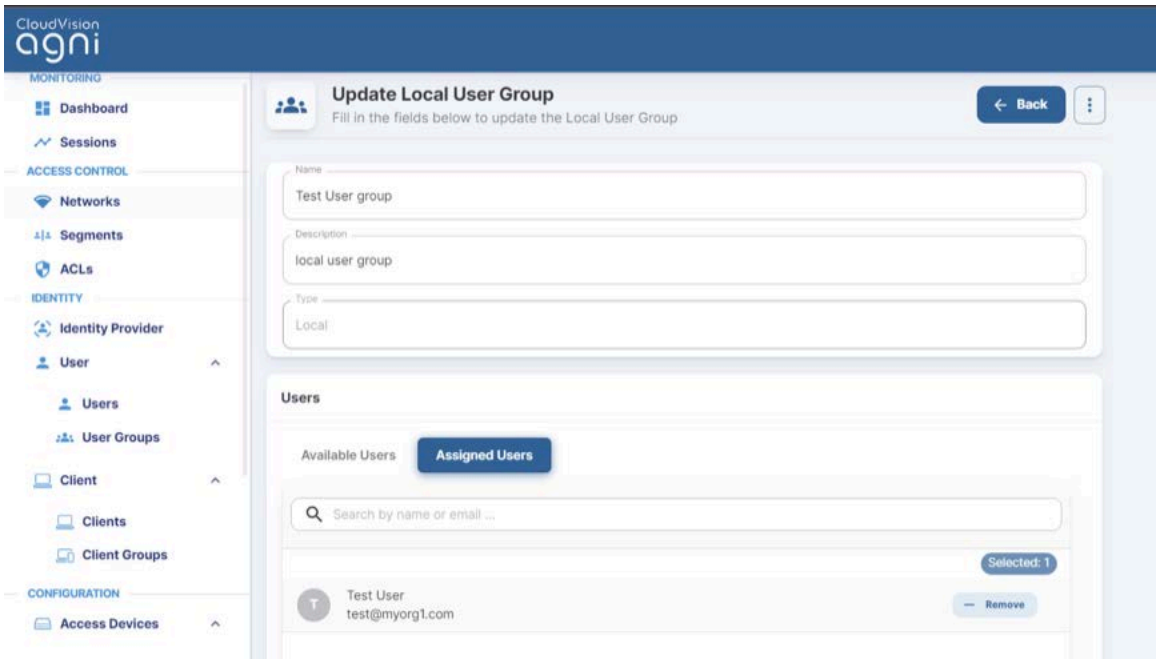
Figure 9-5: External User Groups



9.2.1 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 9-6: Local User Groups

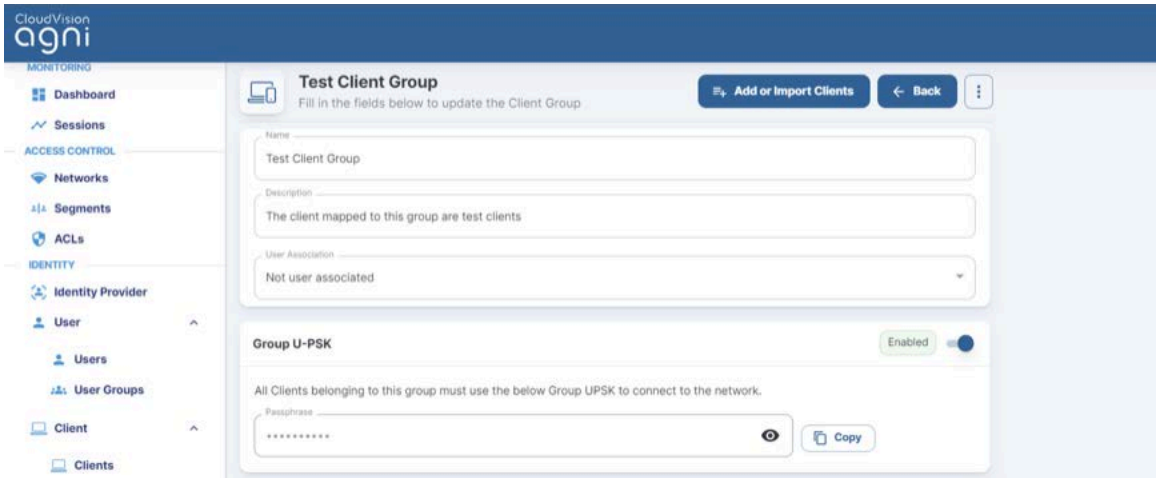


Chapter 10

Client Configuration

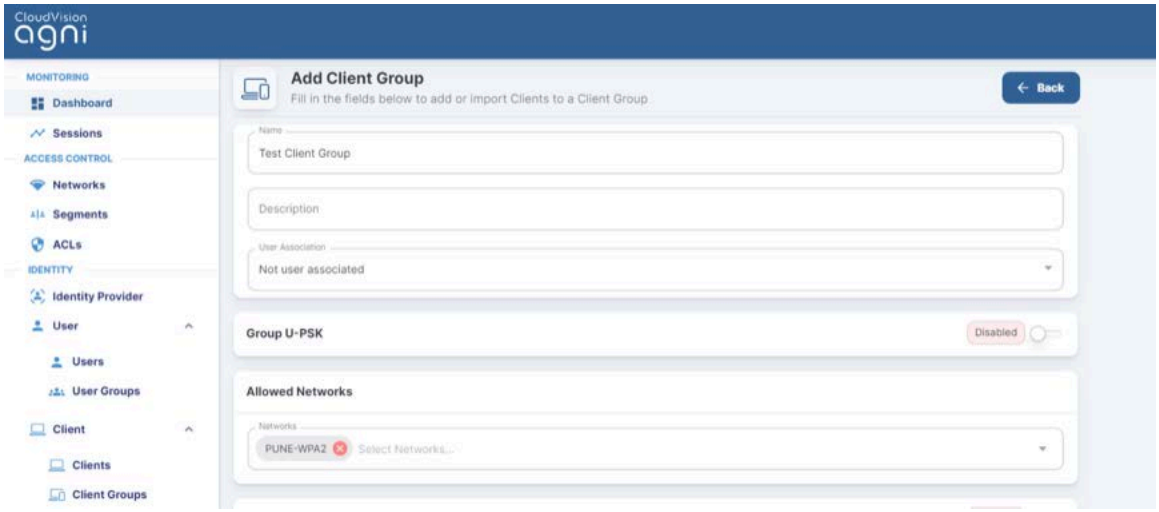
- **Client Groups** - Client Groups manage the client devices that are being authenticated by AGNI. The clients can be added either manually or dynamically by the system.
- **User Association** - The Client Group can either be Not User associated or associated to Onboarding User.
  - **Not User Associated** - 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.

Figure 10-1: Client Group UPSK



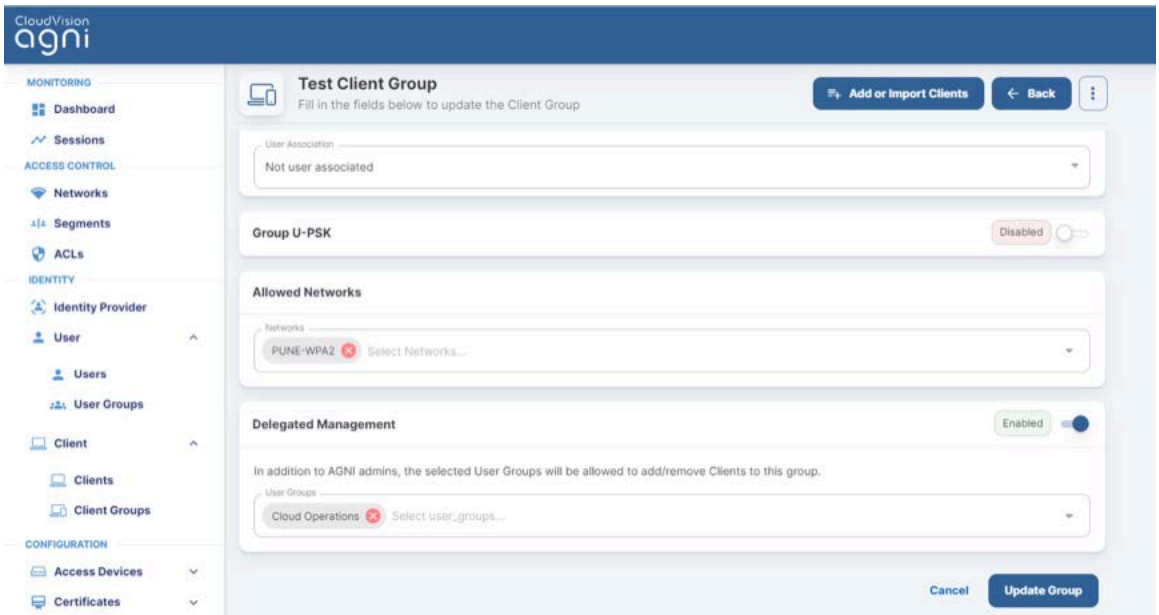
- **Allowed Networks** - The network access to the clients under the group can be controlled by specifying the **Allowed Network** option.

Figure 10-2: Client Group Allowed Network



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

Figure 10-3: Client Group Delegated Management



10.1 Clients

The Clients section captures the endpoints in the following scenarios:

- Dynamically registered clients as part of authentication (e.g., 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.

Figure 10-4: Client Addition

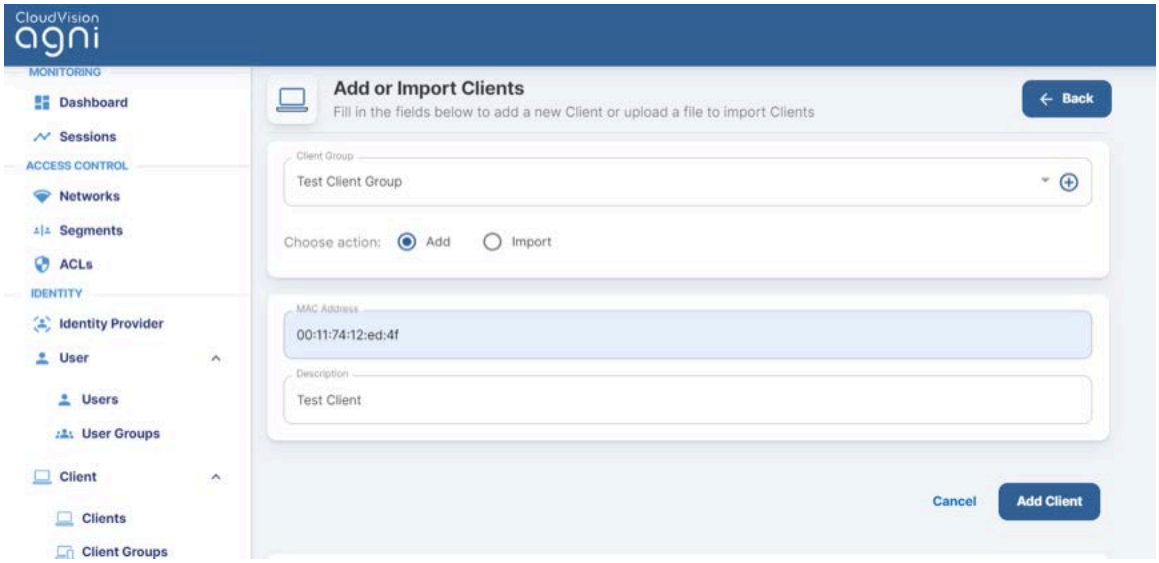
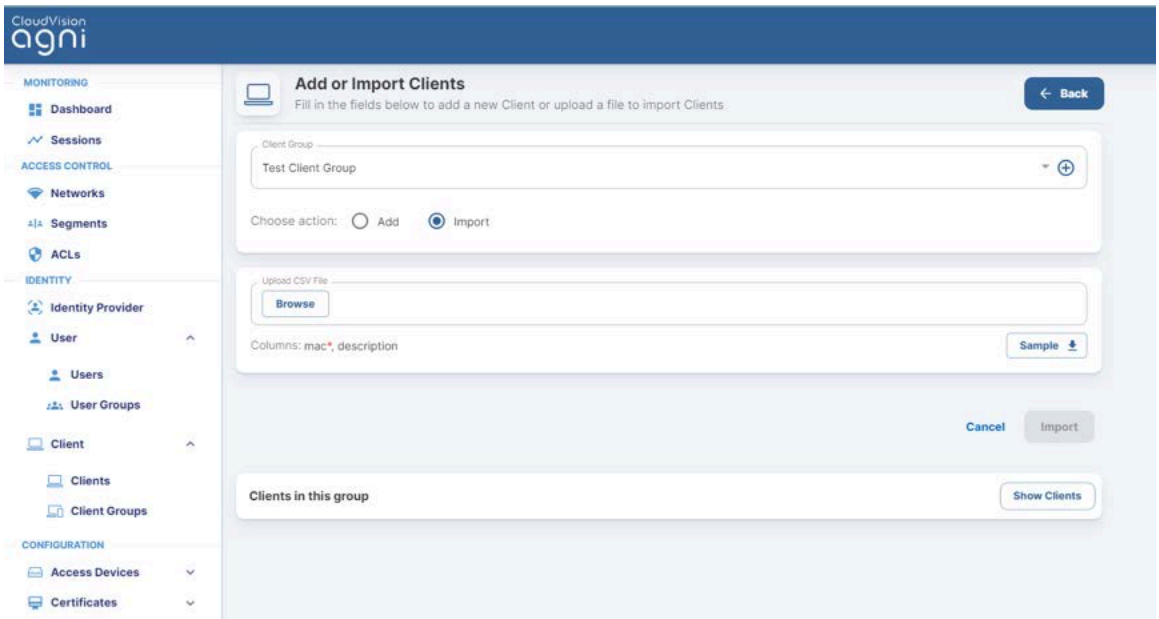


Figure 10-5: Client Import



10.2 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.

Figure 10-6: Client Details

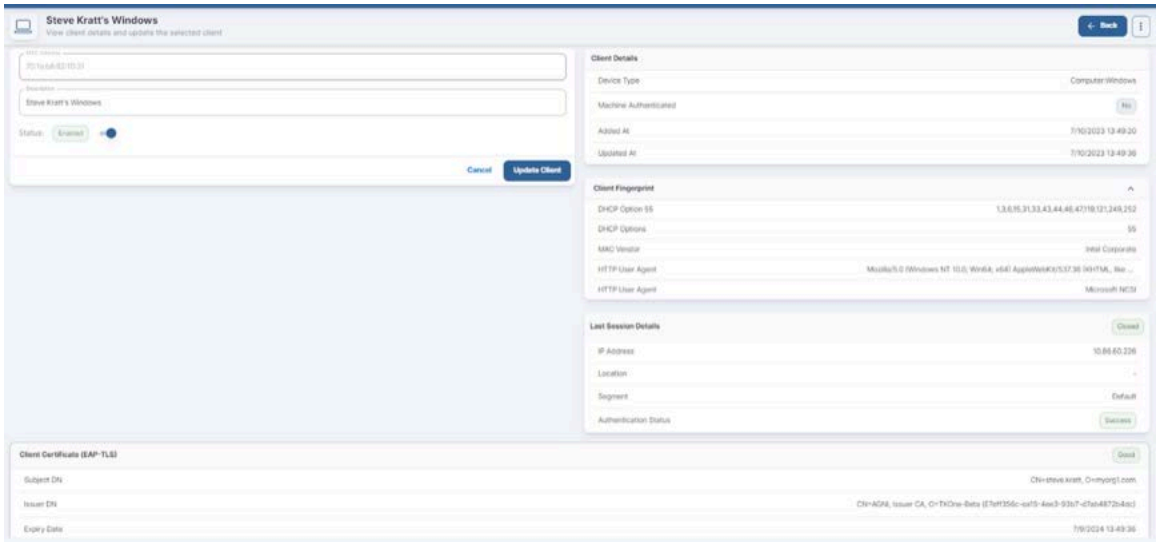
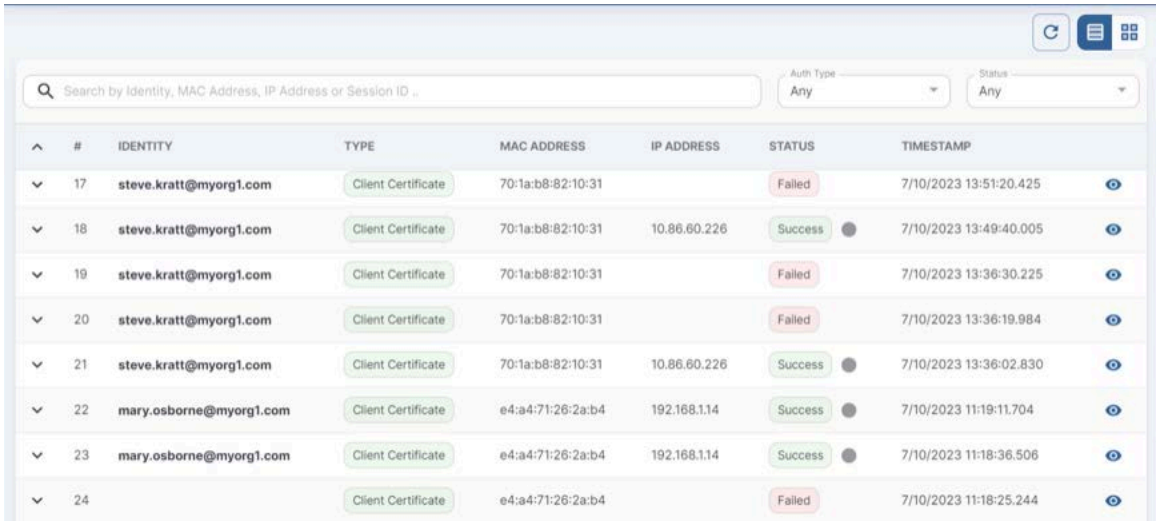


Figure 10-7: Client Sessions



10.3 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.

Prerequisite: 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.

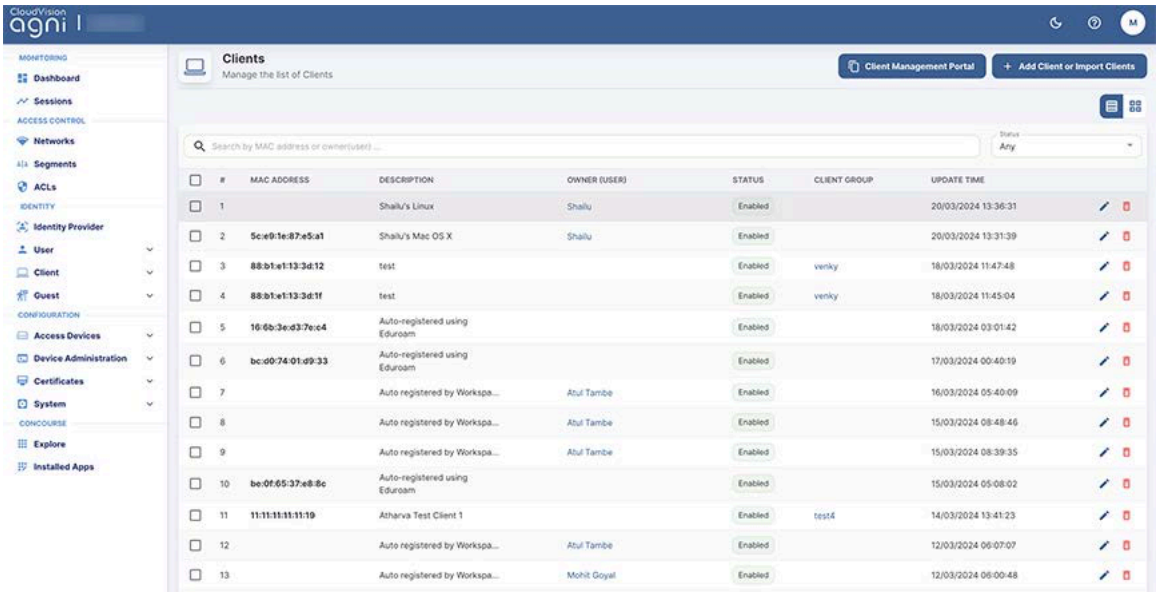
The new certificate is valid for one year from the time the certificate is generated.

> **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, perform the following steps:

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

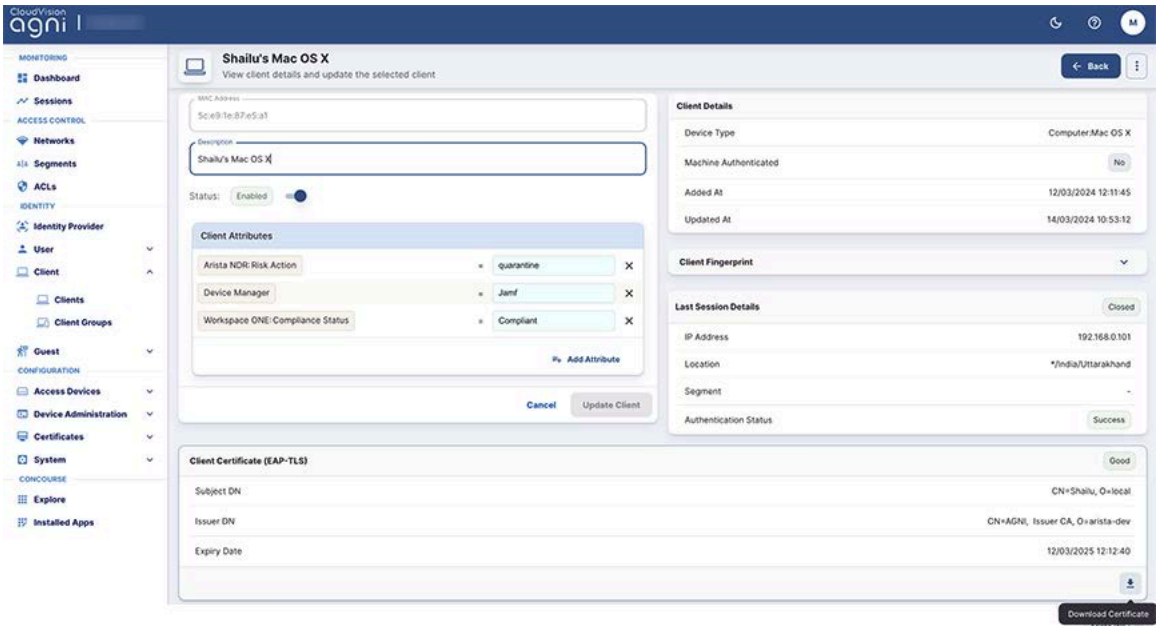
   Figure 10-8: Clients Dashboard



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

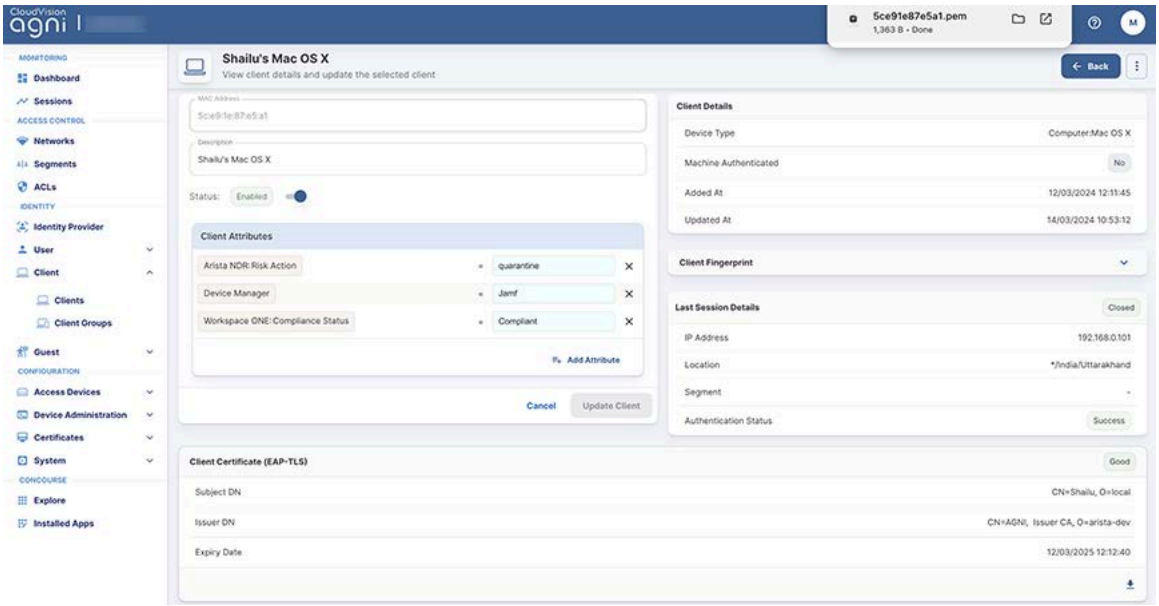
> **Note:** If the client is not present in the client details table, the admin should add the client before generating the client certificate.

Figure 10-9: Select Client



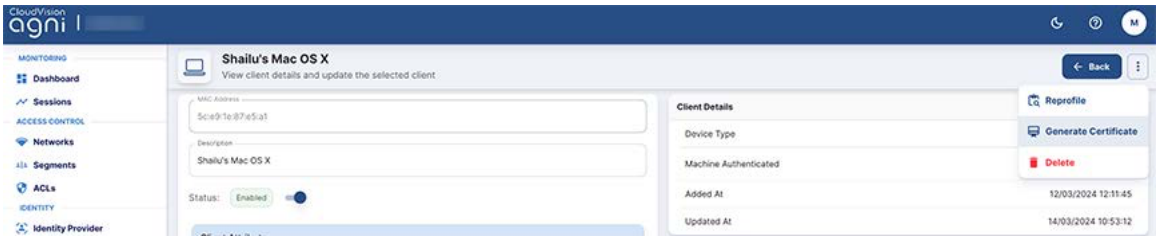
3. Download the certificate by clicking the **Download** button (arrow).
   The X509 certificate (`.pem` file) is saved to the download folder. You can open the file to verify the details.

   Figure 10-10: Download Certificate



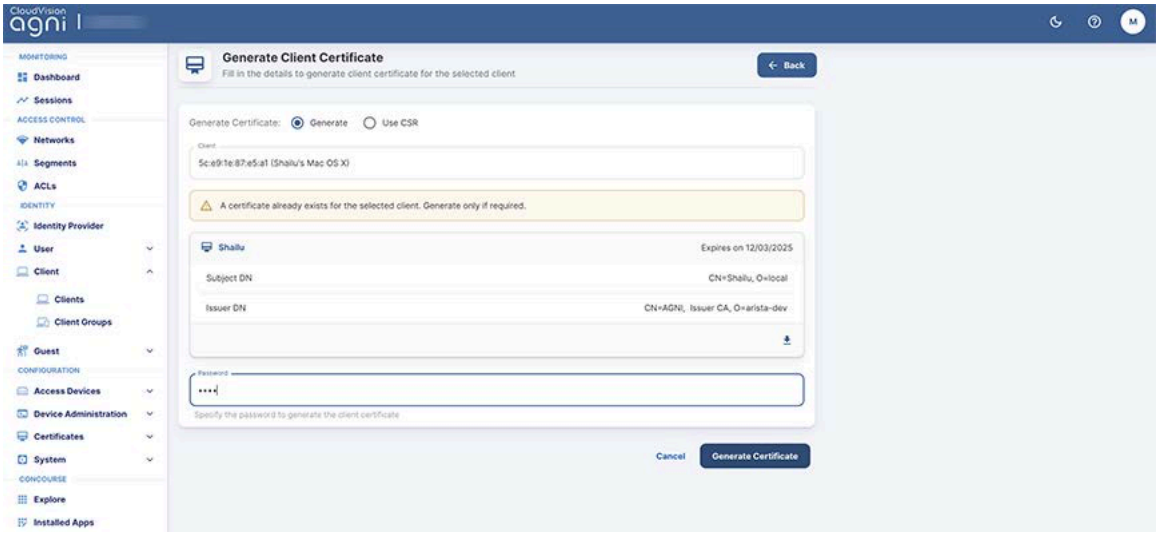
4. You can also generate the certificate using the **Generate Certificate** menu (see image below).

Figure 10-11: Generate Certificate



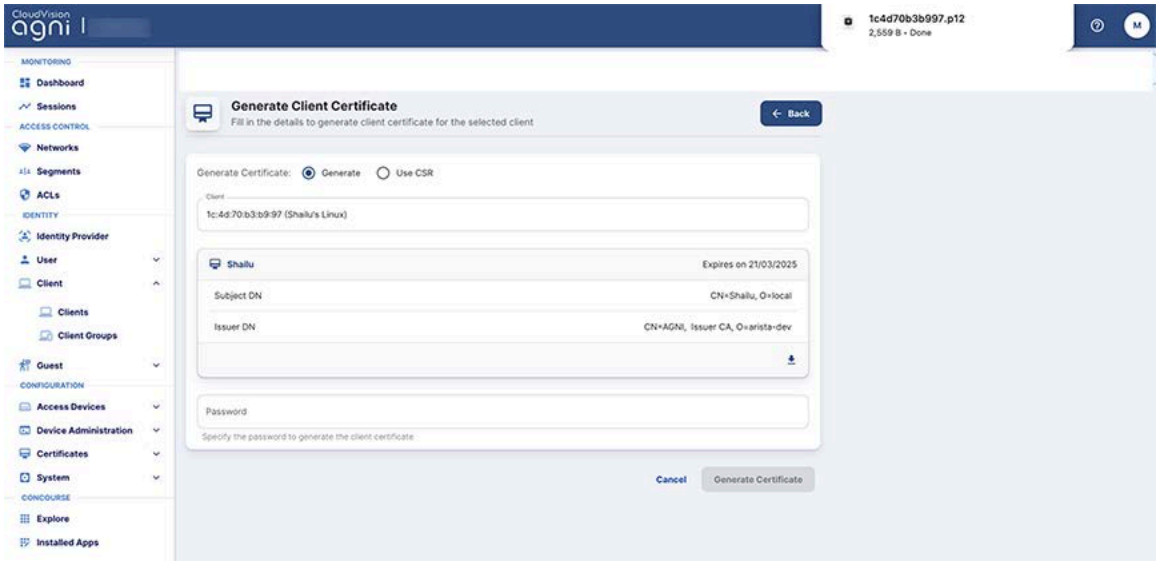
5. Click the **Generate Certificate** menu, select the **Generate** radio button, enter a password (save the password for future reference), and click the **Generate Certificate** button (see image below).

Figure 10-12: Certificate - Generate Radio Button



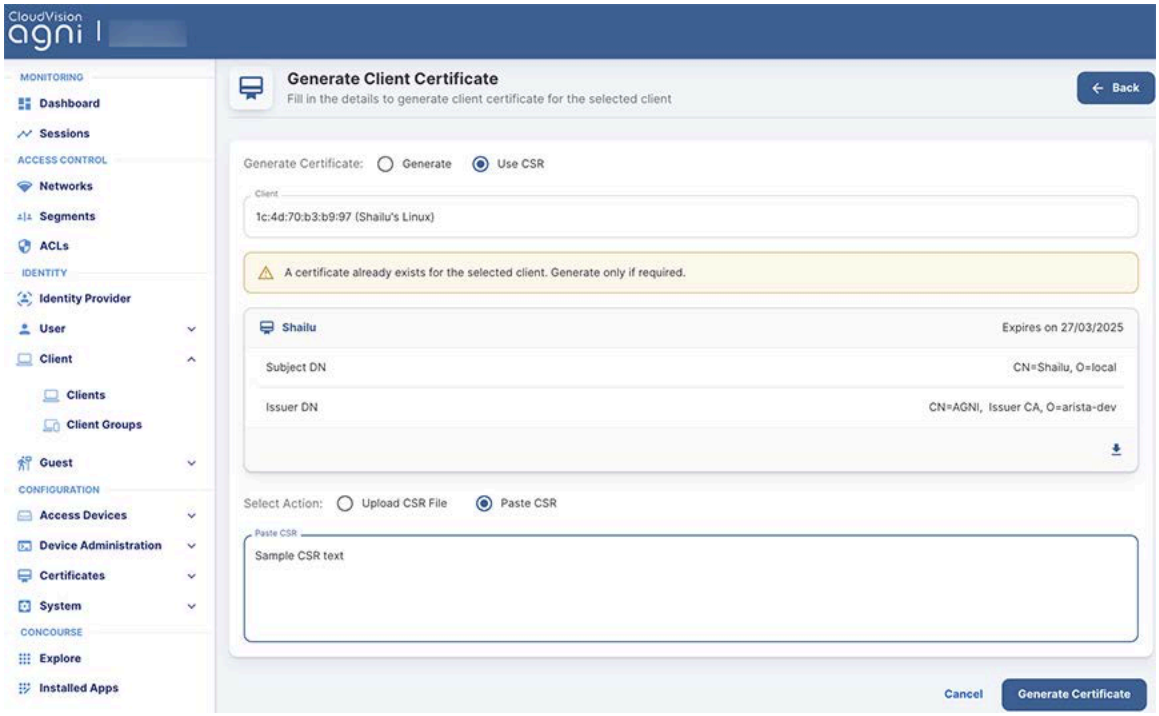
The new certificate is downloaded to your system. The updated page displays the new certificate expiry date (one year from the date of generating the certificate). See the image below.

Figure 10-13: Certificate Added



- 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.

Figure 10-14: Certificate - Use CSR Radio Button



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

Chapter 11

Guest Onboarding Features

The Guest Onboarding topics include:

11.1 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.

11.1.1 Guest User in AGNI

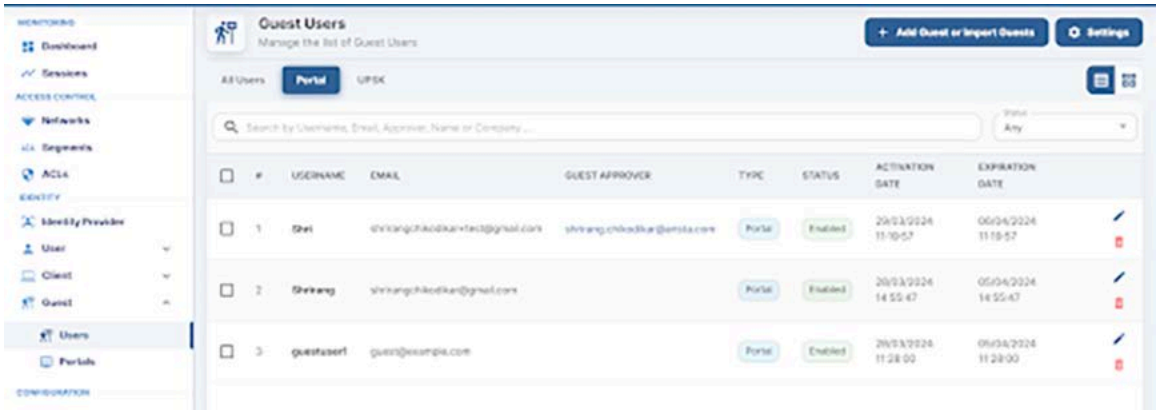
AGNI supports the following user categories to provide the guest onboarding experience:

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

11.1.1.1 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.

Figure 11-1: Guest Users

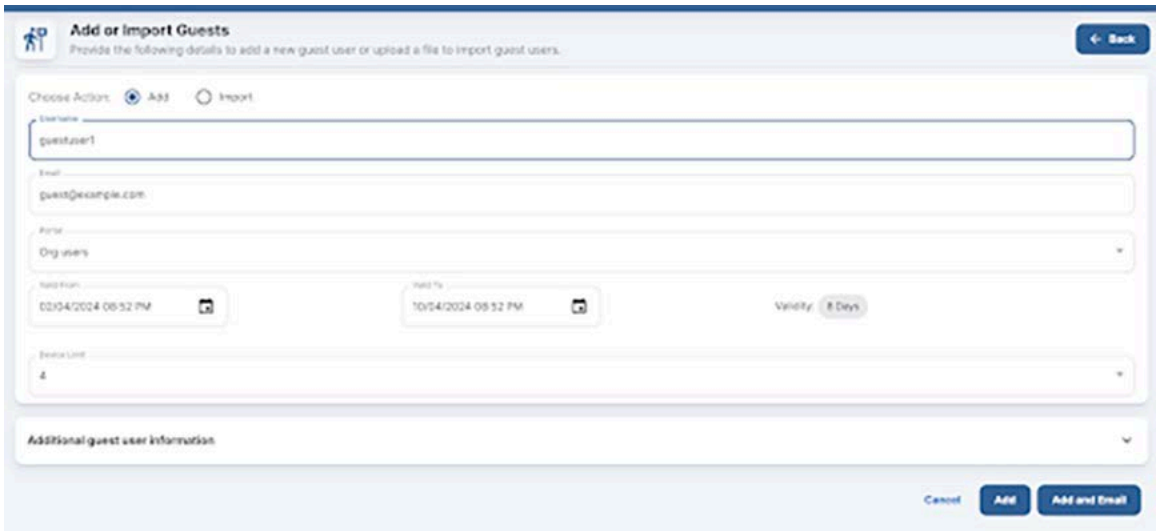


The admin or guest operator can add portal users and share their credentials with the guests in advance. To add the portal users, navigate to **Identity** > **Guest** > **Users**. The guest operator must log into the Self-Service Portal and navigate to **Guests** > **Users**.

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.

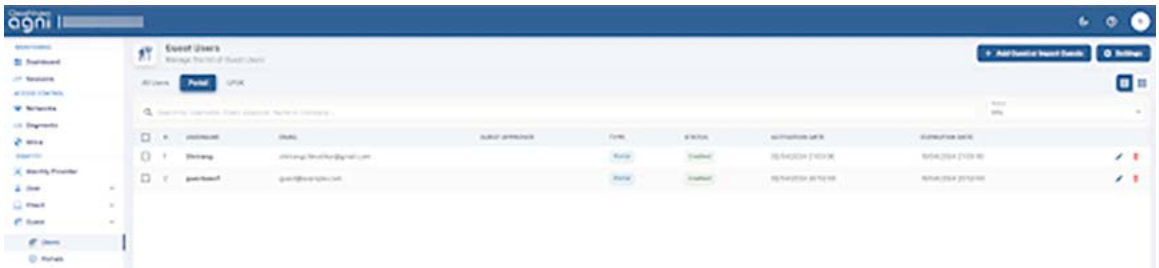
Figure 11-2: Add or Import Guests



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.

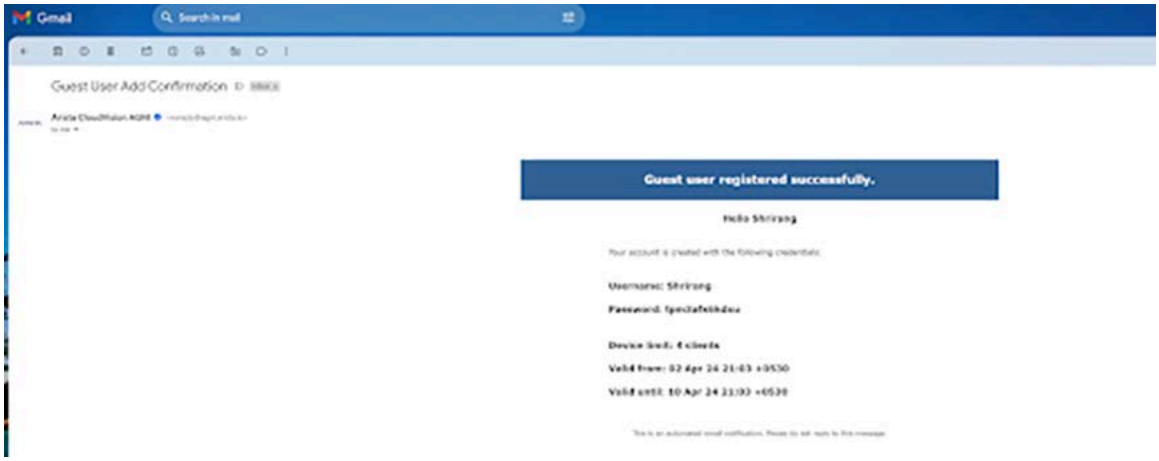
Once the portal user is added, it gets displayed in the Portal User listing.

Figure 11-3: Guest Users List



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

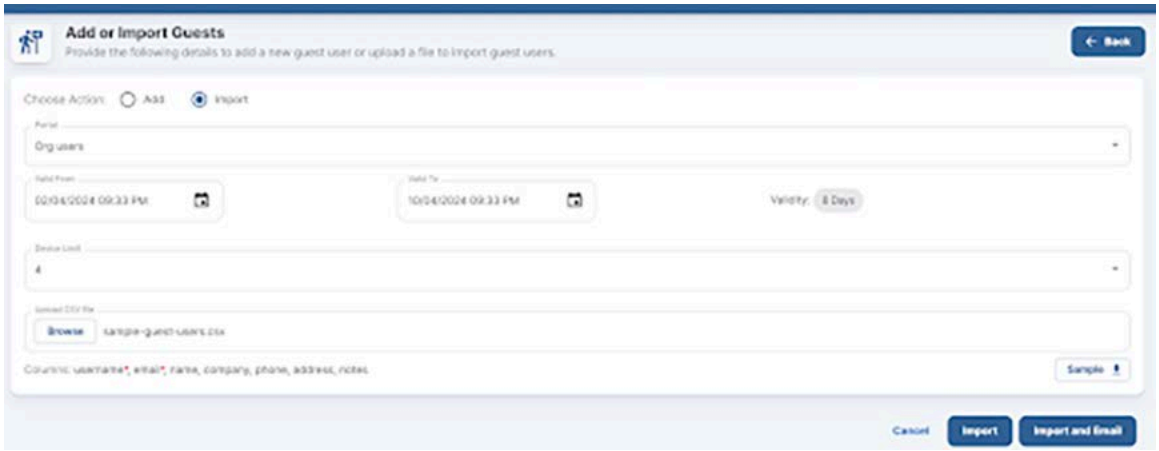
Figure 11-4: Sample Email for New Portal User



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

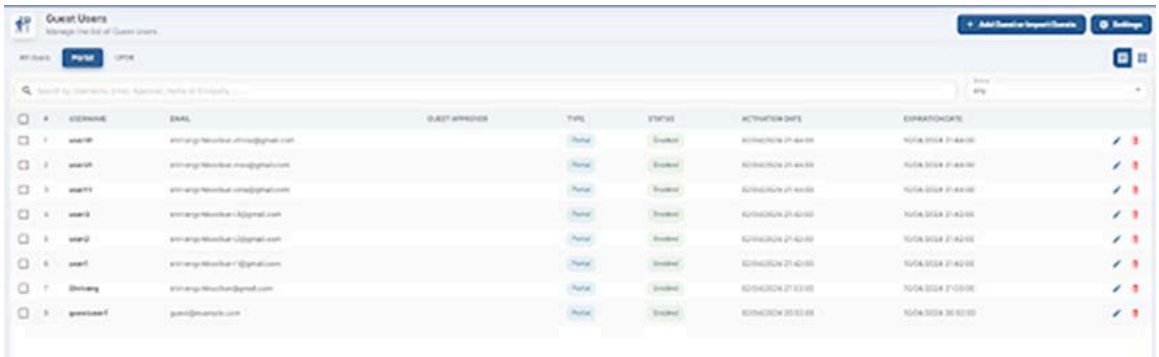
Admin/guest operators can also add portal users using the Import option. In this flow, the admin/guest operators must import the CSV file in a certain format. See the sample CSV file.

Figure 11-5: Sample CSV File



The imported users are listed in the portal user listing.

Figure 11-6: Portal User List



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.

11.1.1.2 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.

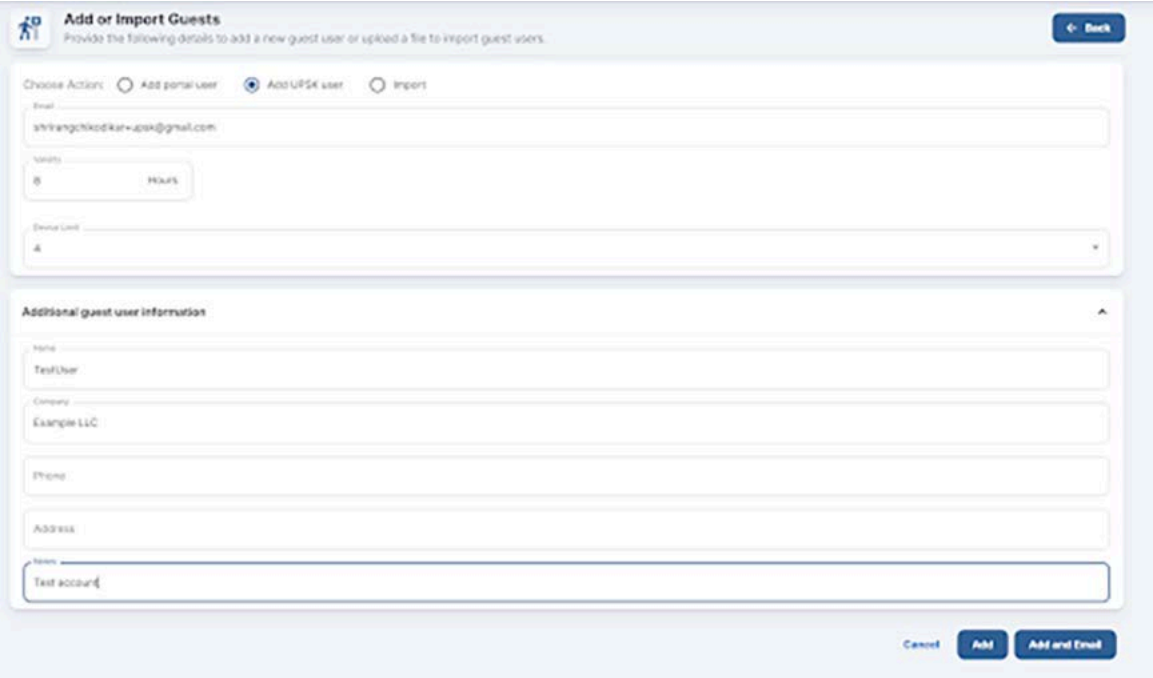
To add UPSK users, the Guest Operator must log in to the self-service portal and:

1. Navigate to **Guest** > **Users** > **UPSK**.
2. Click the **Add Guest** or **Import Guest** button.

3. 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.

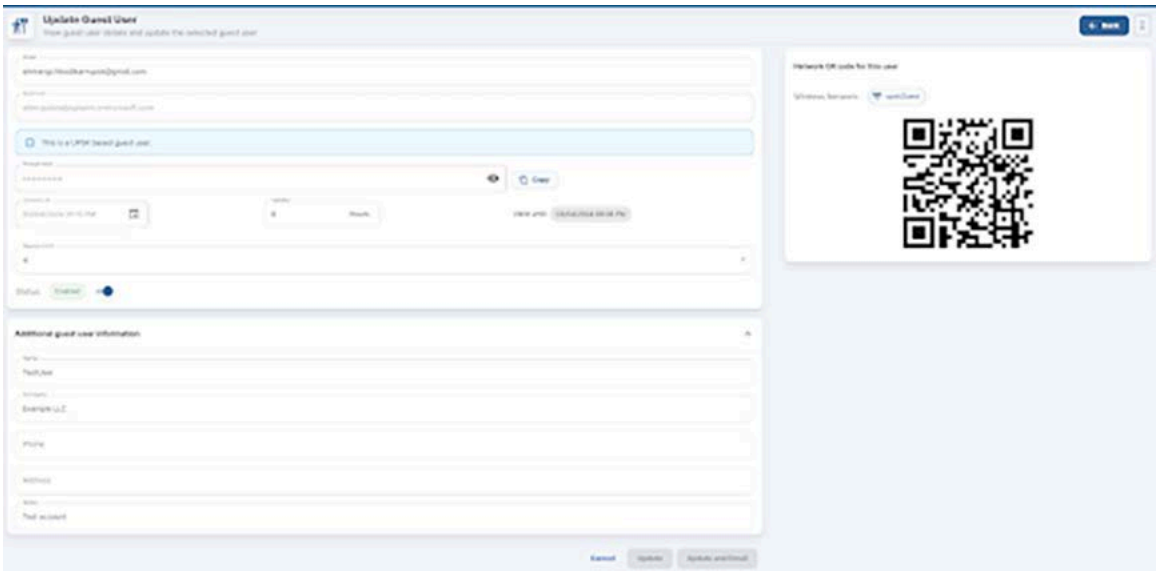
> **Note:** A UPSK network allowing UPSK guests is mandatory for adding UPSK users.

Figure 11-7: Add or Import UPSK Users



4. 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.

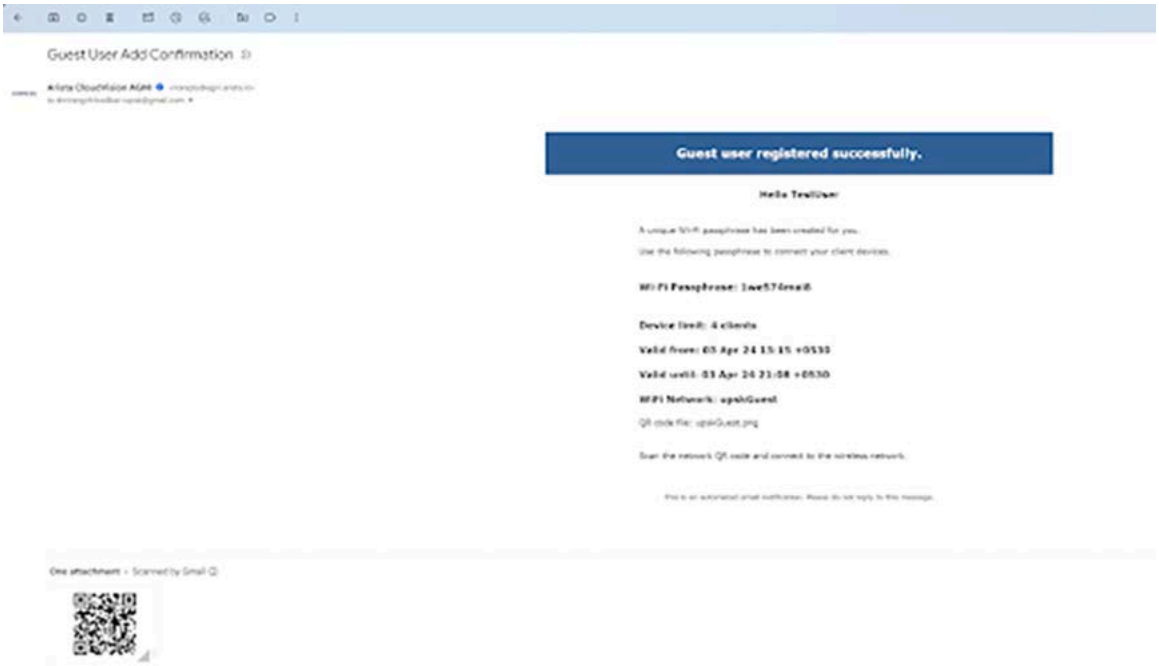
Figure 11-8: UPSK User Details



5. 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.

Figure 11-9: Guest User Registered Successfully

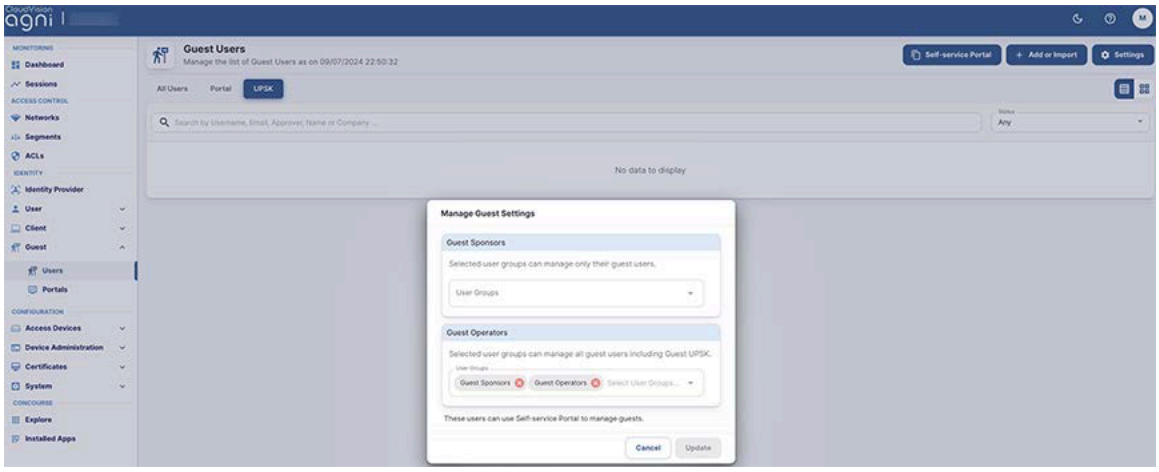


11.1.1.3 Guest Operator

Guest Operators are users who belong to a specified user group. They have the permissions 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.

Figure 11-10: Manage Operator Settings



11.1.1.4 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.

11.2 Guest Onboarding Offerings in AGNI

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

11.2.1 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:

11.2.1.1 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, perform the following steps:

1. Navigate to **Identity** > **Guest** > **Portals**.
2. Choose the **Authentication Type** as either **Clickthrough** or **Guestbook**.
3. **Enable** the CAPTCHA knob.
4. Preview the CAPTCHA, which is displayed on the right side.

5. Click the **Add Guest Portal** button to save the configuration.

Figure 11-11: Enable CAPTCHA

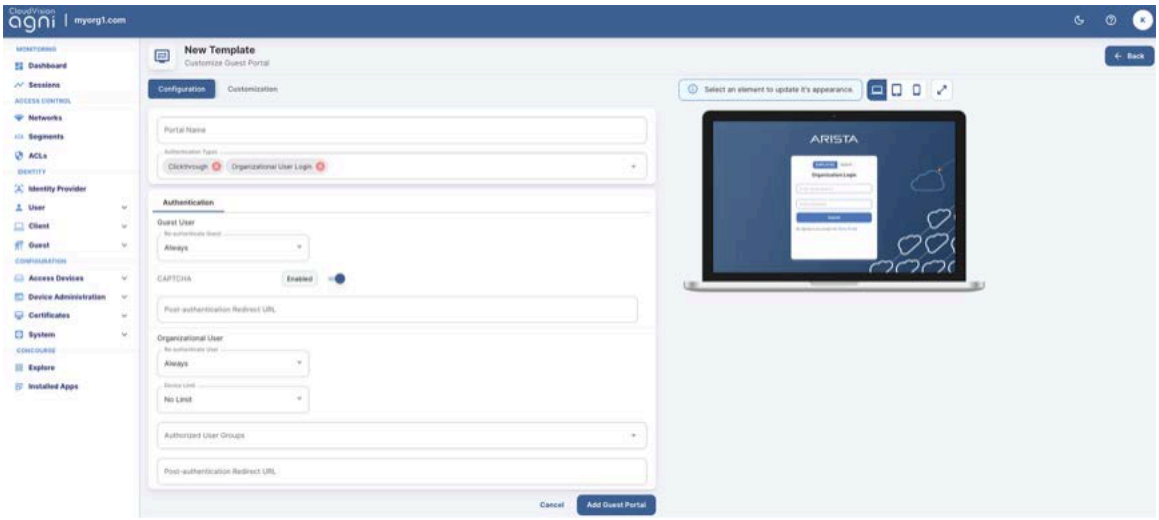
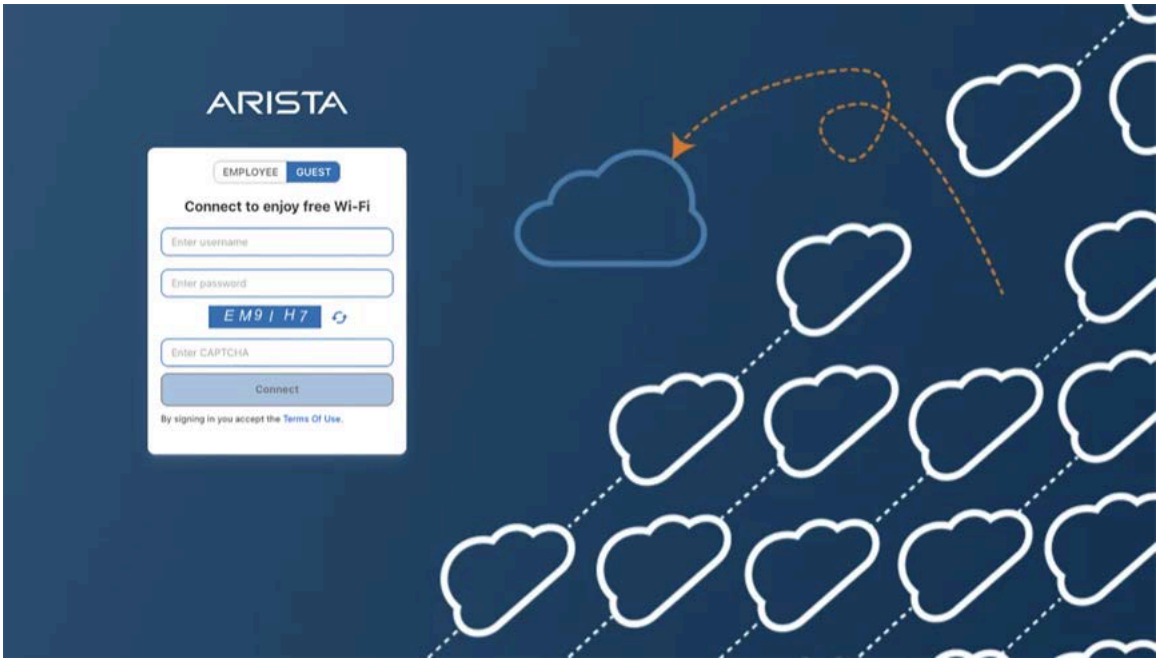


Figure 11-12: Guest Login



11.2.1.2 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 redirect URL, 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, perform the following steps:

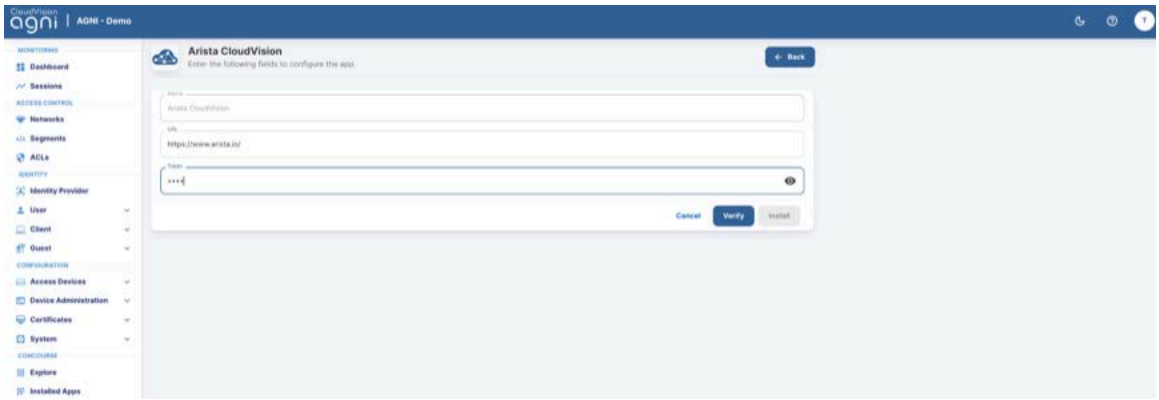
1. Navigate to **Identity→Guest→Portals**.

2. Select the **Guest Portal** for which you want to configure the redirect URL.
3. Enter the URL in the **Post-authentication Redirect URL** field.
4. 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 redirect URL may or may not be visible after successful portal authentication because the Android CNA transitions to connected state very quickly.

Figure 11-13: Redirect URL

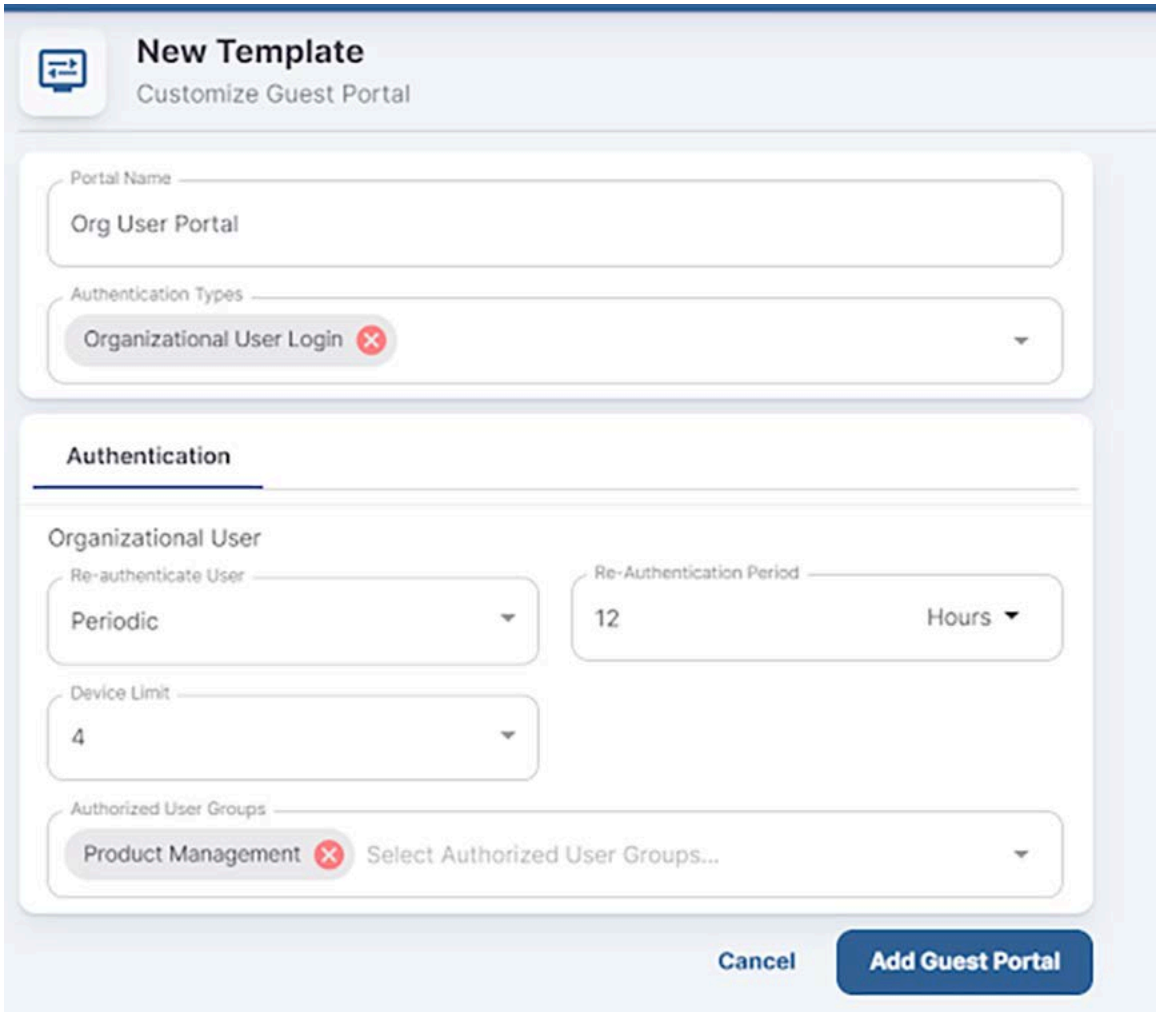


11.2.1.3 Organizational User Login

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

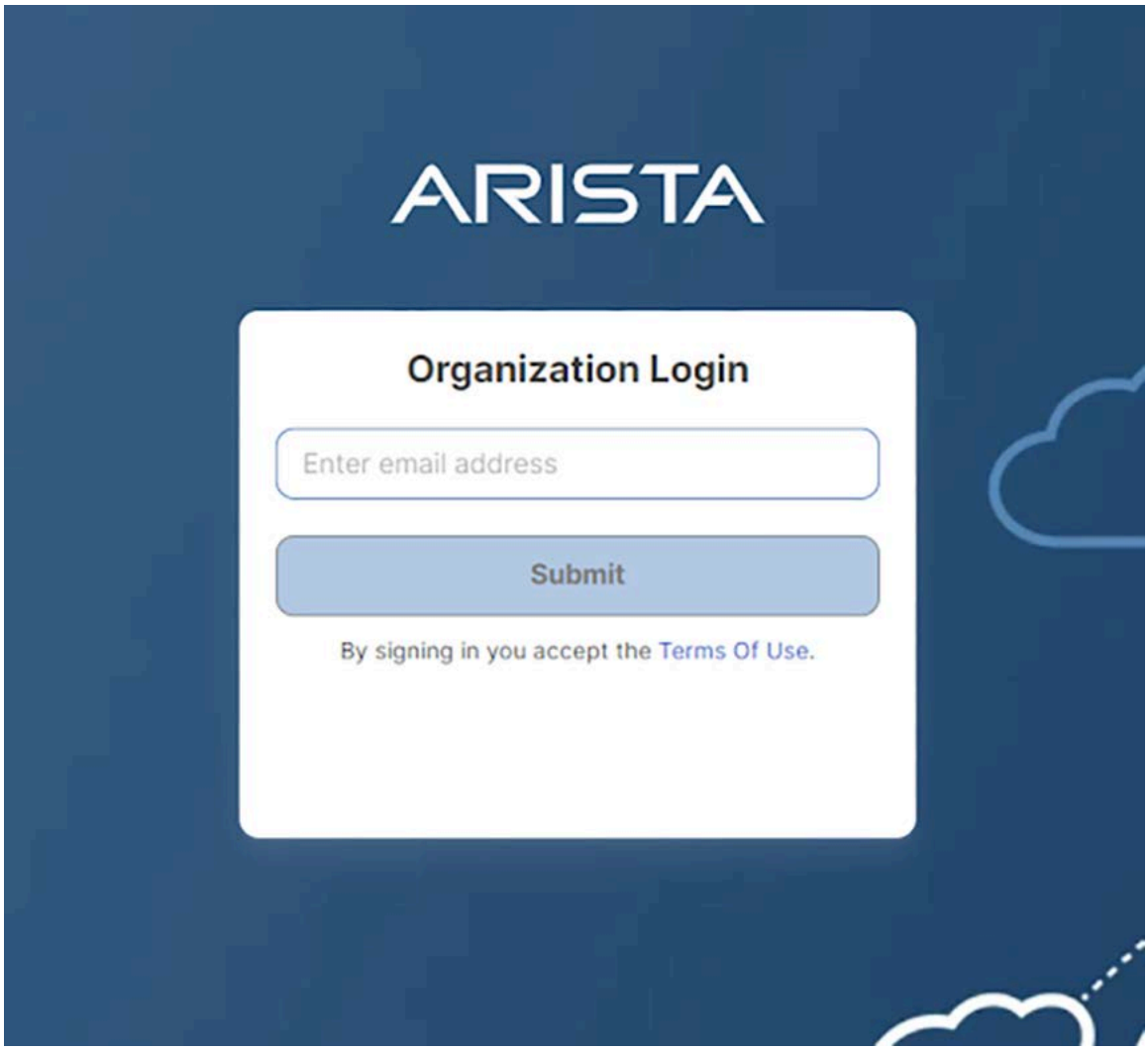
users and the rest are rejected access. The admin can configure the re-authenticate method and device limit for the guest users. The sample configuration for this portal-based onboarding method is as follows:

Figure 11-14: Organizational User Login Configuration



See the sample portal below:

Figure 11-15: Organizational User Login Portal



11.2.2 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.

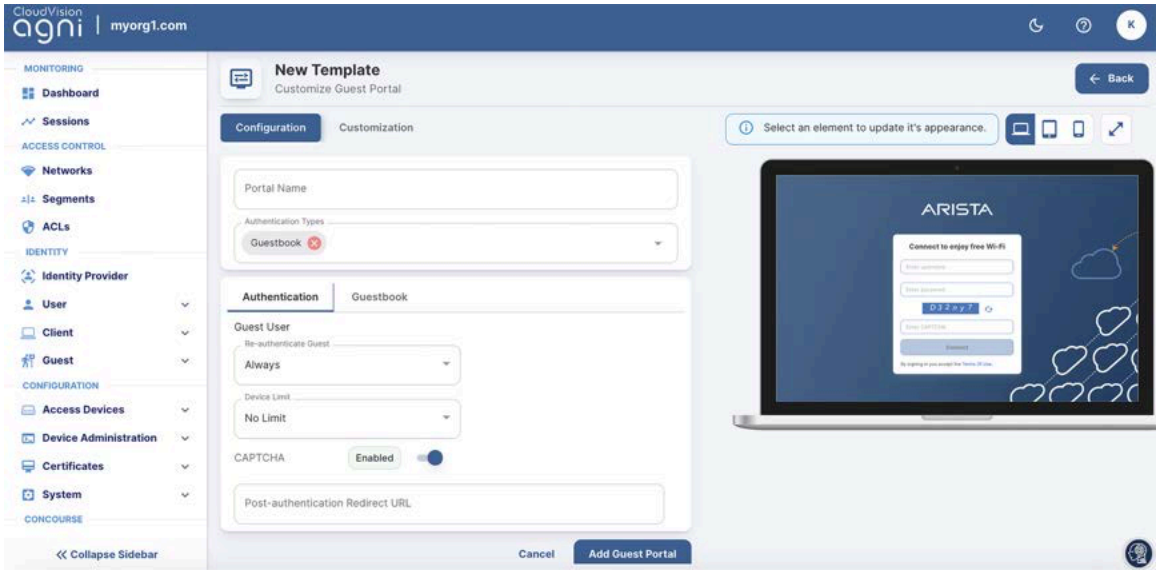
11.2.2.1 Guestbook Method

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.

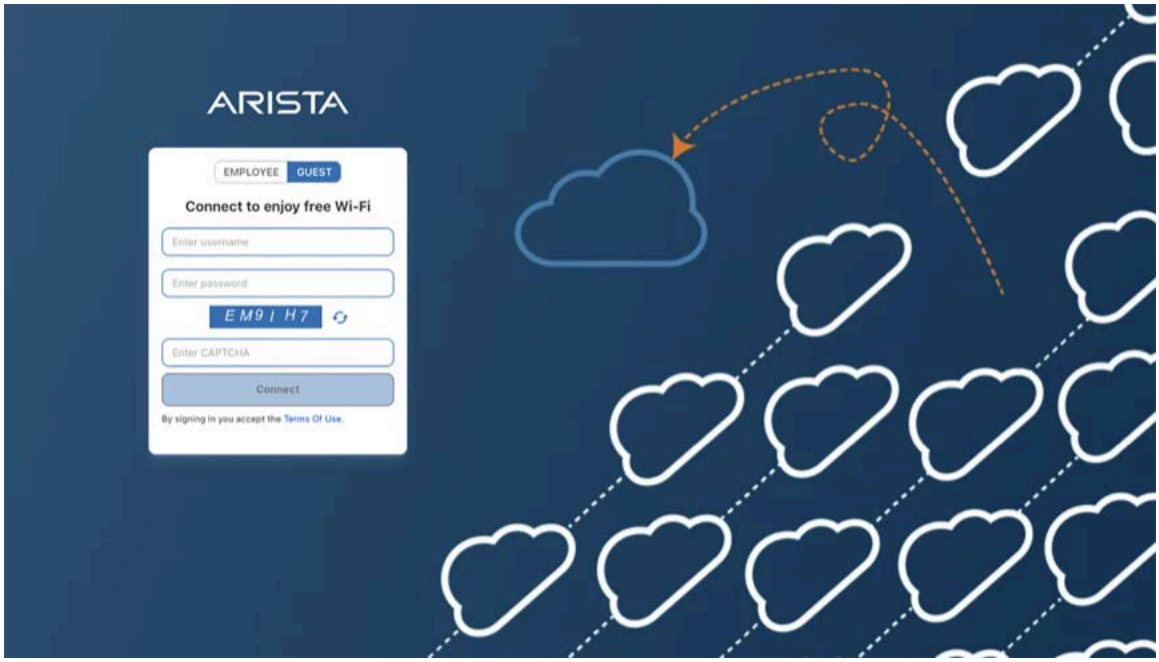
Below is the screenshot of a sample configuration of the guestbook method:

Figure 11-16: Guestbook Configuration



The sample portal is as follows:

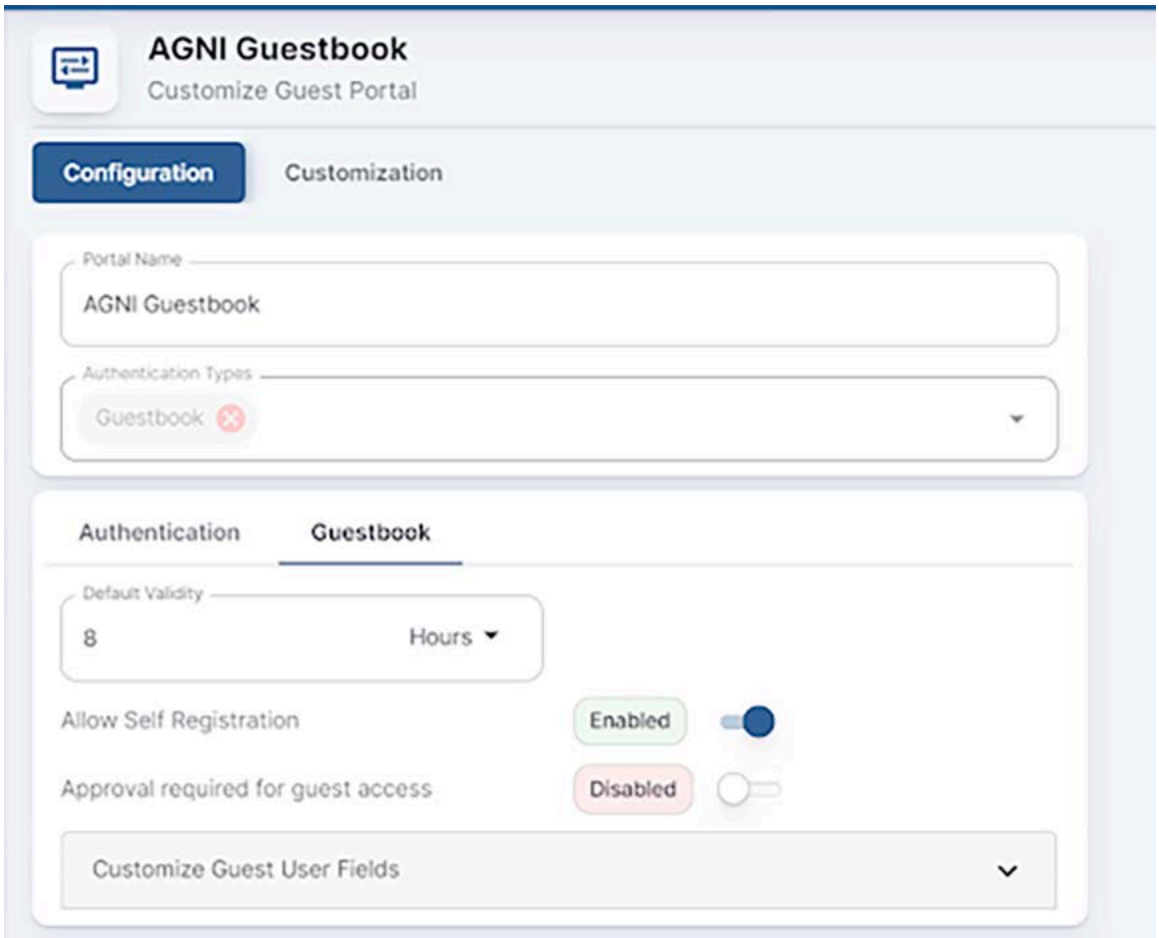
Figure 11-17: Guestbook Login Portal



11.2.2.2 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:

Figure 11-18: Enable Self Registration

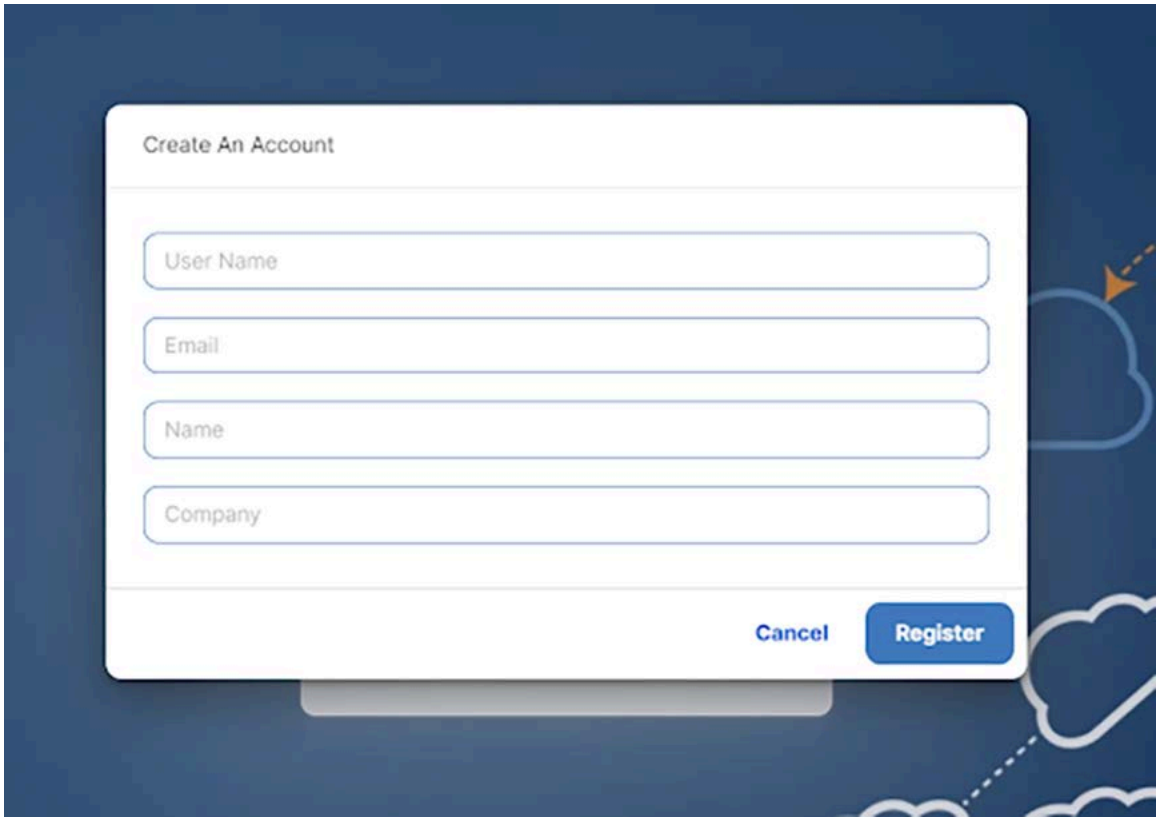


Below is a sample portal:

Figure 11-19: Self Registration Login 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. Below is a sample form:

Figure 11-20: Create an Account



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.

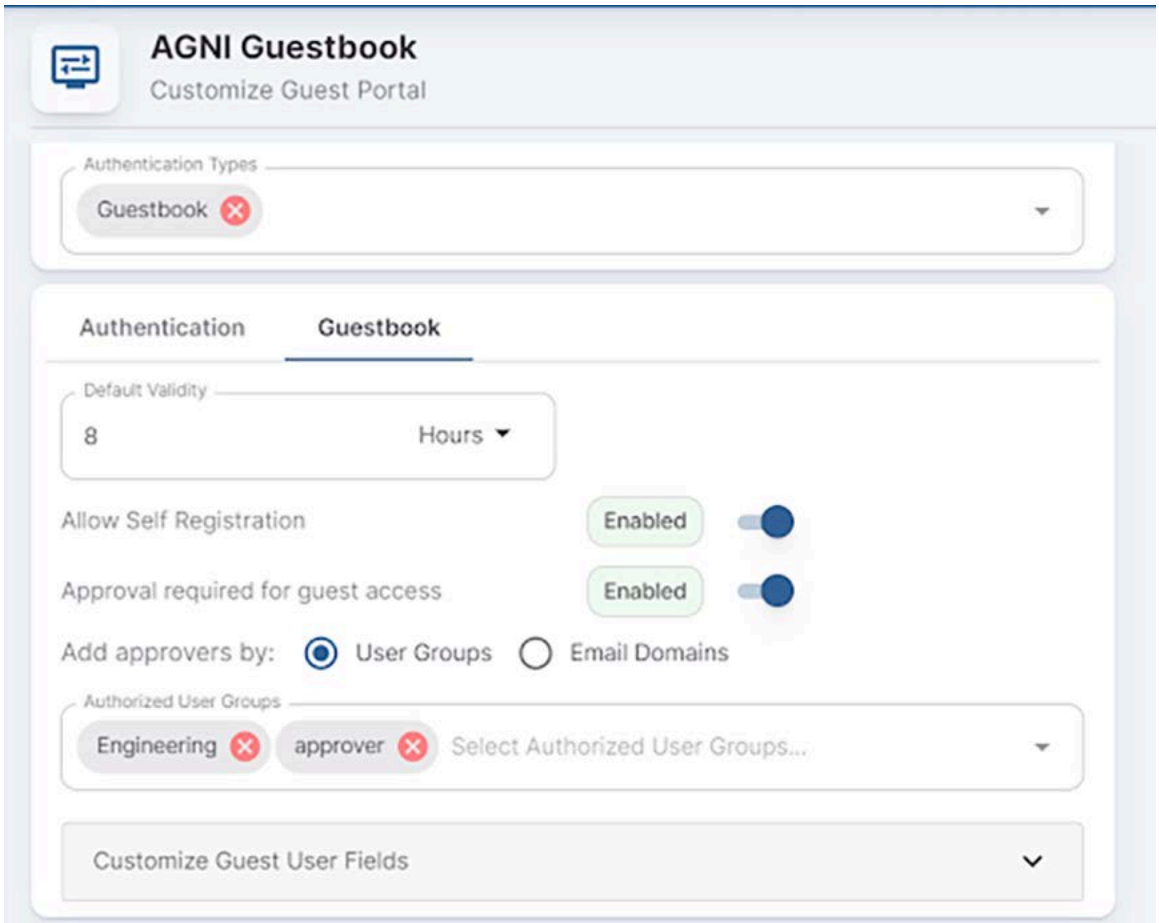
Guests can use these credentials to log into the portal.

11.2.2.3 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:

Figure 11-21: Host Approval Configuration



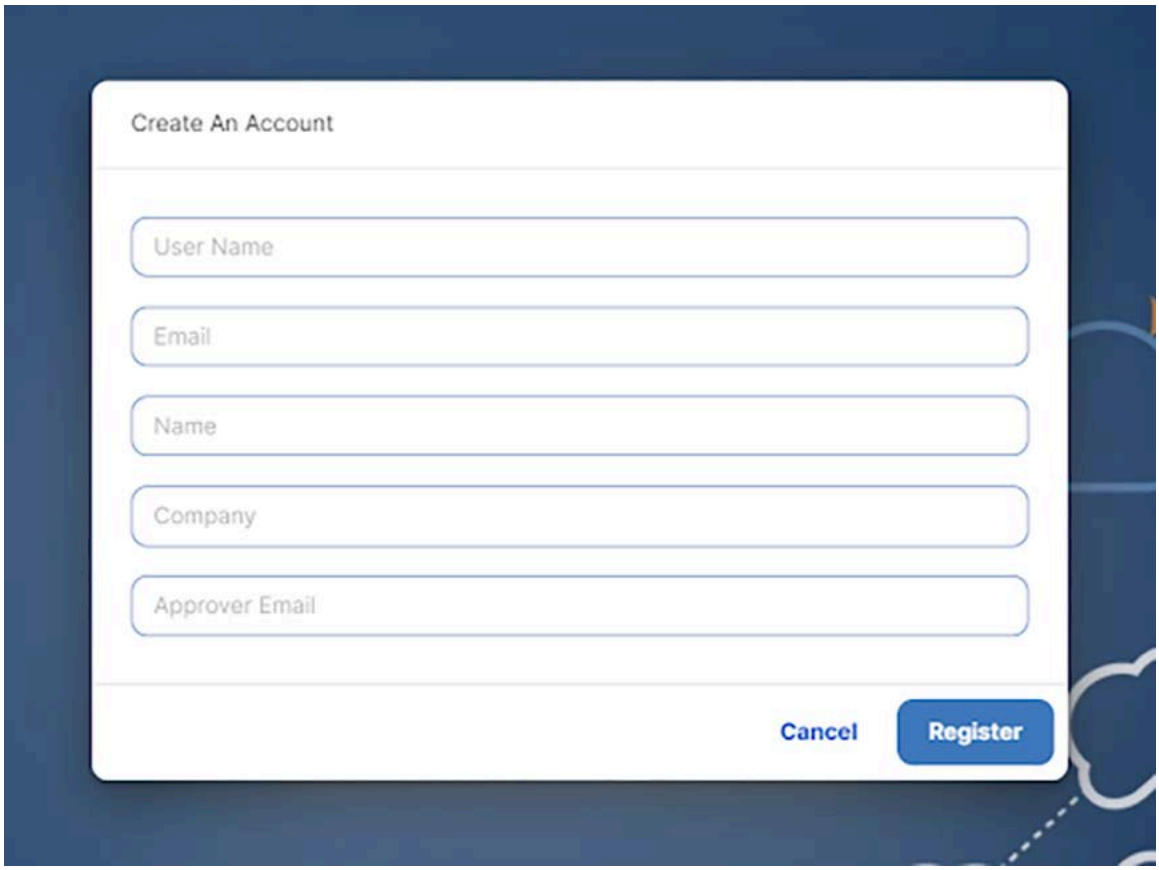
Below is a sample portal:

Figure 11-22: Host Login 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.

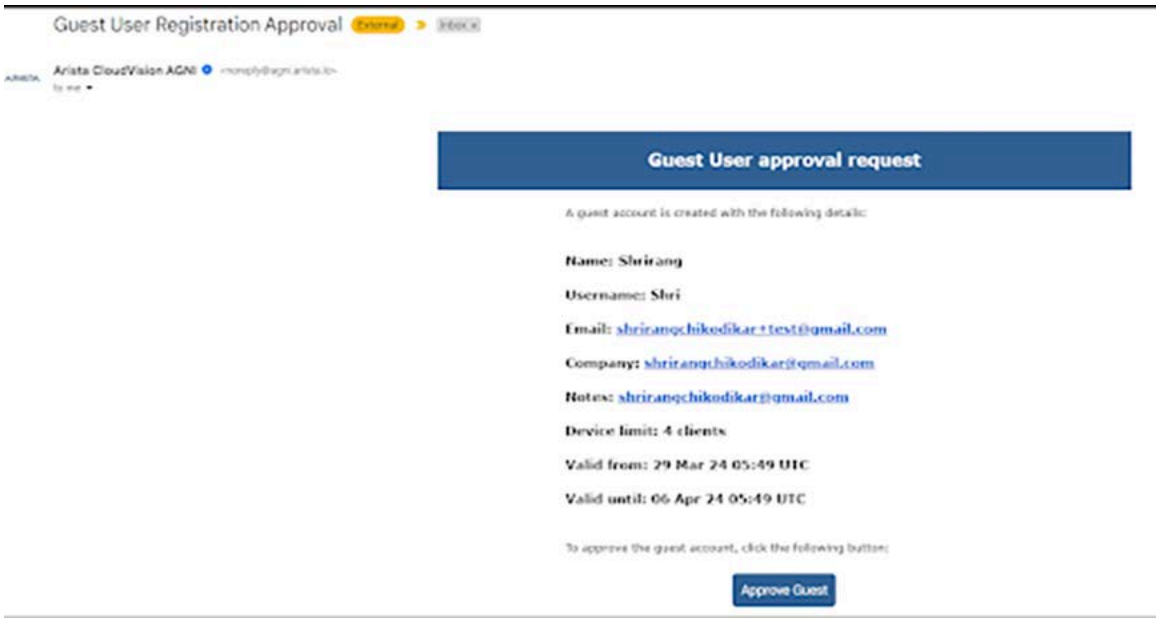
Following is a sample form:

Figure 11-23: Create an Account



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

Figure 11-24: 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.”

11.2.3 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.

11.3 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.

11.3.1 Configuring AGNI

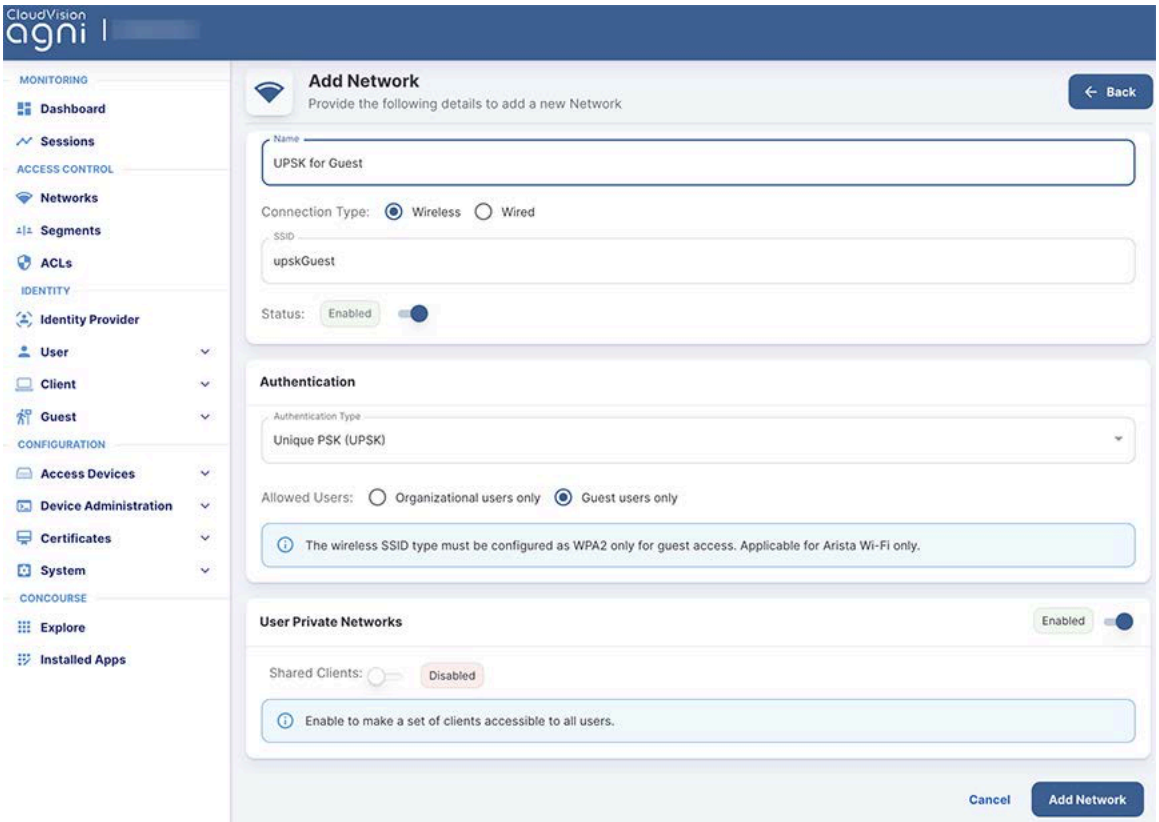
Perform the following steps:

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**
      1. **Authentication Type** - **UPSK**
      2. **Allowed Users** - **Guest Users Only**
      3. **User Private Network** - **Enabled**

4. **Shared Clients - Disabled**

3. Click the **Add Network** button.

Figure 11-25: Add Network



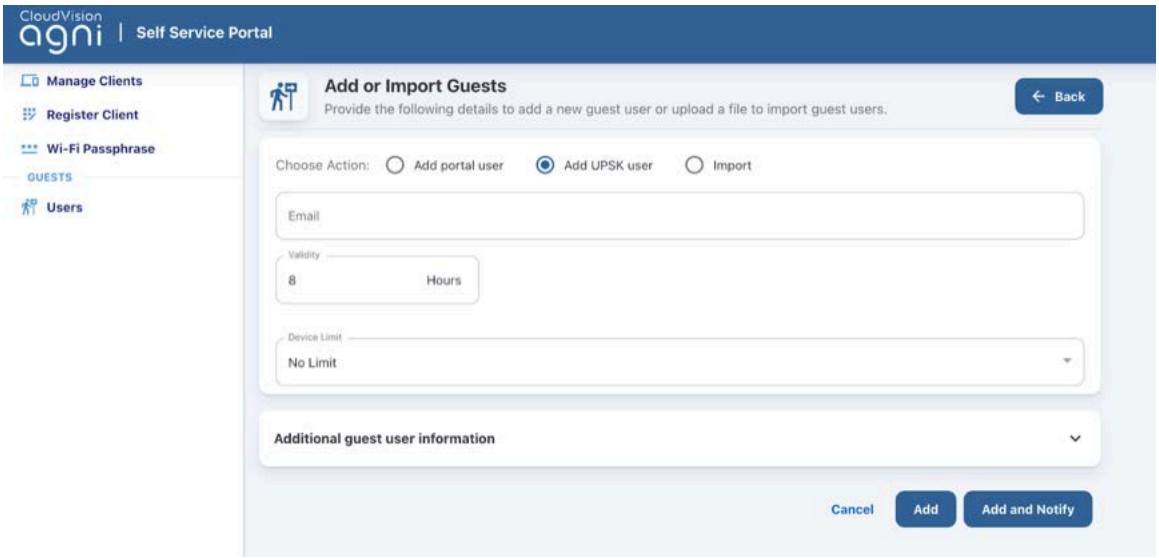
4. Login to the self-service portal with a guest operator user group access.

> **Note:** You must be part of the **Guest Operator** access group to make these configuration changes.

5. Navigate to **Guests** > **Users** from the left side panel.
6. Click the **Add or Import Guest** option to add a UPSK guest.

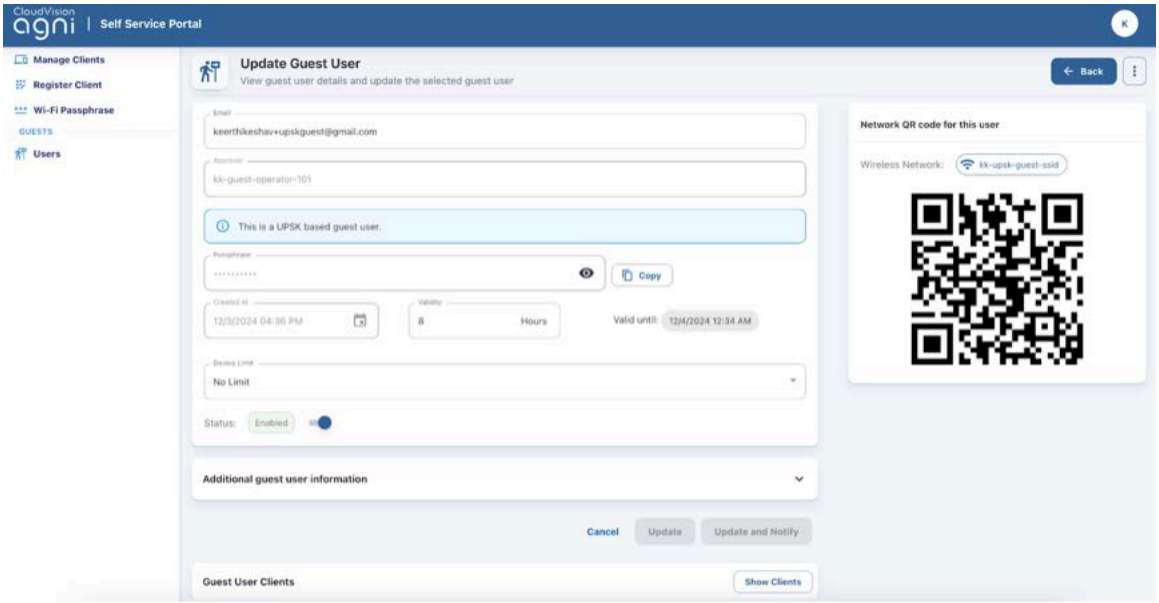
7. Select the **Add UPSK** user option.

Figure 11-26: Add UPSK User



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.

Figure 11-27: Update Guest User



The following is an example of the email received:

Figure 11-28: Guest Account Registration Success

11.3.1.1 General Behavioral Guidelines

For WPA2 + UPSK client registrations:

- **Unregistered Clients:** Client or user machine can connect directly to USPK 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.

11.3.2 Configuring CV-CUE

1. Login to CV-CUE and navigate to **Configure** > **WiFi**.
2. Add a **WLAN** profile with the following settings:
   a. **SSID Name** - upskGuest
   b. **Security** - **WPA2 + UPSK**

c. **Access Control**

1. **Radius Settings - RADIUS or RadSec enabled**
2. **Authentication Server**
3. **Accounting Server**
4. **CoA - Enable**

Figure 11-29: Configure WiFi UPSK Guest

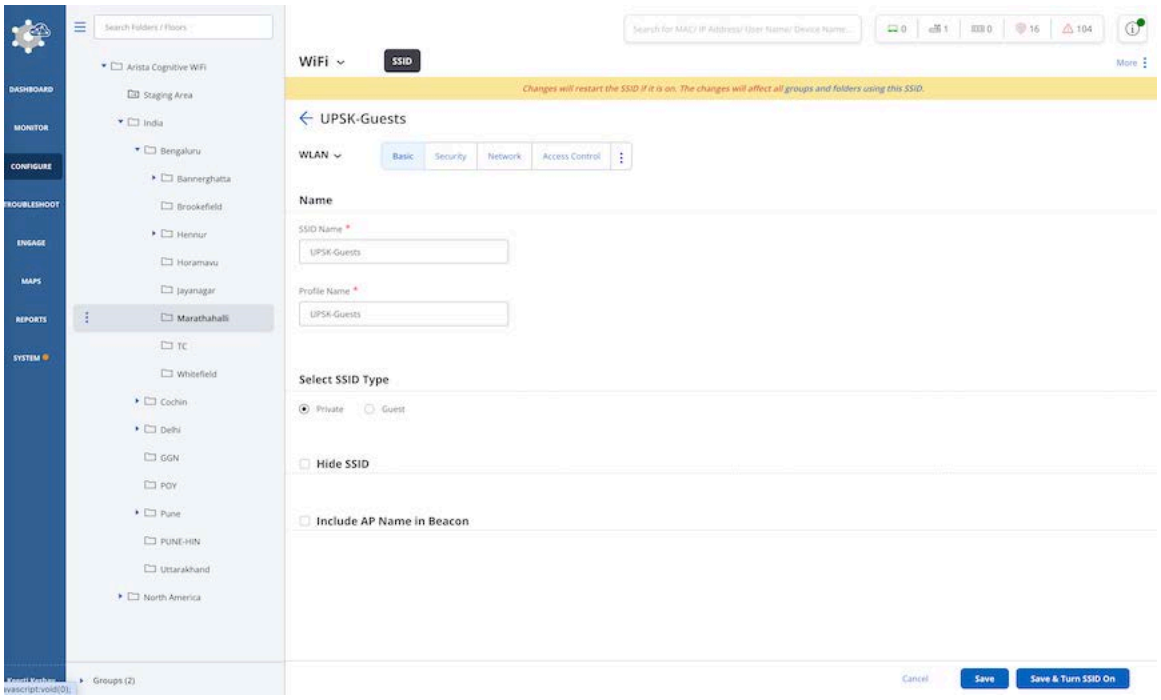


Figure 11-30: WiFi Security

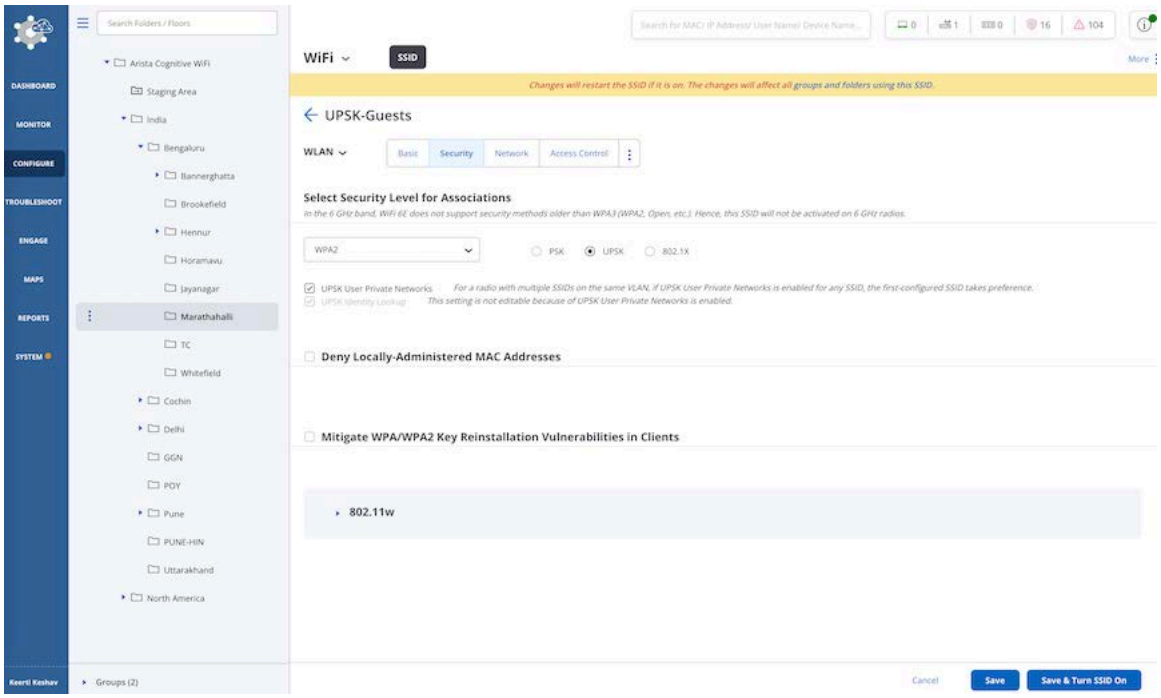


Figure 11-31: WiFi Access Control

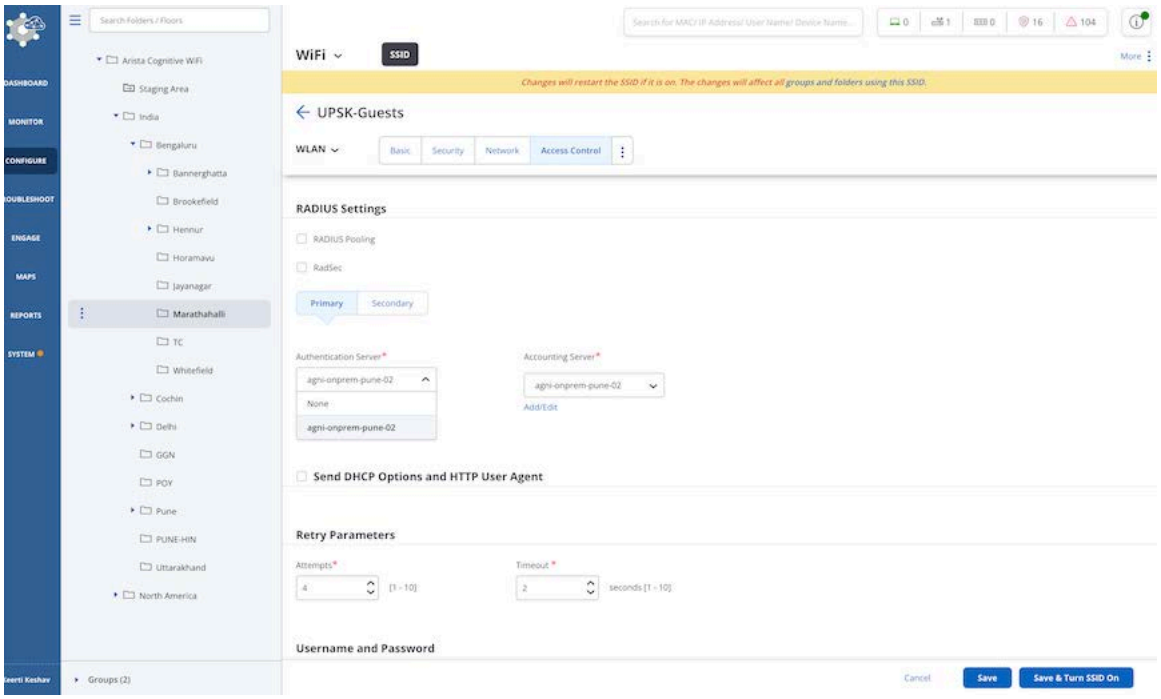
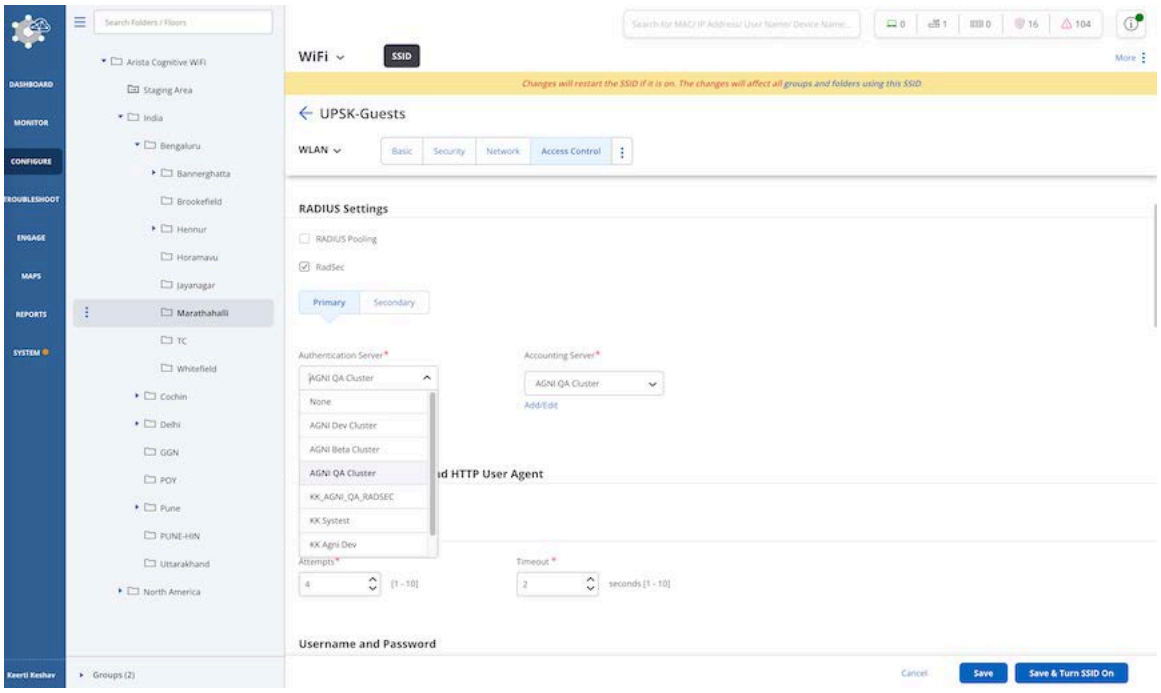


Figure 11-32: WiFi Access Control



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

11.3.3 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.

11.4 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.

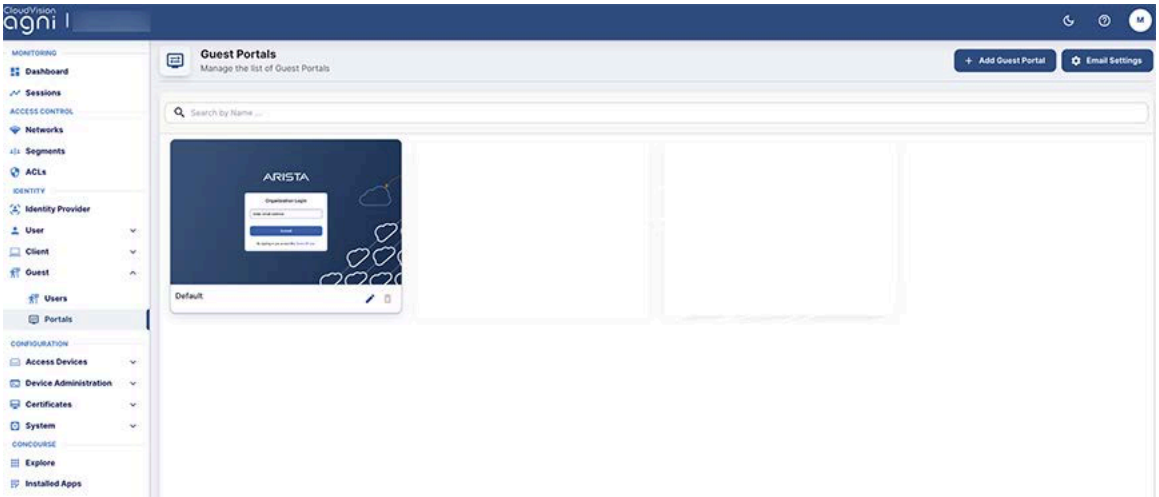
11.4.1 Configuring the Portal on AGNI

To configure the Guest Portal Using Guestbook (Wireless), perform the following steps:

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

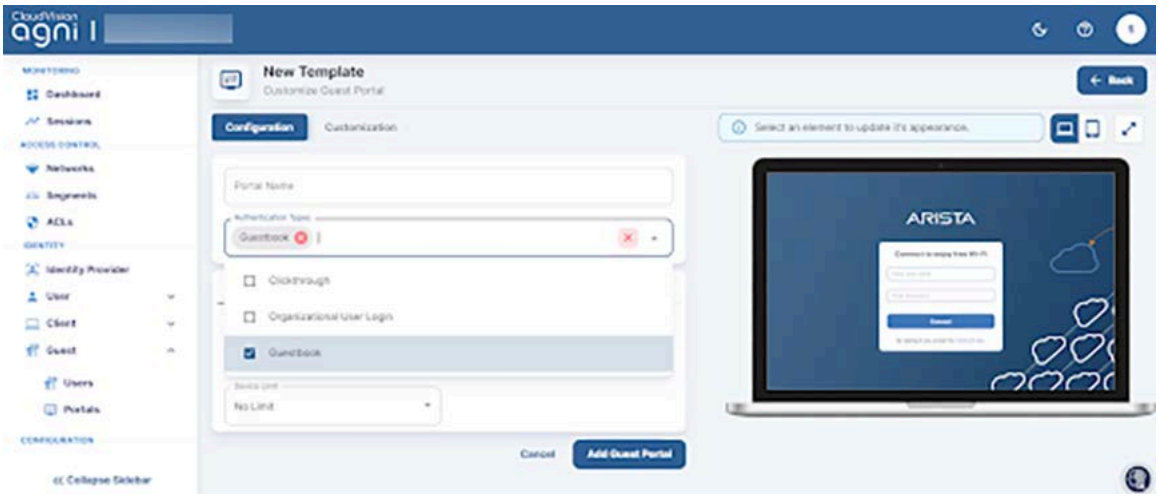
> **Note:** The **Default** portal is always present and non-removable in the portals. You can use the default portal to configure, if desired. For this article, let's create a new guest portal.

Figure 11-33: Identity Guest Portals



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**.
4. Select **Guestbook** as the Authentication Type.

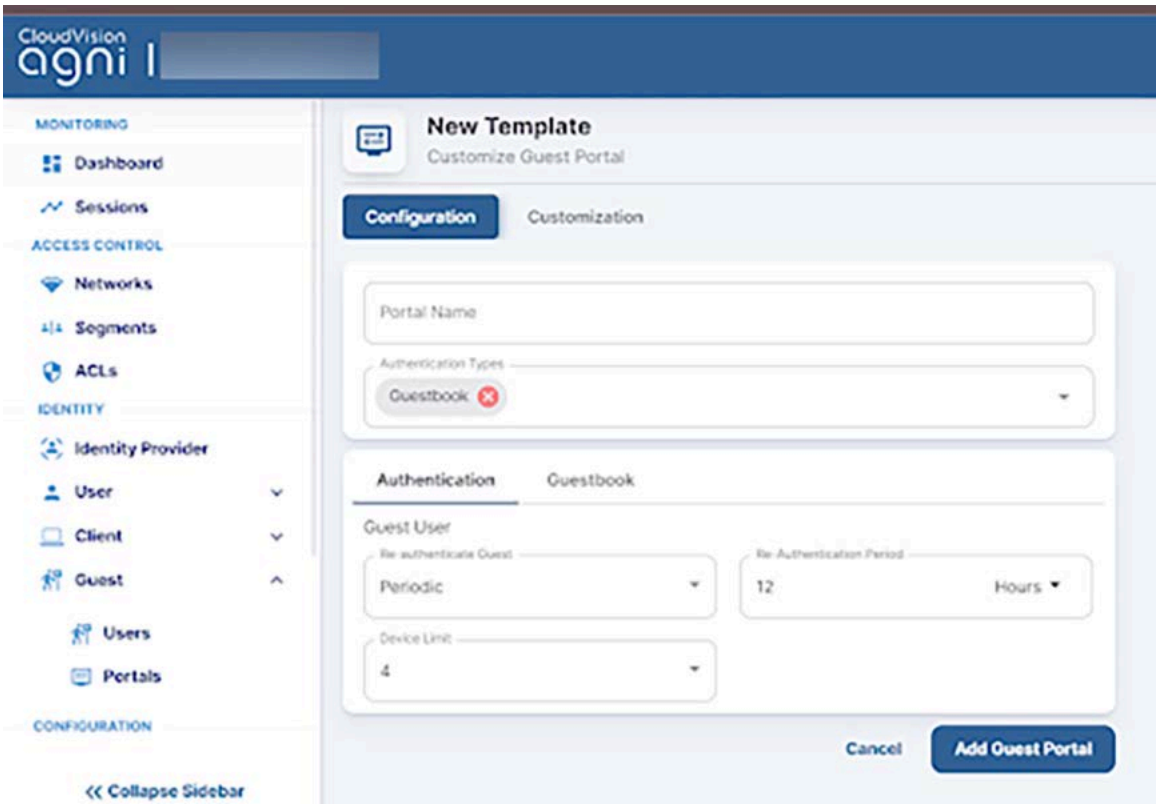
Figure 11-34: Configure Guest Portal - Guestbook



5. From the **Authentication** section, select the following settings for the guest user:
   - **Re-authenticate Guest** - **Periodic**
   - **Re-authentication Period** - 12 Hours

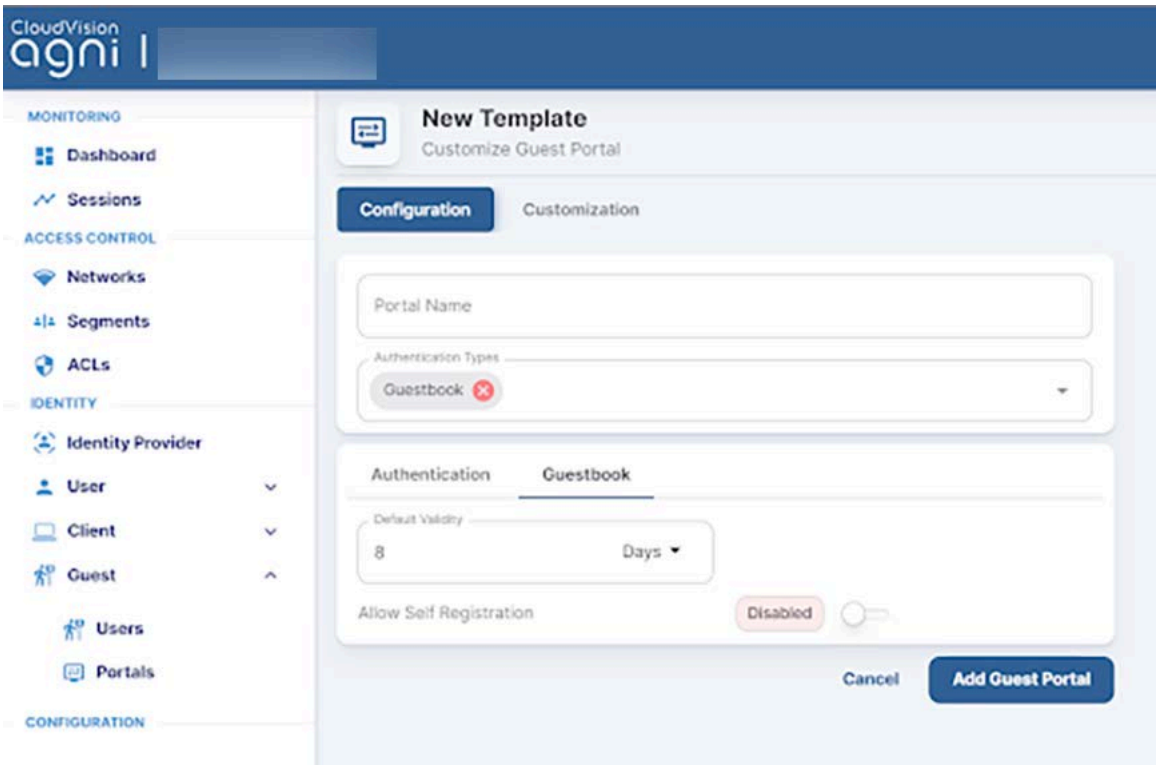
- **Device Limit - 4**

Figure 11-35: Re-authenticate Guest Periodic



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

Figure 11-36: Device Validity



> **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:
   - 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

Figure 11-37: Customization Settings

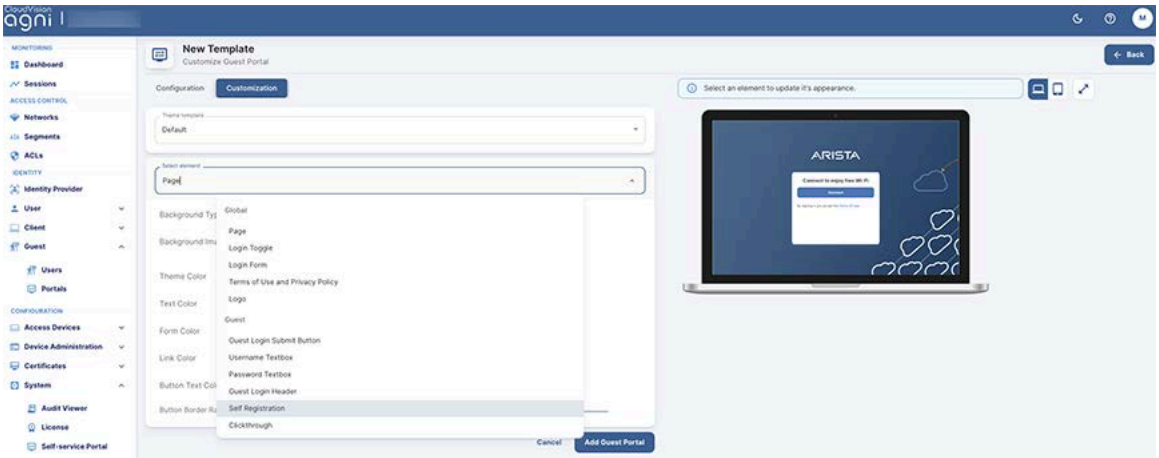
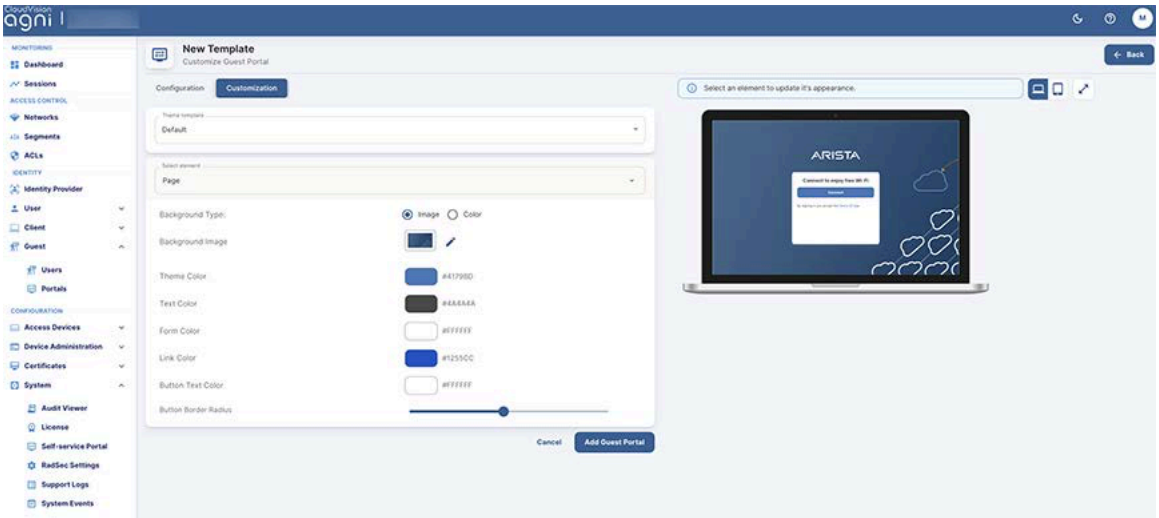


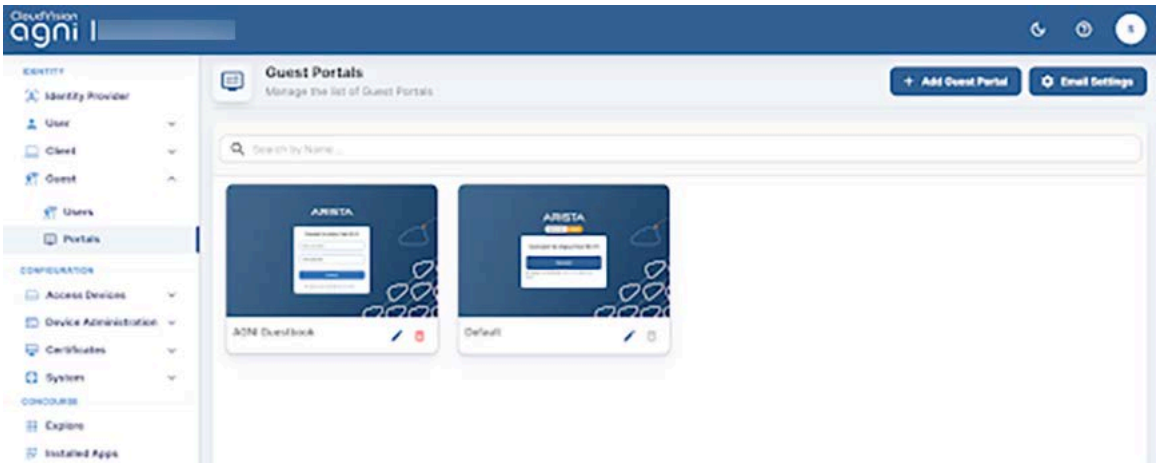
Figure 11-38: Additional Customization Settings



8. When done, click **Add Guest Portal**.

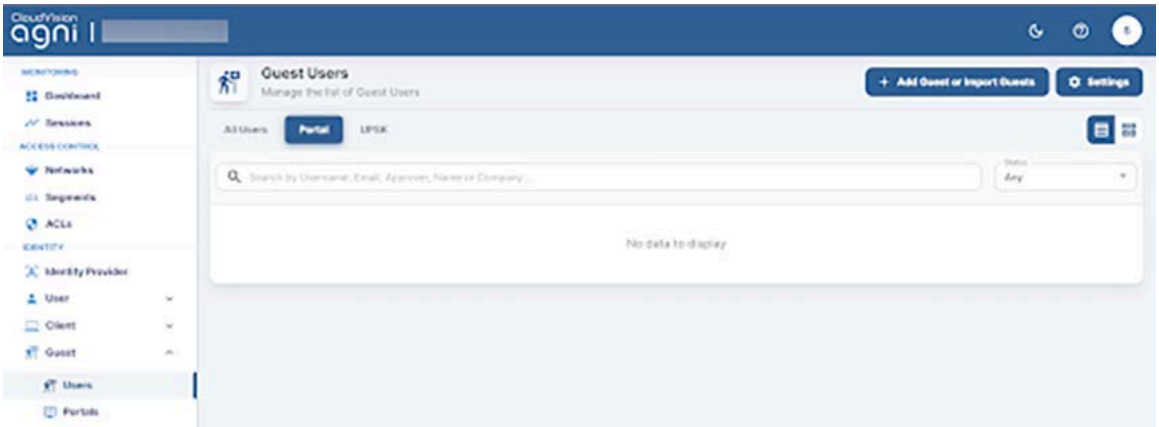
The portal gets listed in the portal listing.

Figure 11-39: Add Guest Portal



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

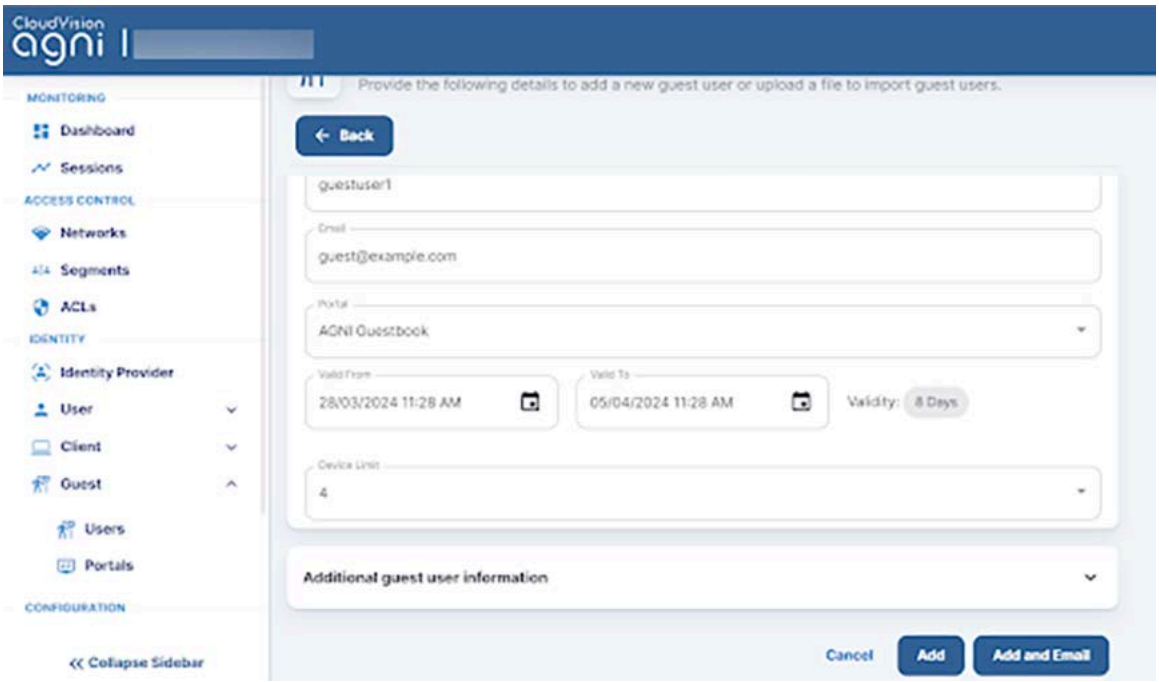
Figure 11-40: Add or Import Guest



11. 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.

Figure 11-41: Guest User Settings

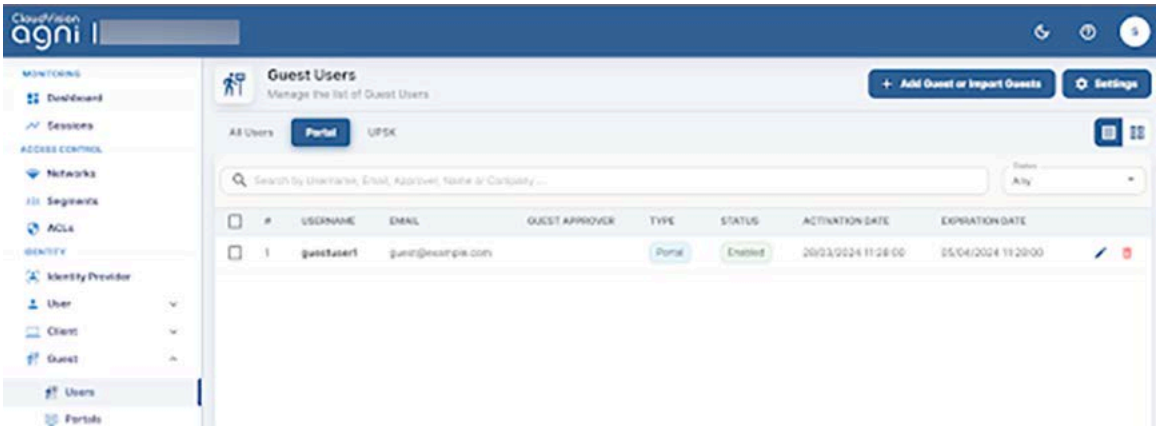


12. Click the **Add** button to add the guest user.

    If the admin clicks on **Add and Email**, you receive an email with the username, password, and other details.

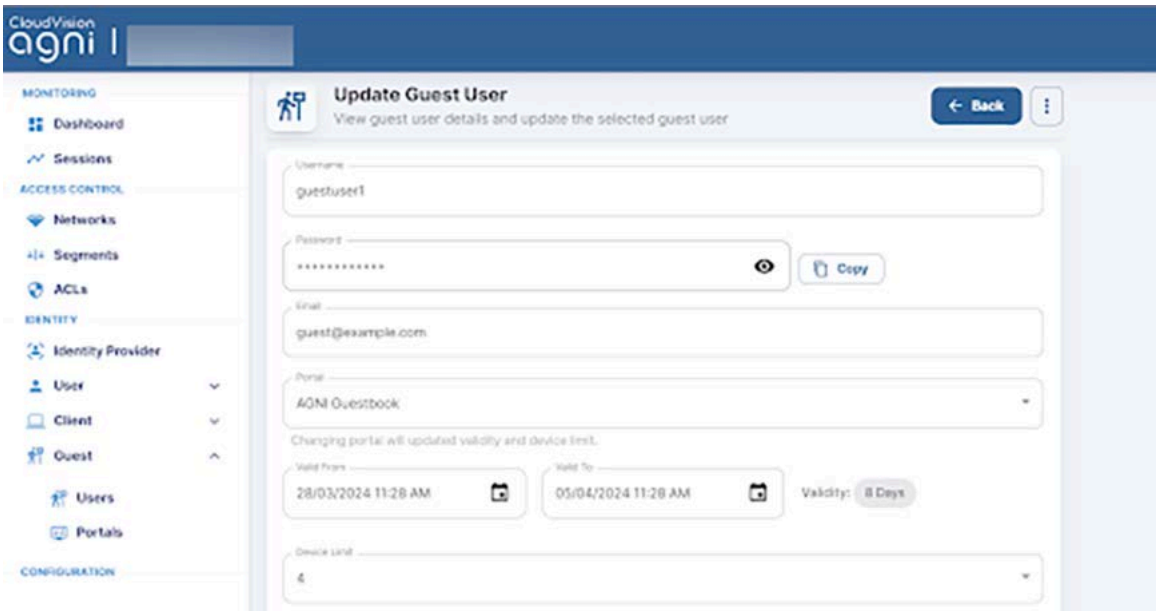
    The guest user is listed in the Portal User listing.

    Figure 11-42: Added Guest



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

Figure 11-43: Edit 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.

Figure 11-44: Export User Details

11.4.2 Configuring the Network

To configure the Guest Portal Using Guestbook (Wireless) network, perform the following steps:

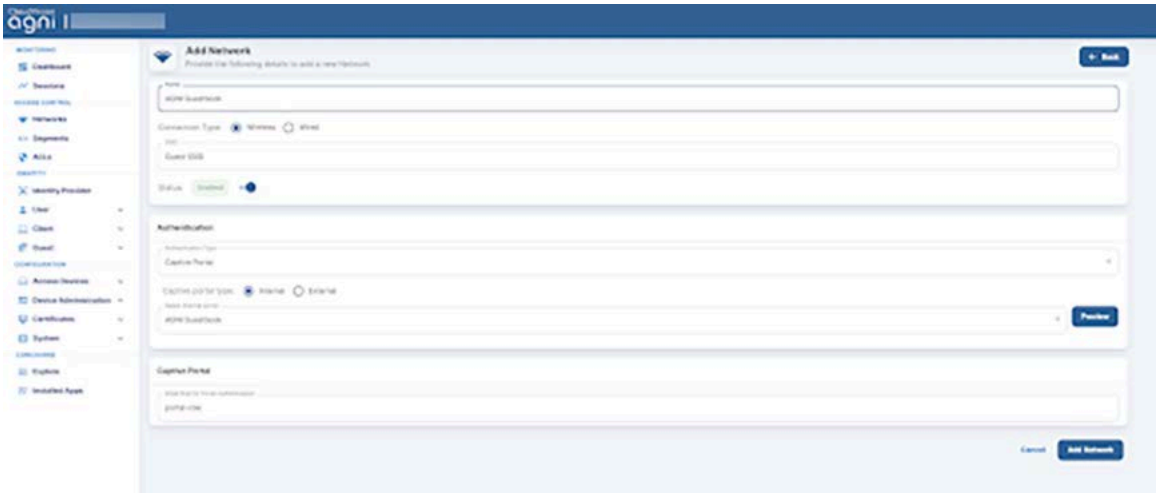
1. Navigate to the **Access Control** > **Network**.
2. Add a new network with the following settings:
   a. **Network Name - AGNI Guestbook**
   b. **Connection Type - Wireless**
   c. **SSID - Guest SSID**
   d. **Status - Enabled**
   e. **Authentication**
      1. **Authentication Type - Captive Portal**
      2. **Captive Portal Type - Internal**

3. **Select internal portal - AGNI Guestbook**

f. **Captive Portal**

- **Internal Role for Portal Authentication - portal-role**

Figure 11-45: Add Network



11.4.3 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.

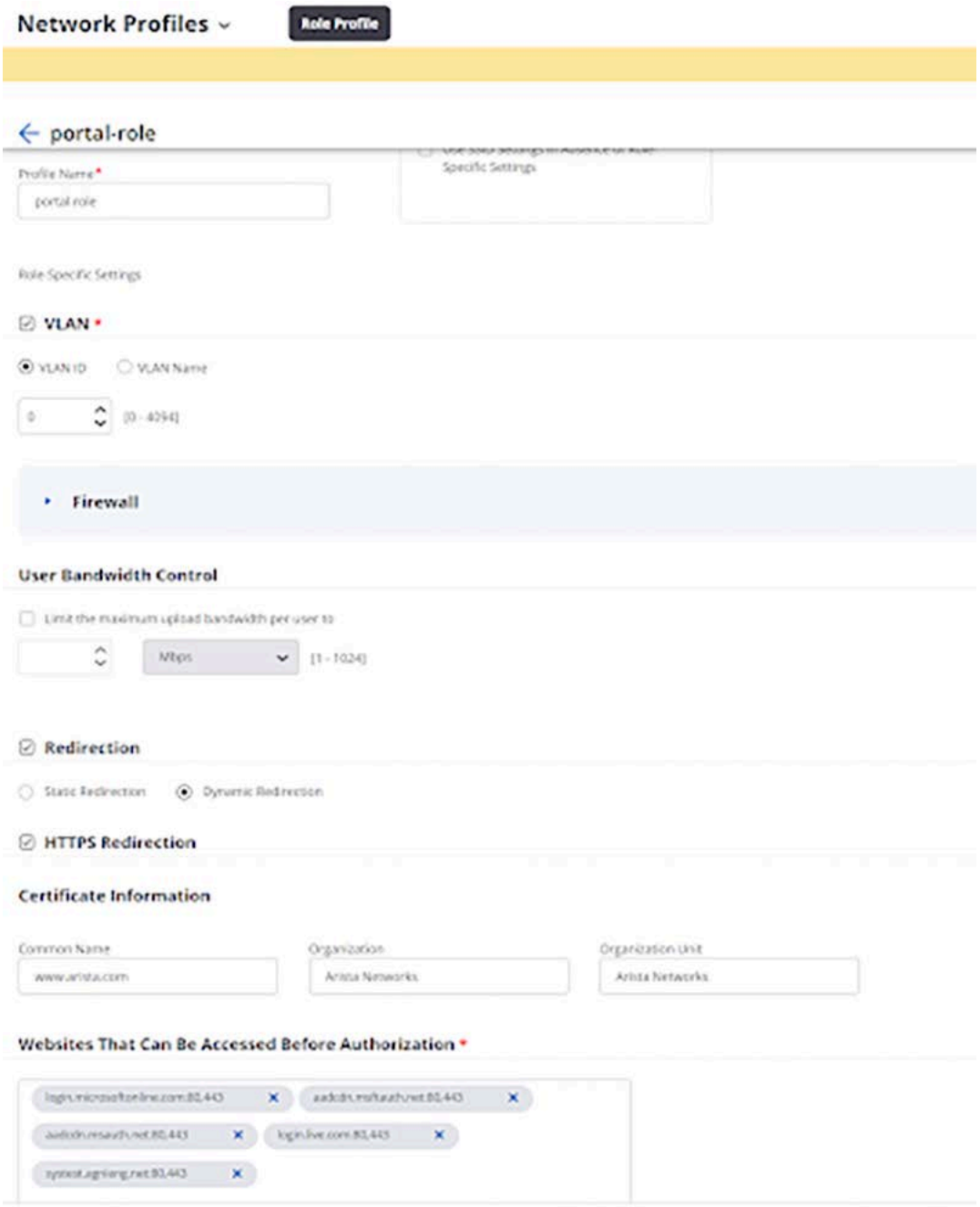
11.4.3.1 Configuring Role Profile

To configure the Guest Portal Using Guestbook (Wireless) role profile, perform the following steps:

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.

Figure 11-46: Configuring Role Profile



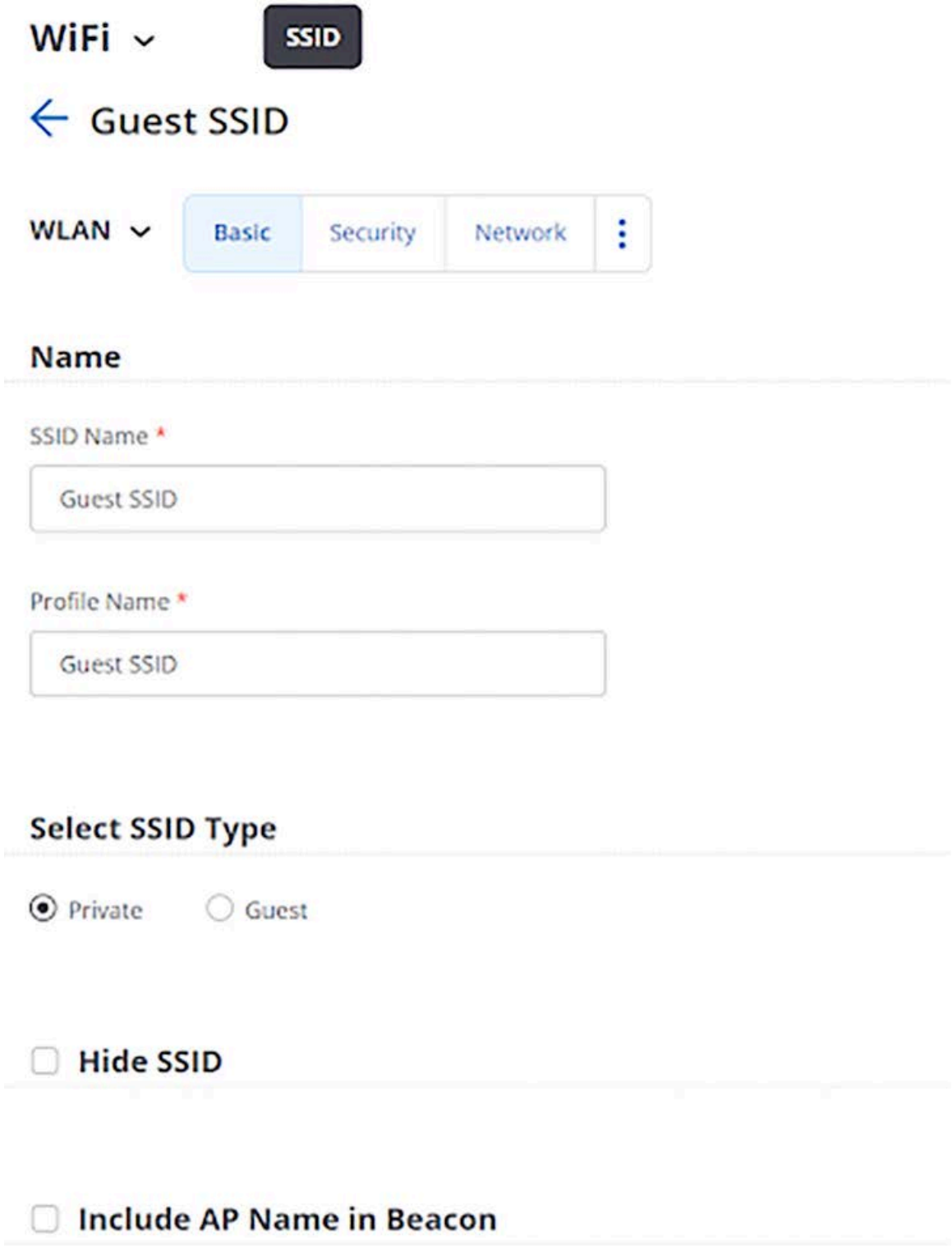
11.4.3.2 Configuring SSID

To configure the Guest Portal Using Guestbook (Wireless) SSID, perform the following steps:

1. Navigate to **Configure** > **WiFi**.
2. Add a new **SSID**.

3. Provide the **SSID Name** - Guest SSID.

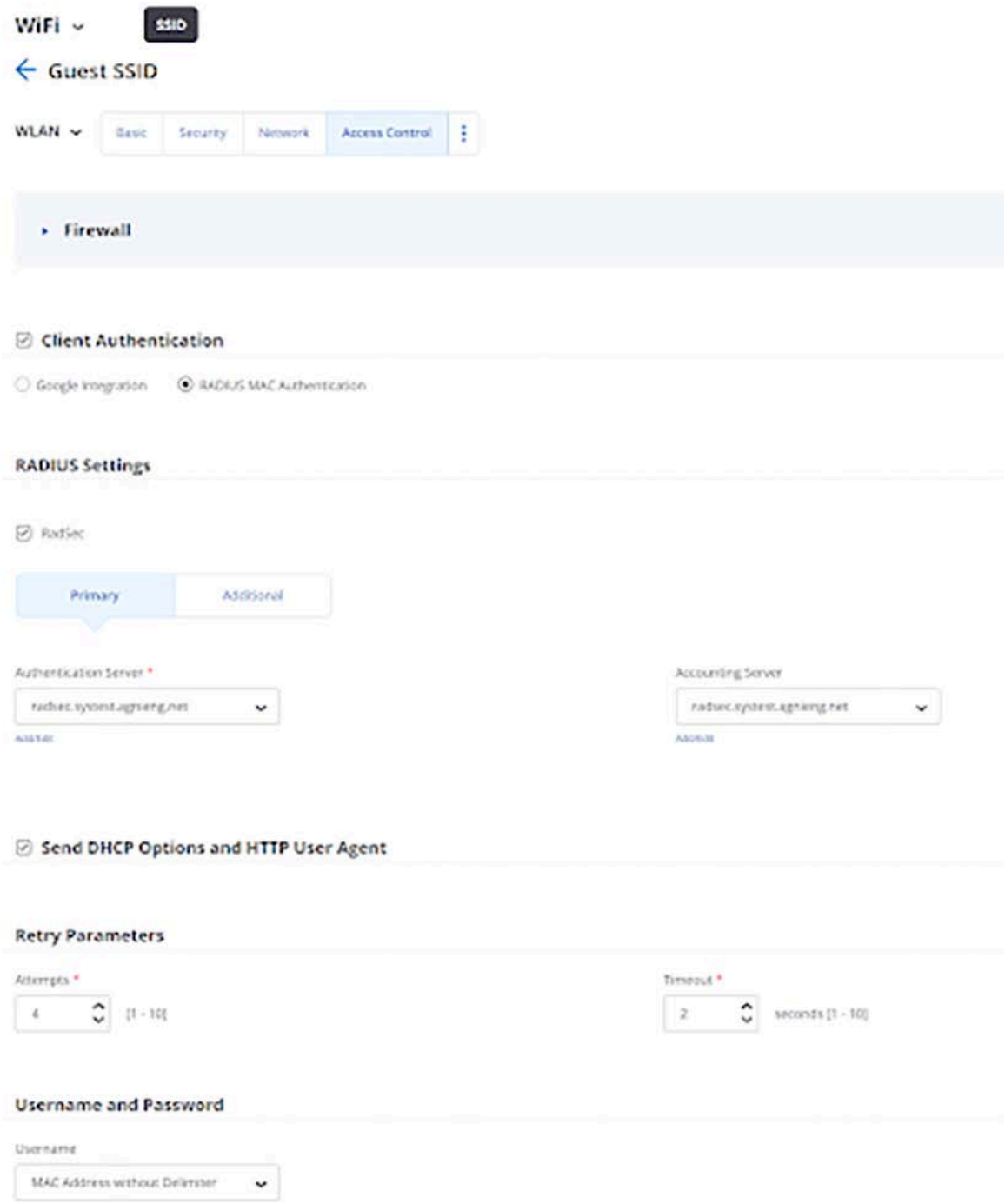
Figure 11-47: Guest SSID



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

6. Select **RadSec** if required. Uncheck this option to use RADIUS.
7. Select the **Authentication** and **Accounting** servers.

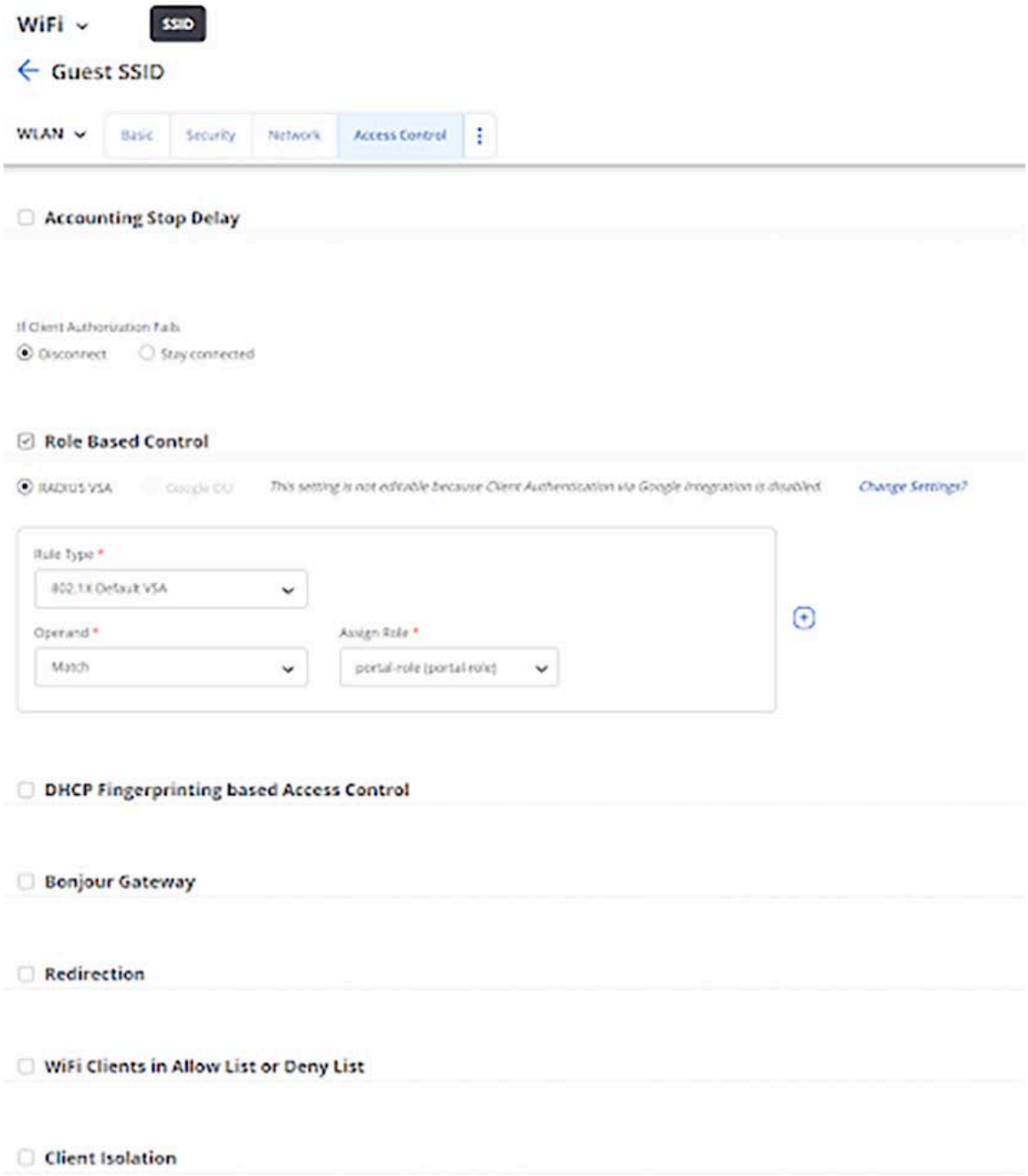
Figure 11-48: Authentication and Accounting Servers



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.

Figure 11-49: Portal Role



9. Save the settings and turn **ON** the SSID.

The clients get connected and authenticated via portal authentication after entering their username and password.

11.5 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.

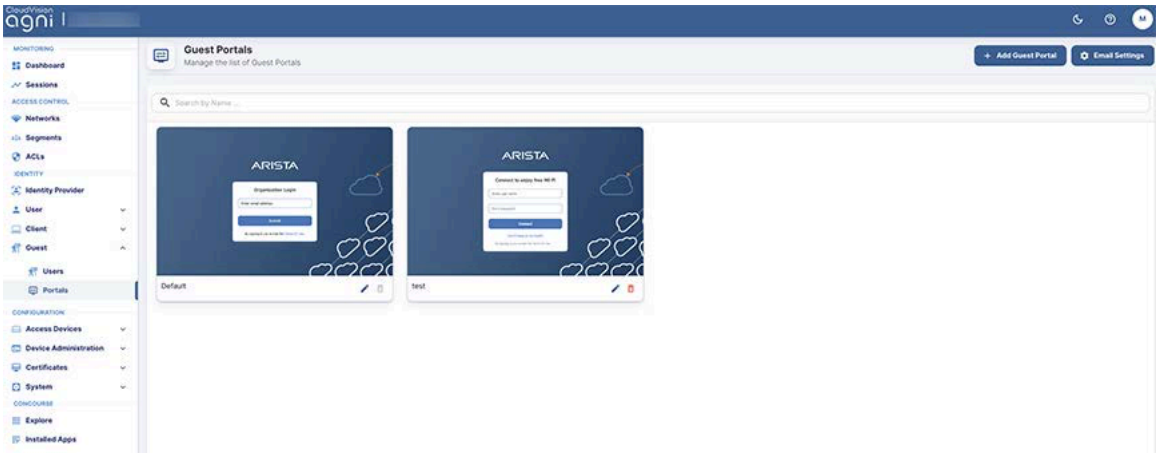
11.5.1 Configurations on AGNI

To configure AGNI for Guestbook authentication, perform the following steps:

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.

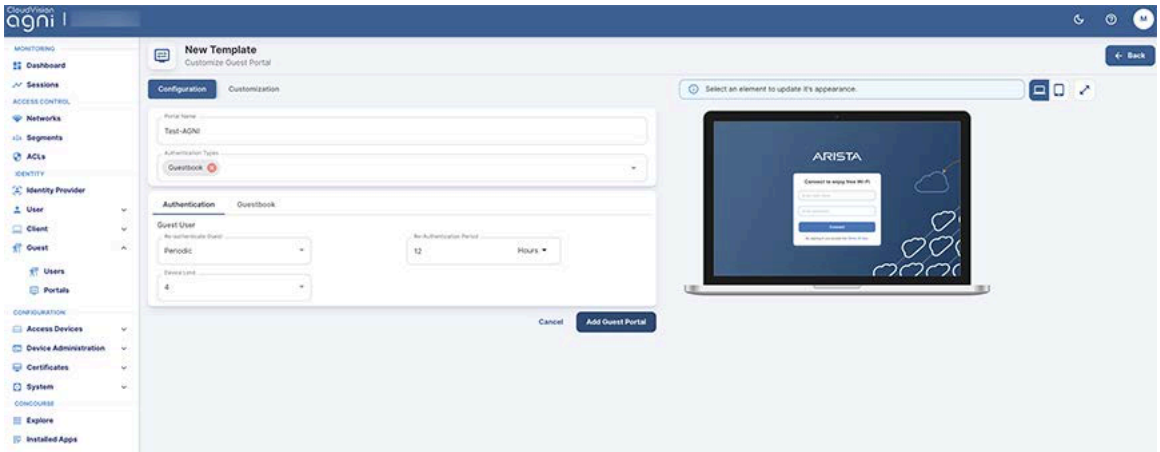
Figure 11-50: Identity Guest Portal



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**.
4. Select Guestbook as the Authentication Type.
5. 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**

Figure 11-51: Configure Portal



6. 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

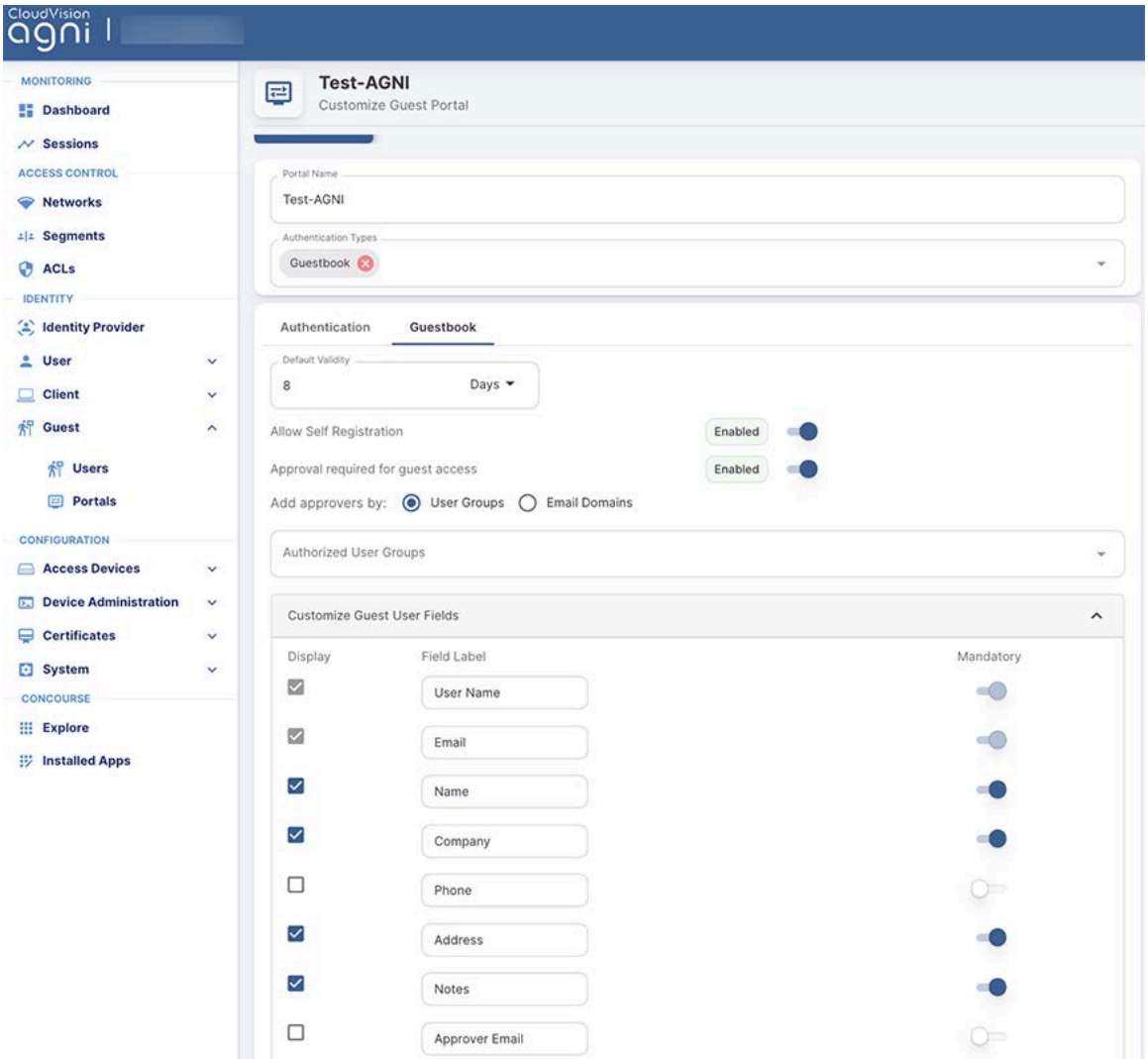
   d. Company

   e. Address

   f. Notes

7. Click the **Update** button.

Figure 11-52: Update Portal



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.

8. Click the **Customization** tab to customize the portal settings, including:

   a. Theme template

      1. Default
      2. Split Screen

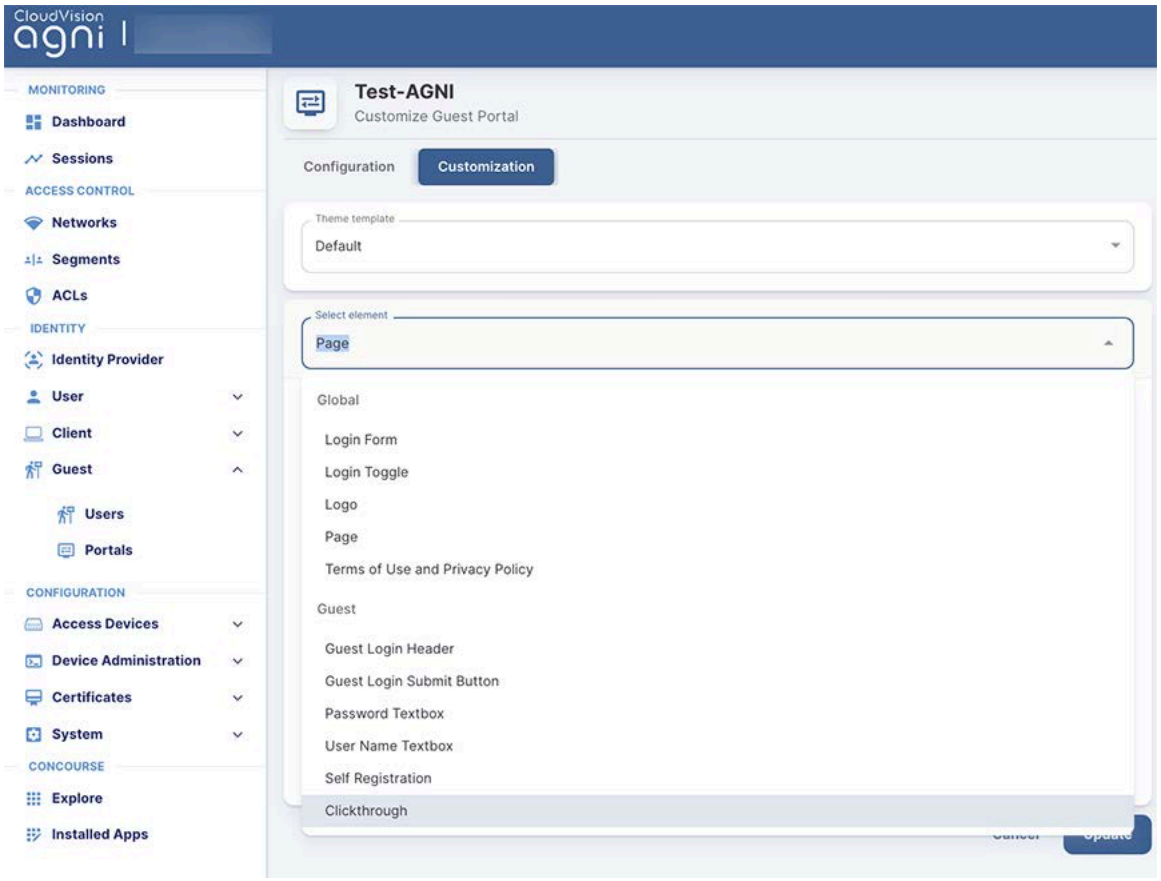
b. Select element

1. Global
2. Page
3. Login Toggle
4. Terms of Use and Privacy Policy
5. Logo

c. 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

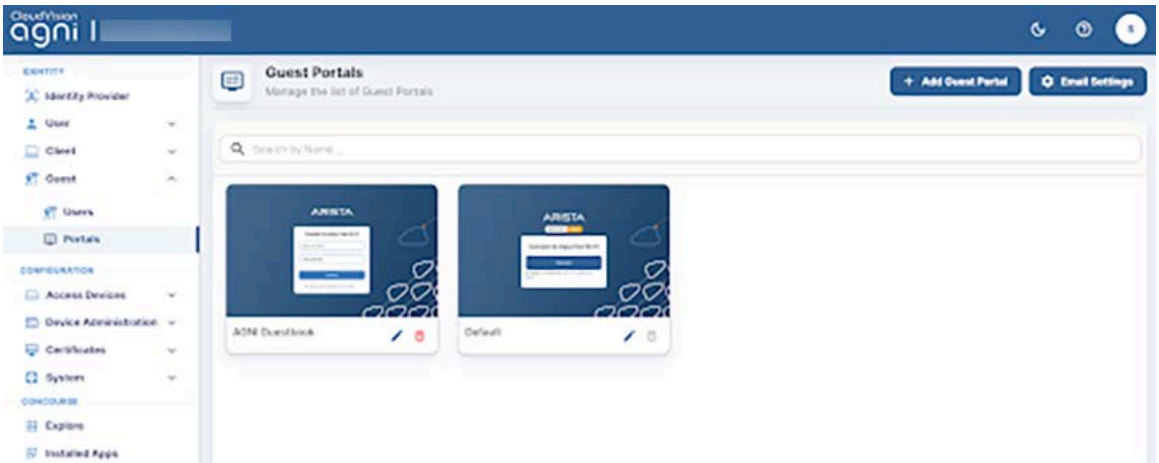
Figure 11-53: Customize Portal



9. When done, click **Add Guest Portal**.

The portal gets listed in the portal listing.

Figure 11-54: Guest Portal Added



11.5.2 Configuring the Network

For details, see the Configuring the Network section above.

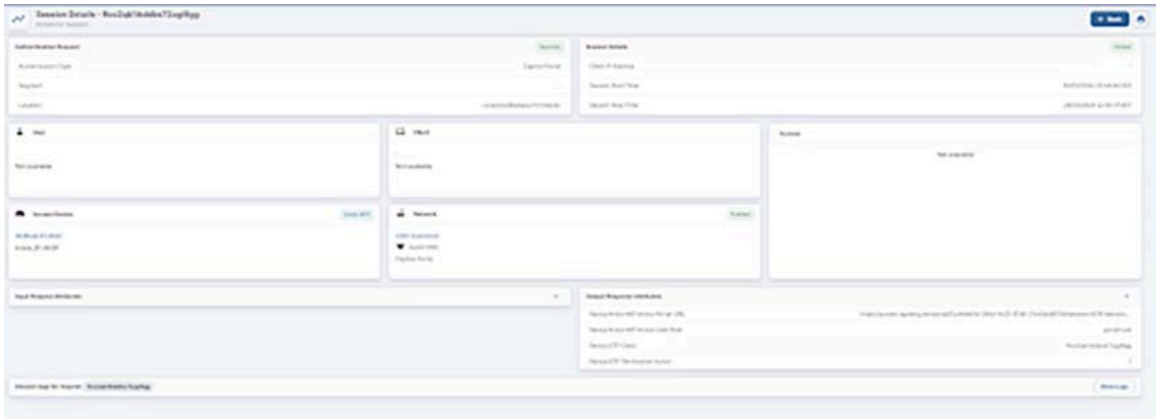
11.5.3 Configuring CV-CUE

For details, see the Configuring CV-CUE section above.

11.5.4 User Onboarding

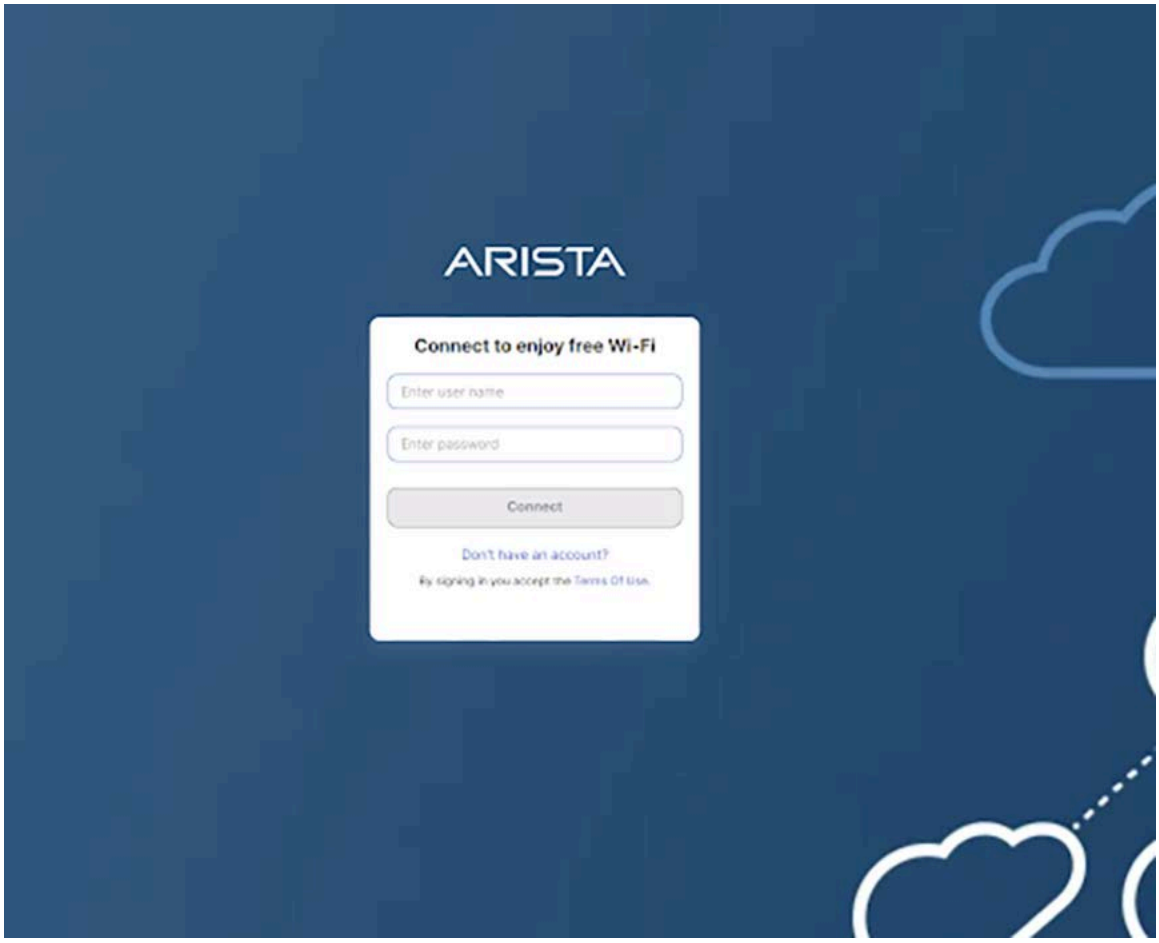
When the user connects to the Guest SSID, a session is opened in AGNI. AGNI sends the role profile and portal URL in the radius access accept message.

Figure 11-55: User Onboarding



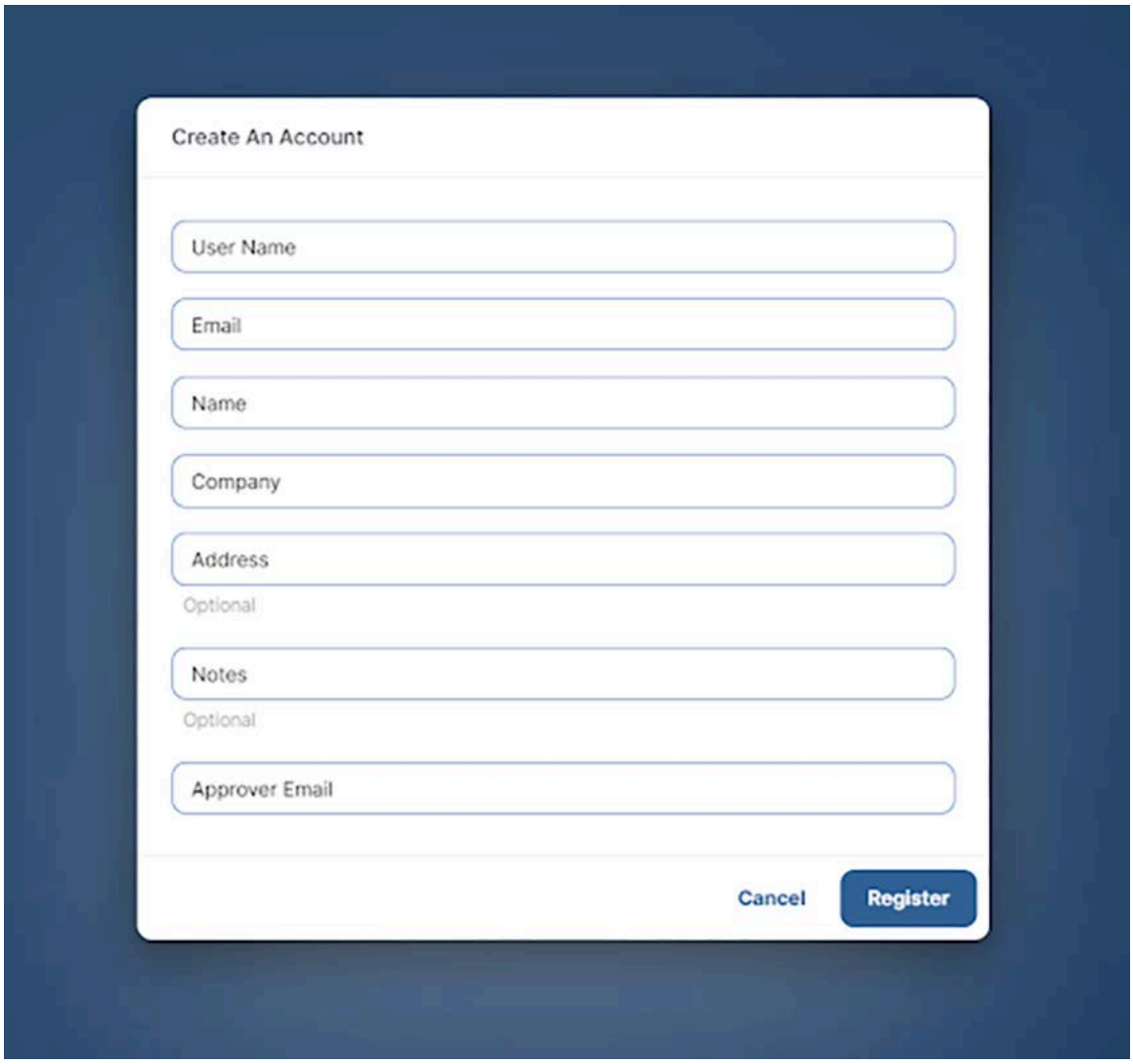
On the portal page, the user is asked for login credentials. If the guest user does not have the login credentials, select the **Don’t have an account?** link to generate the credentials.

Figure 11-56: Login Portal - Require Account



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

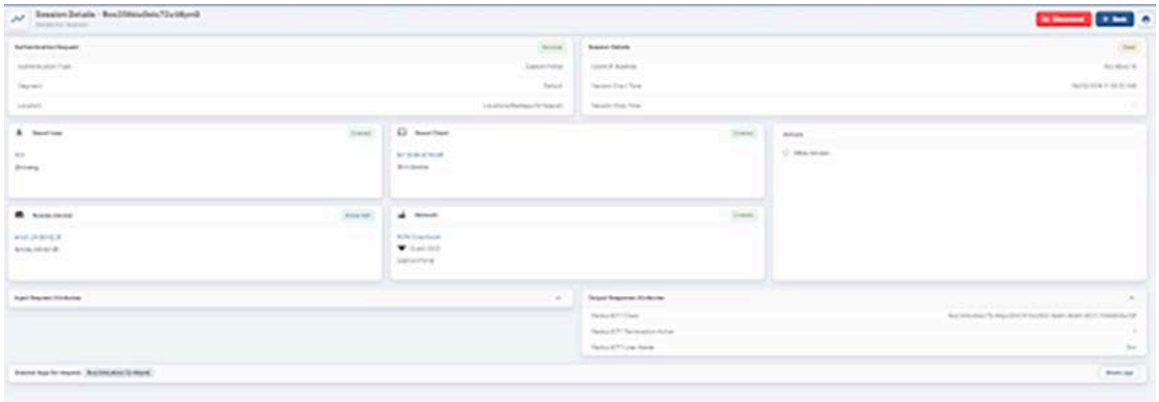
Figure 11-57: Create an Account



- 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.

Figure 11-58: Onboarded User Details



11.6 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.

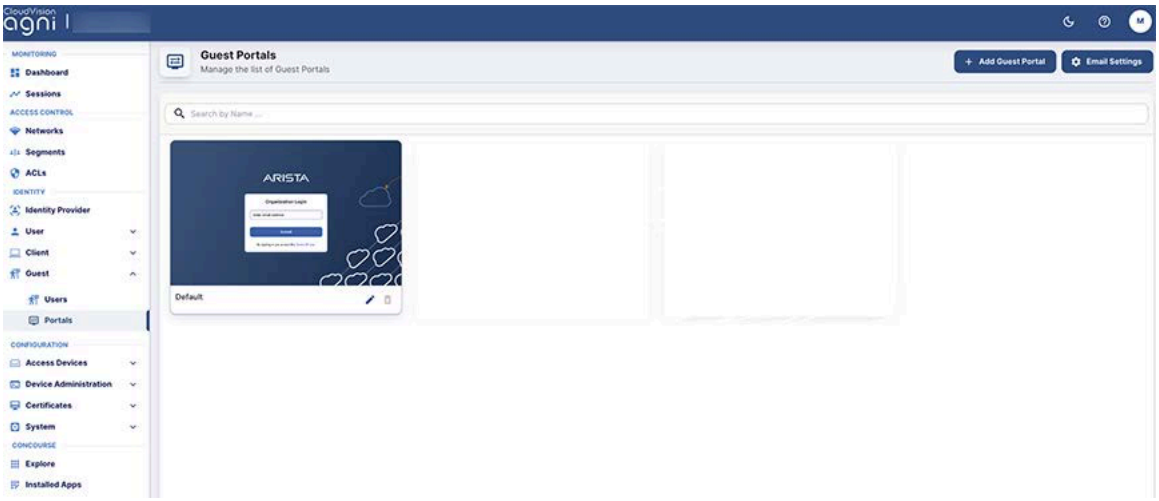
11.6.1 Configuring the Portal on AGNI

To configure the portal, perform the following steps:

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.

Figure 11-59: 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**

Figure 11-60: Guest Portal Settings

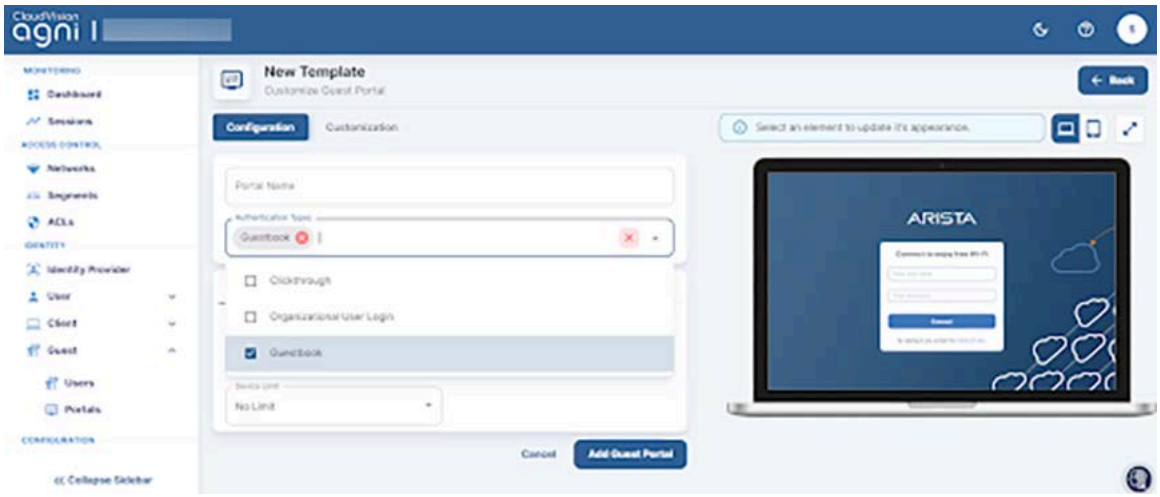
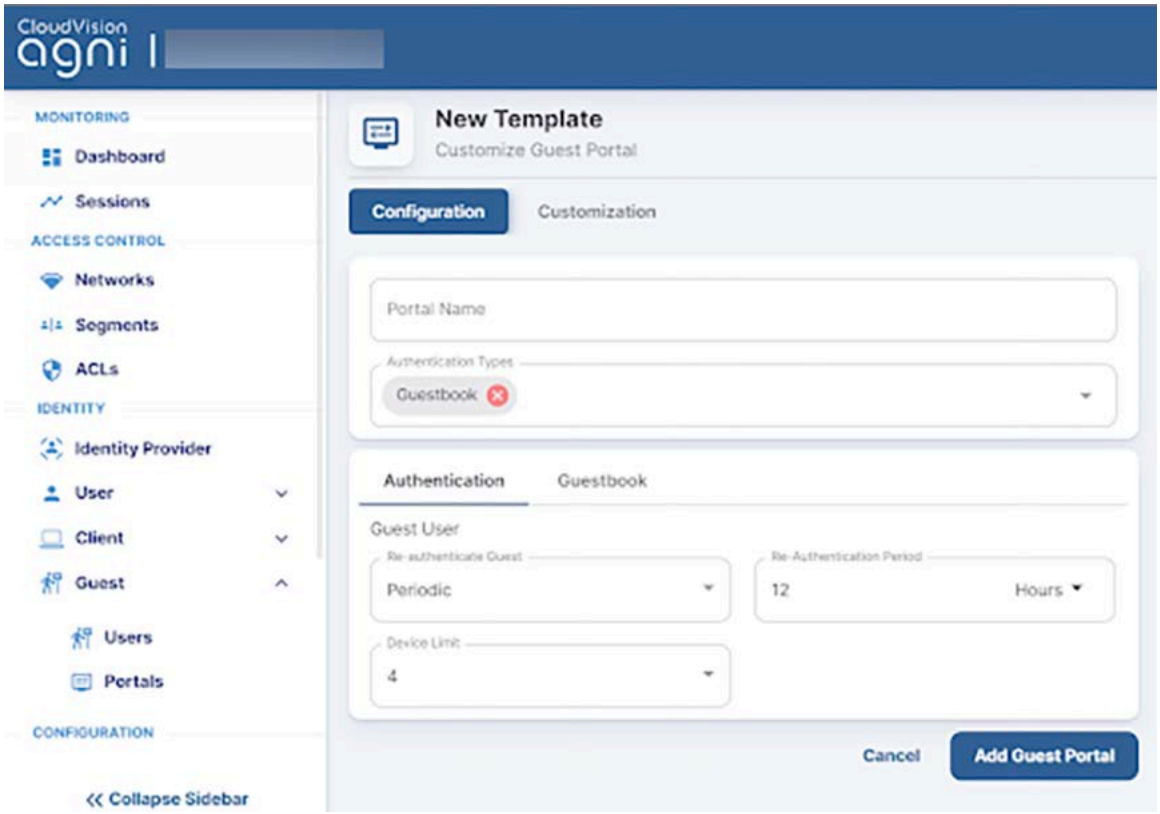


Figure 11-61: Guest Portal Settings



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

   a. User Name

   b. Email

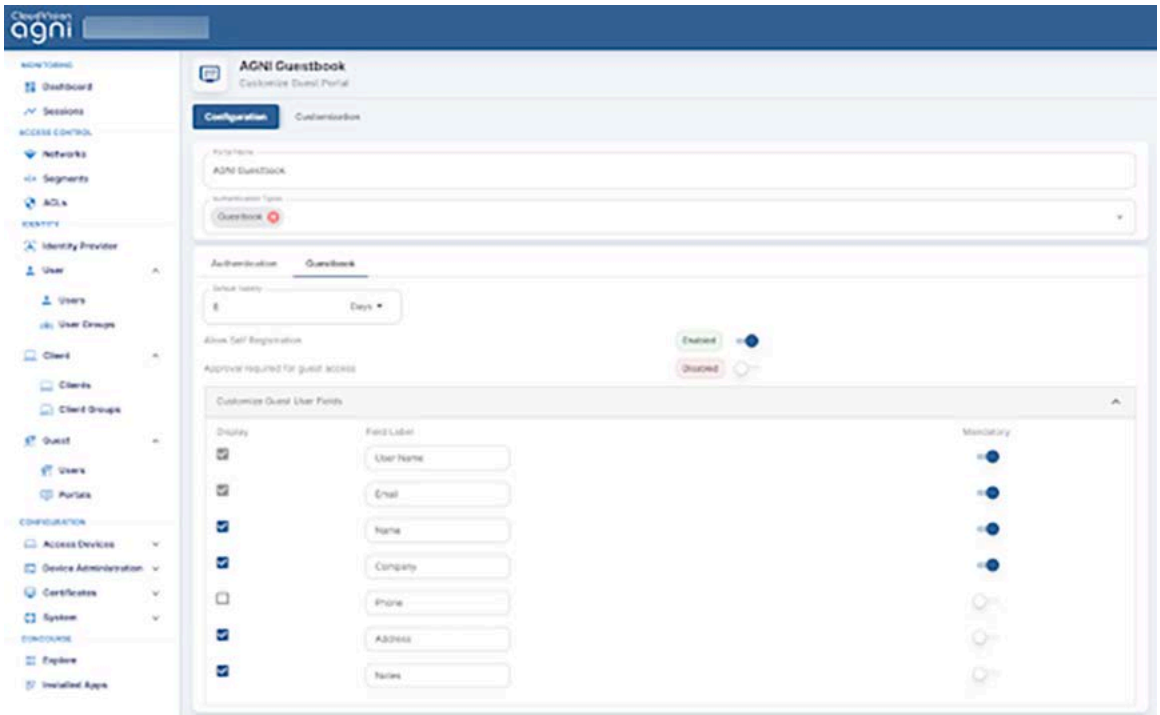
   c. Name

   d. Company

e. Address

f. Notes

Figure 11-62: Guest Portal User Fields



> **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
      1. Default
      2. Split Screen
   b. Select element
      1. Global
         a. Page
         b. Login Toggle
         c. Terms of Use and Privacy Policy
         d. Logo
      2. Guest
         a. Guest Login Submit Button
         b. User Name Text box
         c. Password Text box
         d. Guest Login Header
         e. Guest Login Form
         f. Self Registration

g. Clickthrough

Figure 11-63: Guest Portal Customize

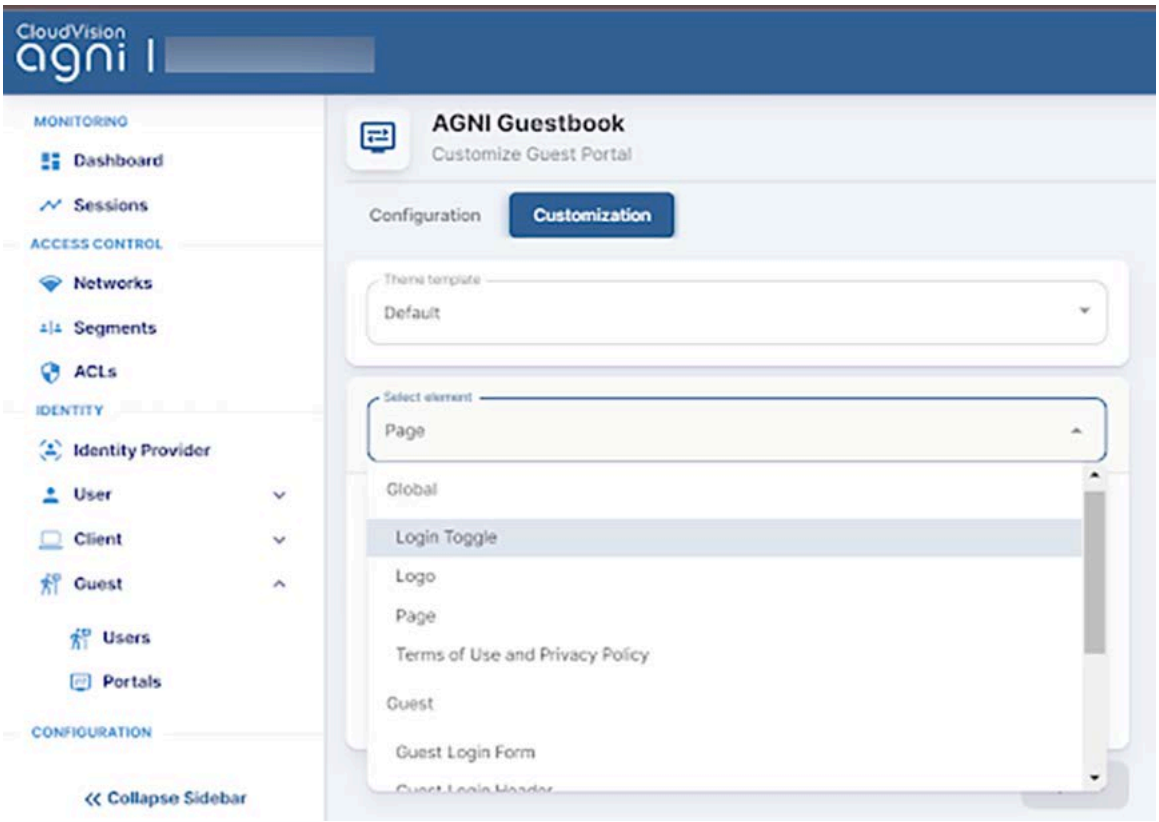
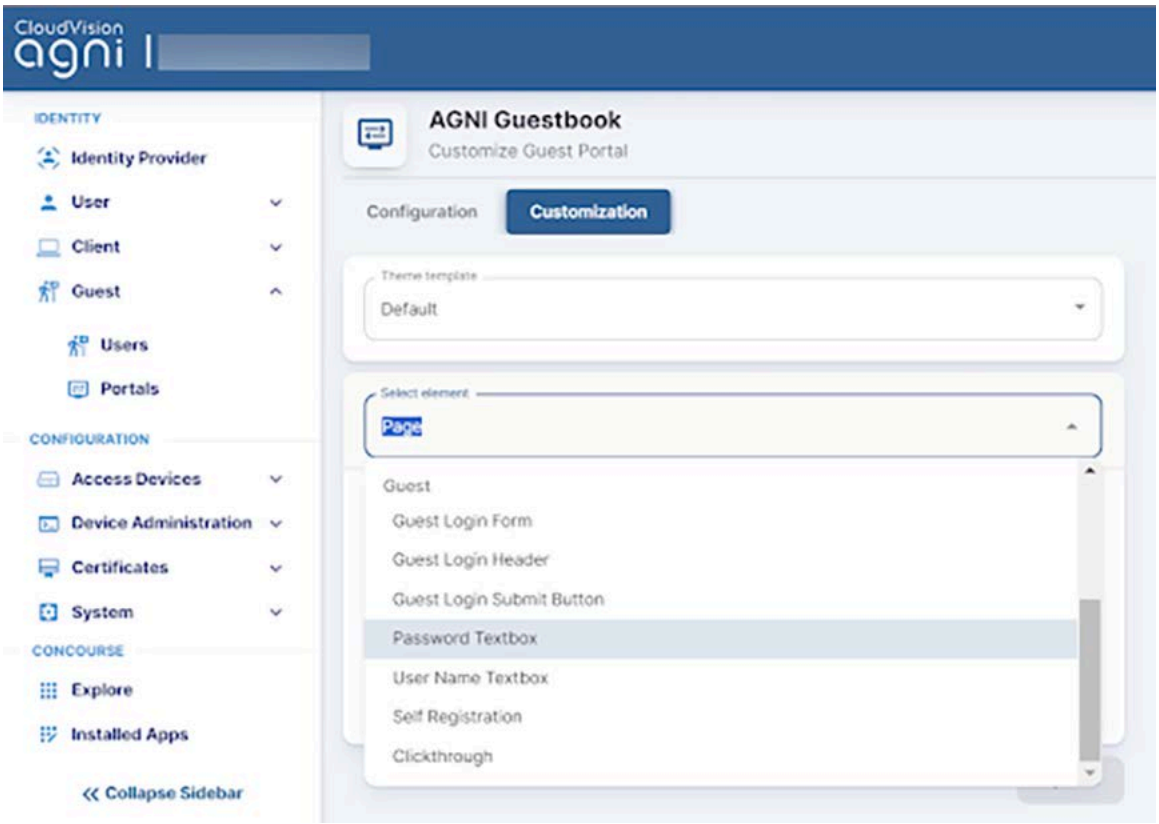
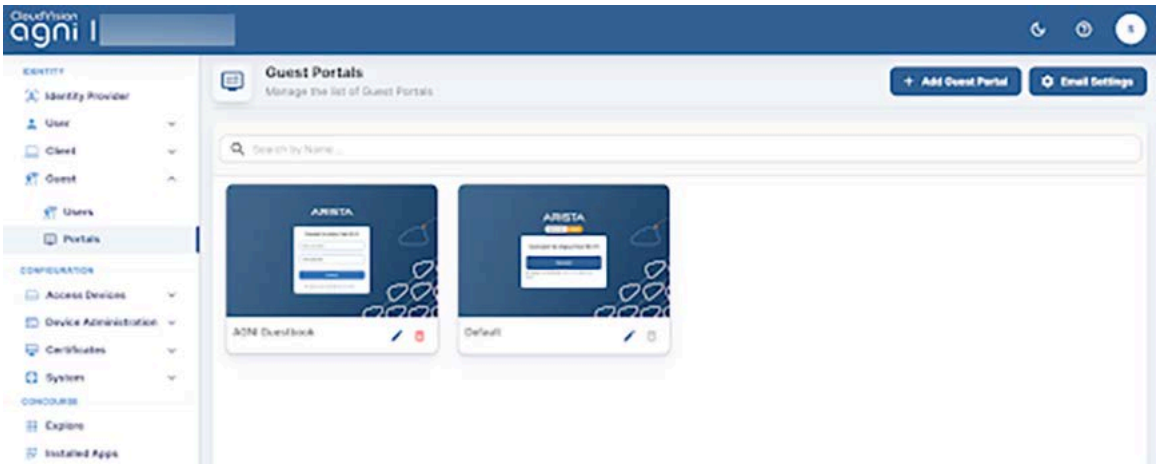


Figure 11-64: Guest Portal Customize



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

Figure 11-65: Guest Portal Added



11.6.2 Configuring the Network

For details, see the Configuring the Network section above.

11.6.3 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.

11.6.4 User Onboarding

For details, see the User Onboarding section above.

11.7 Configuring Guest Portal in AGNI for Wired Clients

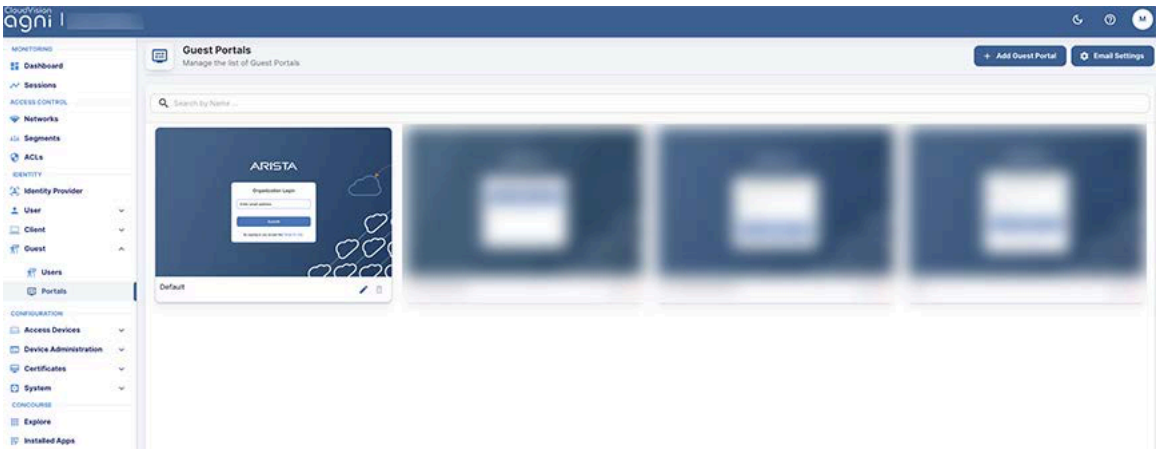
This section describes the steps to configure the guest portal using AGNI for wired clients. To configure the guest portal, you must configure AGNI and the switch.

11.7.1 Configuring AGNI

To configure AGNI, perform the following steps:

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

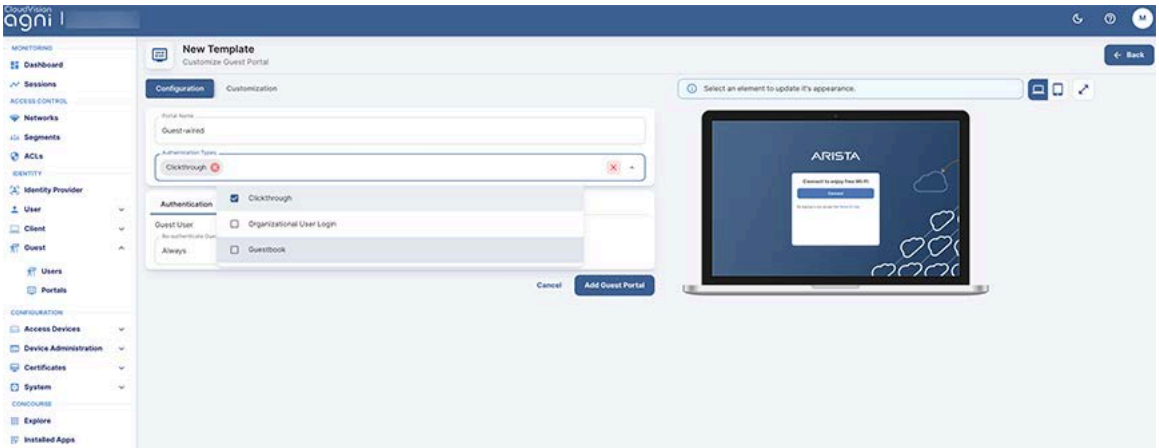
   Figure 11-66: Identity Guest Portals



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

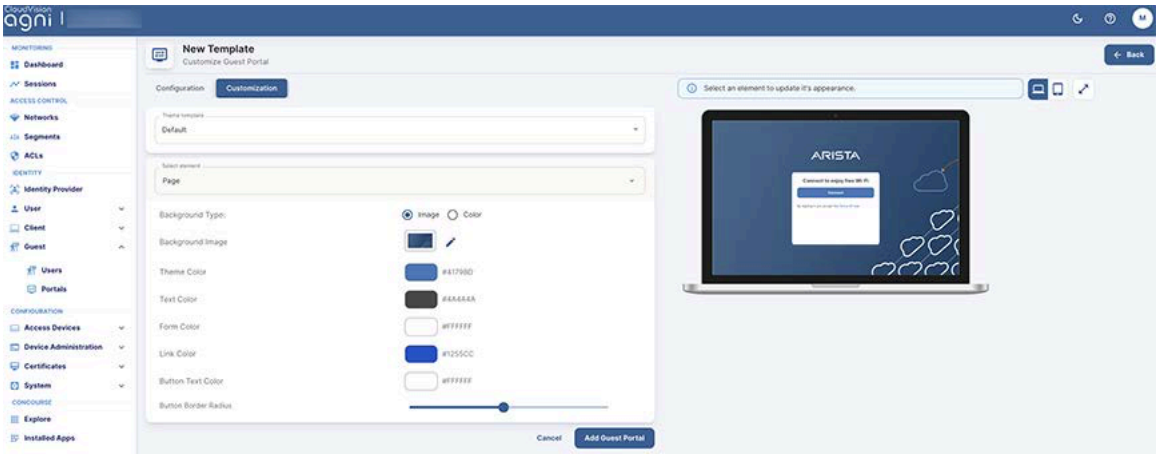
3. In the **Configuration** tab, provide the portal name and select the theme of the portal. The available theme options are **Default** or **Split Screen**.

   Figure 11-67: Configure Portal



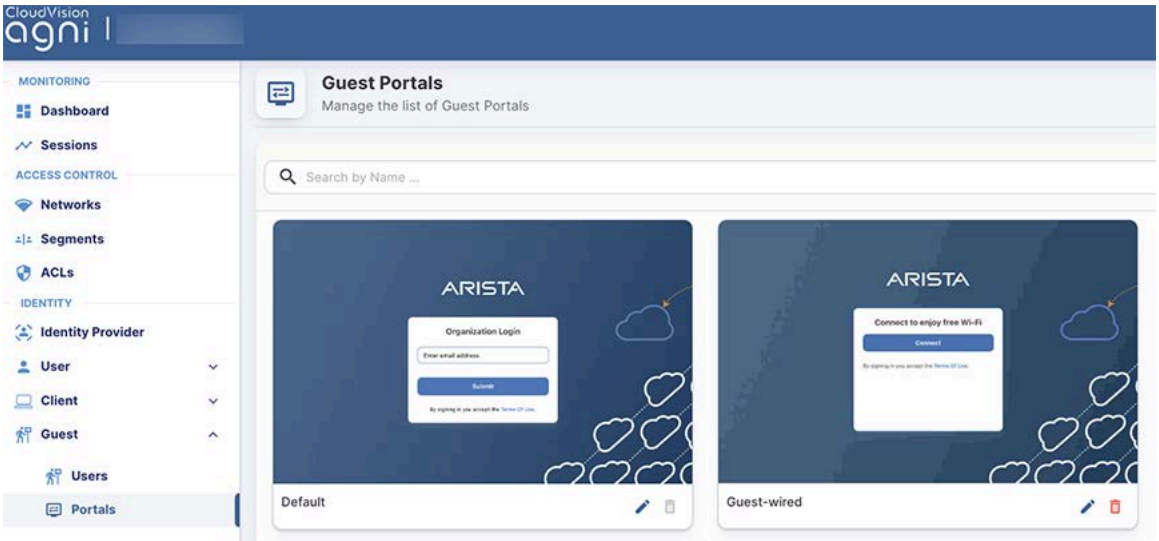
4. Select the **Authentication Type** as **Clickthrough**.
5. Click the **Customization** tab to customize the portal settings, including:
   a. Page
   b. Login Toggle
   c. Terms of Use and Privacy Policy
   d. Logo
   e. Guest Login Submit Button

   Figure 11-68: Customize Portal



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

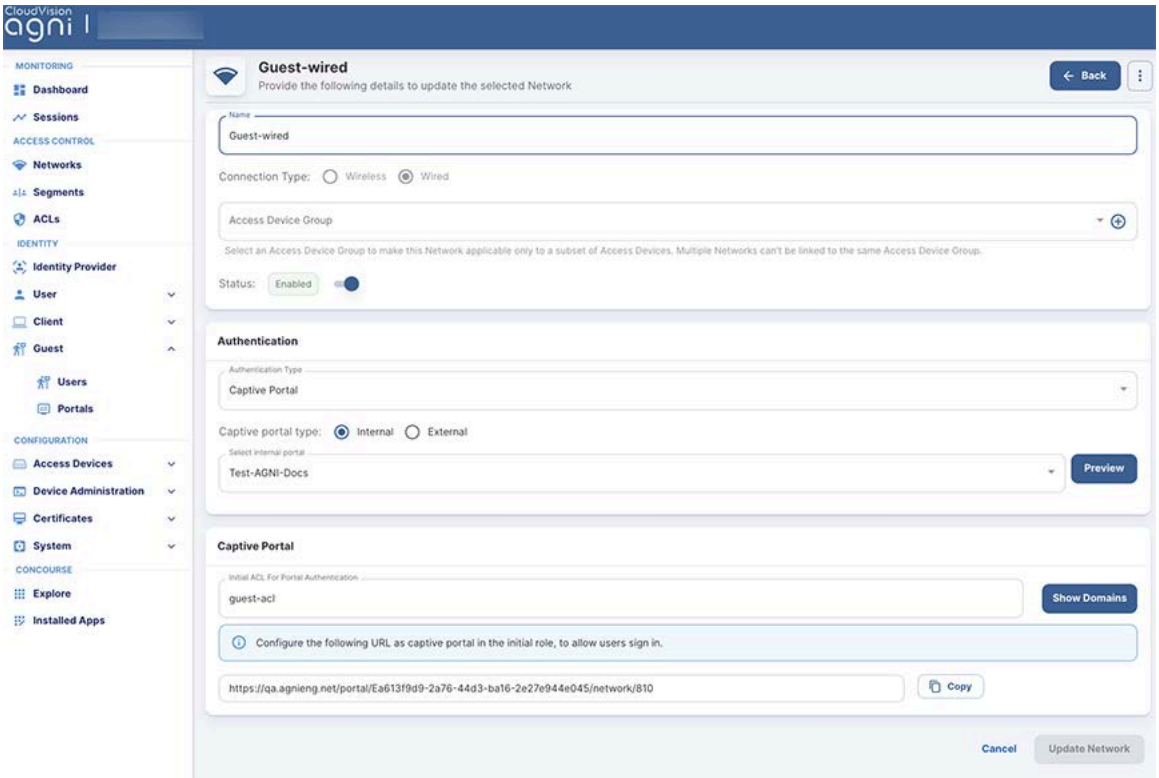
Figure 11-69: Add Guest Portal



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

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

Figure 11-70: Copy URL



11.7.2 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
!
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
!
```

11.8 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.

11.9 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.

11.10 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.

Chapter 12

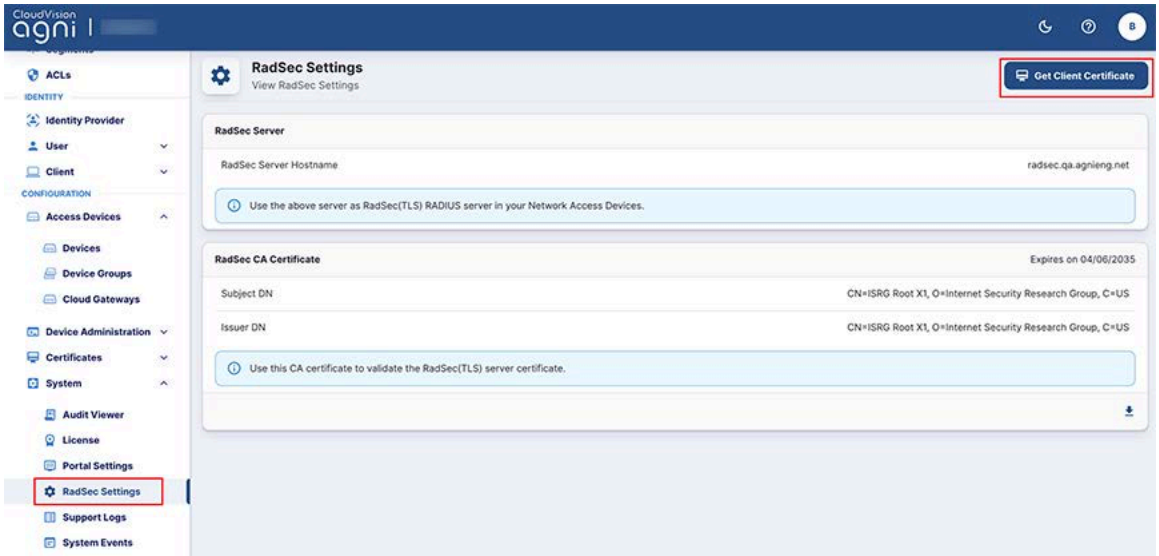
Generating Client Certificates for RadSec

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).

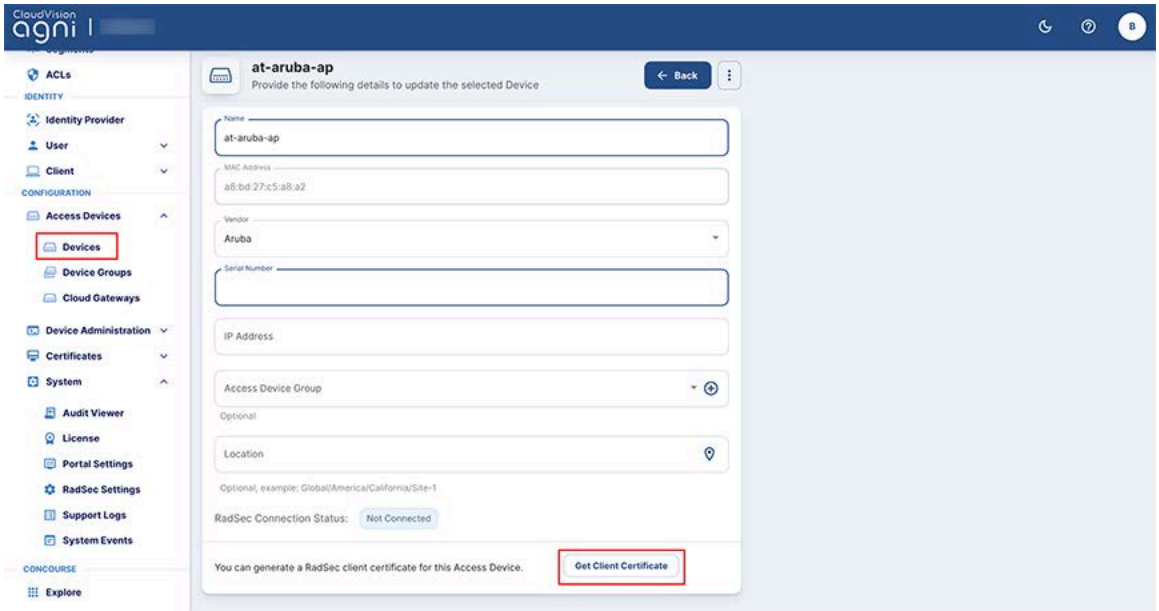
Figure 12-1: RadSec Settings Certificate Generate Page



OR

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

Figure 12-2: Device Settings Certificate Generate Page



You can generate the certificate in one of the three ways as below (see image) :

- 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).

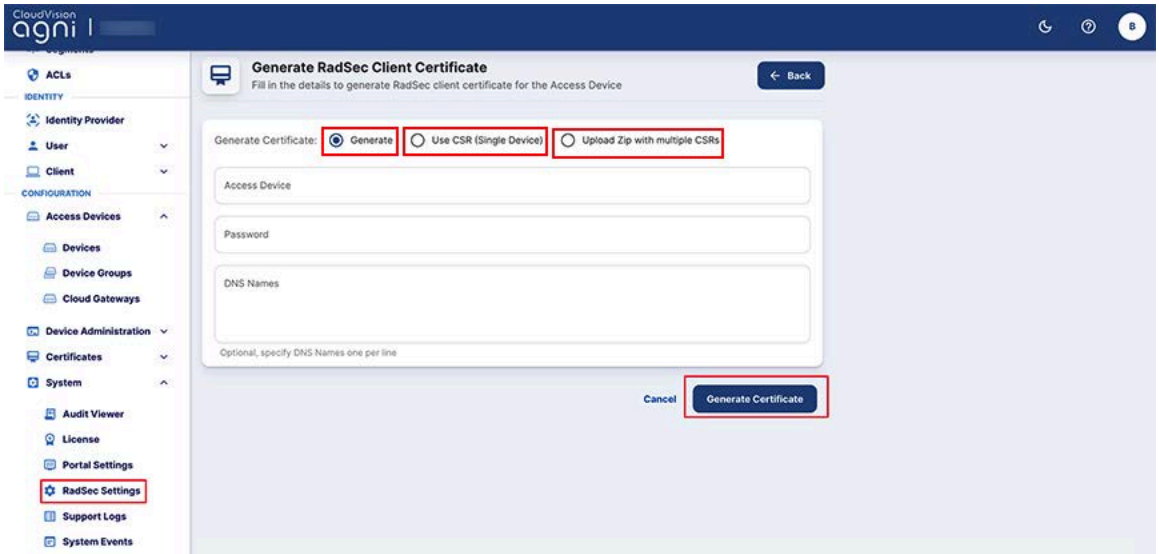
- Click the **Use CSR (Single Device)** option to generate a CSR certificate for a single device.

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 Wi-Fi devices, you can generate bulk CSRs from Arista CV-CUE interface. Bulk CSRs can be uploaded as a zip file to generate the client certificates.

Figure 12-3: RadSec Client Certificate Generating Options



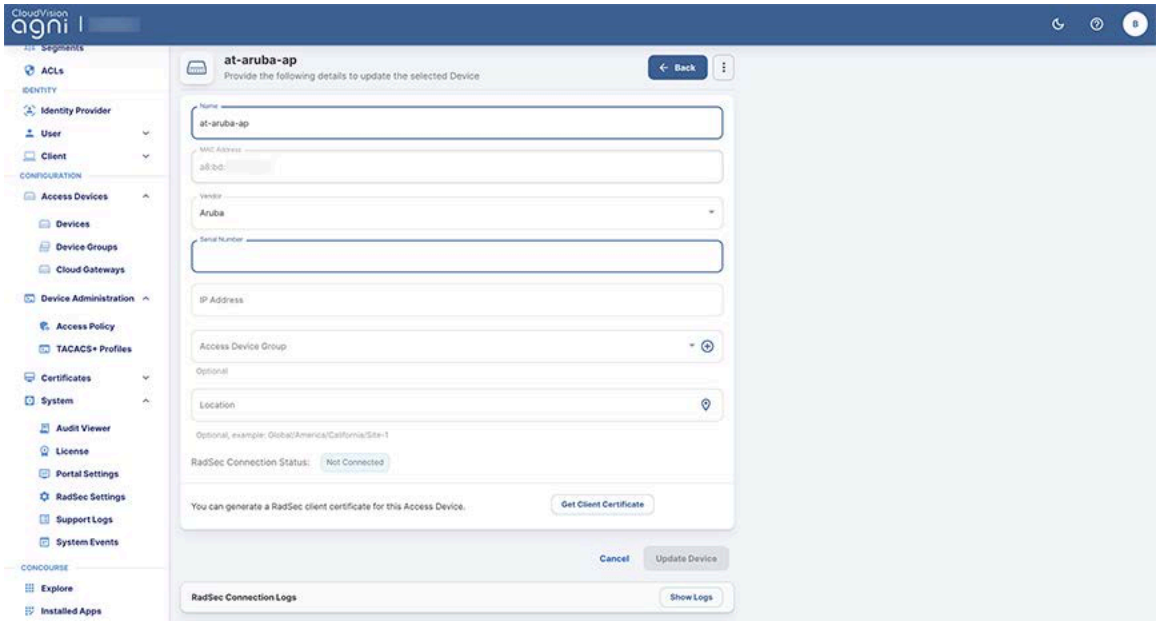
After selecting one of the Generate Certificate options, enter the following details:

- **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 12-4: Device Details

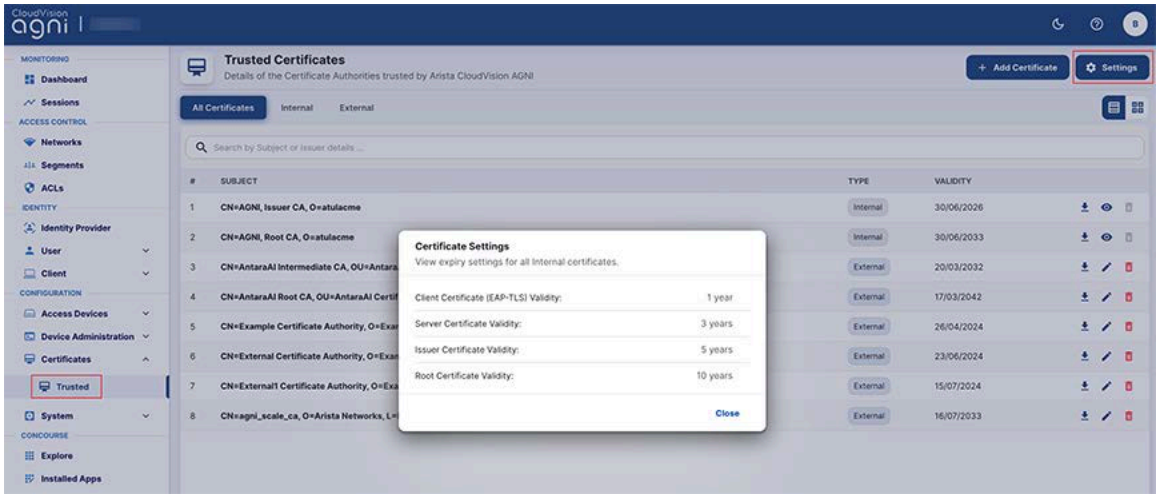


12.1 Viewing the Certificates

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 12-5: 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.

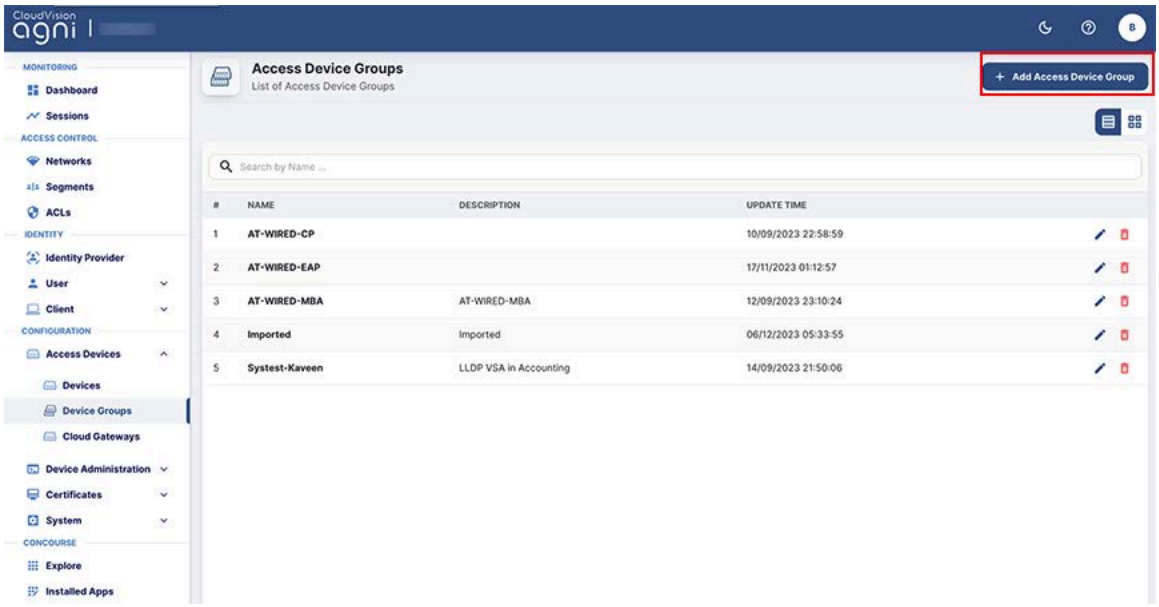
12.2 Configuring Device Groups

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).

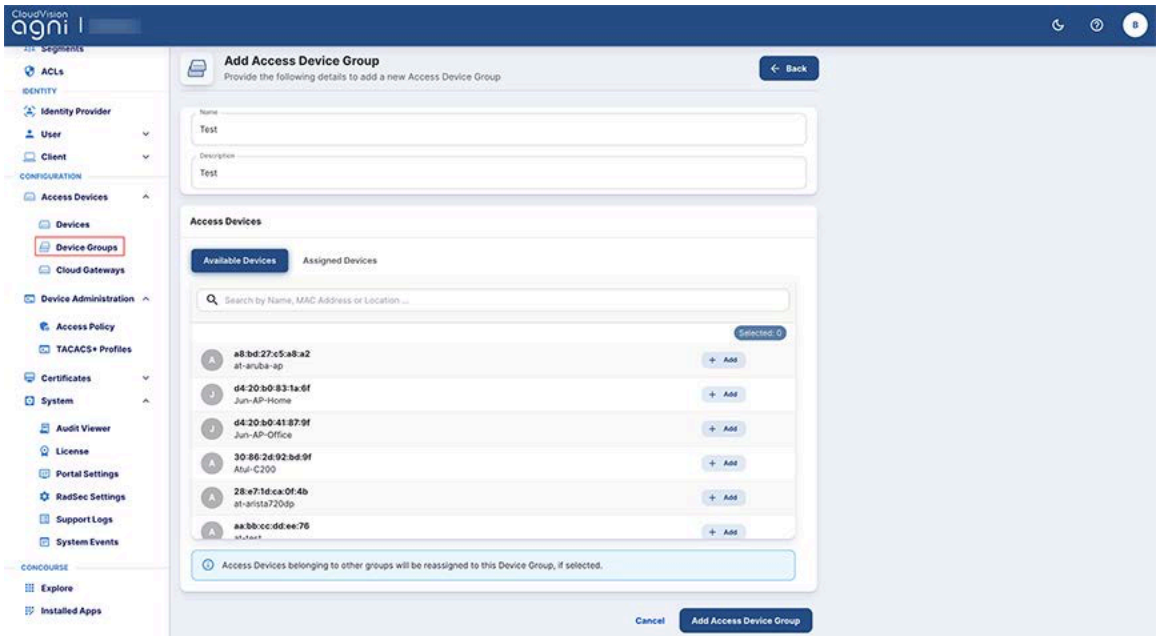
Figure 12-6: Access Device Groups



- 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 12-7: Adding Access Device Groups



Chapter 13

Overview - TACACS Plus with AGNI

This section explains the process of configuring TACACS+ on AGNI and Arista switches.

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

13.1 Configuring TACACS Plus 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.

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

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

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

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

13.2 Enabling Device Administration on AGNI

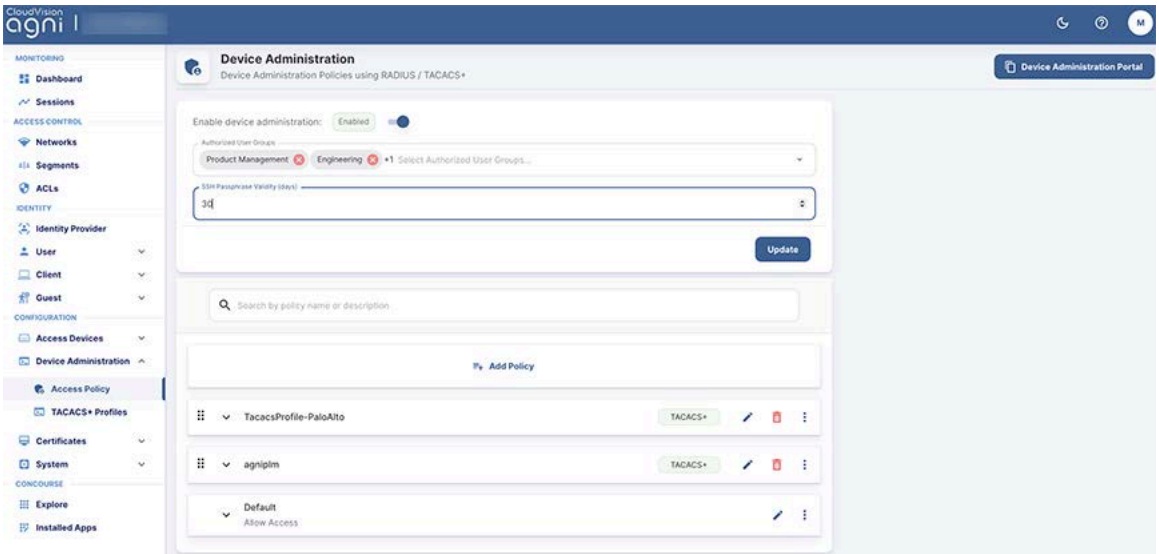
For TACACS+ to function correctly, enable Device Administration on AGNI and specify the authorized user groups. Users belonging to the authorized user groups should log in to the Device Administration portal using their SSO and generate an SSH Password. Using this SSH password, administrators can log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

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

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

> **Note:** he 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 13-1: Device Administration Enabled with Passphrase Validity



13.3 Configuring TACACS Plus on AGNI

Configure TACACS+ on AGNI by creating a TACACS+ Profile and applying the Profile through an Access Policy. To do this:

Navigate to **Device Administration** > **TACACS+** > **Profiles**. Click the **+Add TACACS+ Profile** button.

The Add TACACS+ Profile page is displayed (see image below).

Figure 13-2: TACACS+ Profile Creation

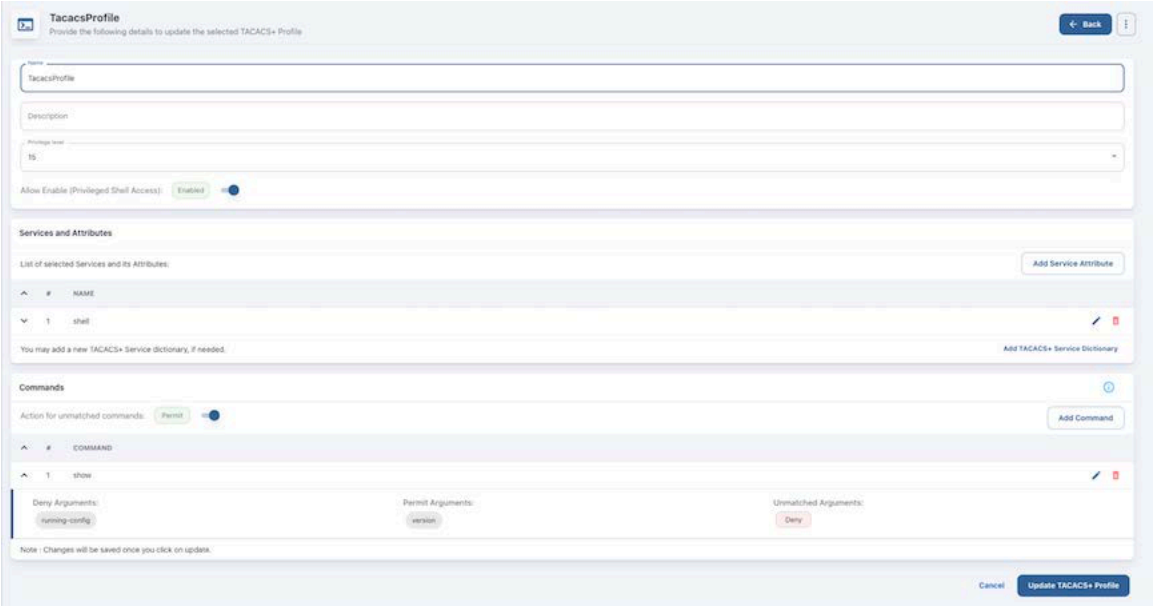
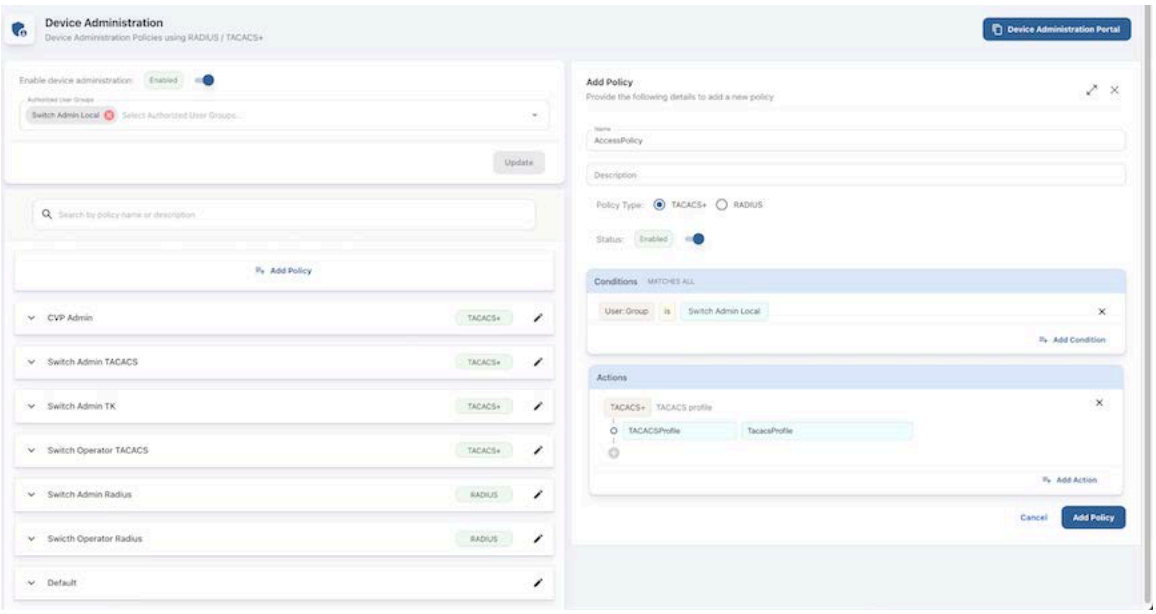


Figure 13-3: Adding TACACS+ Access Policy



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

Figure 13-4: Creating TACACS+ Policy Details

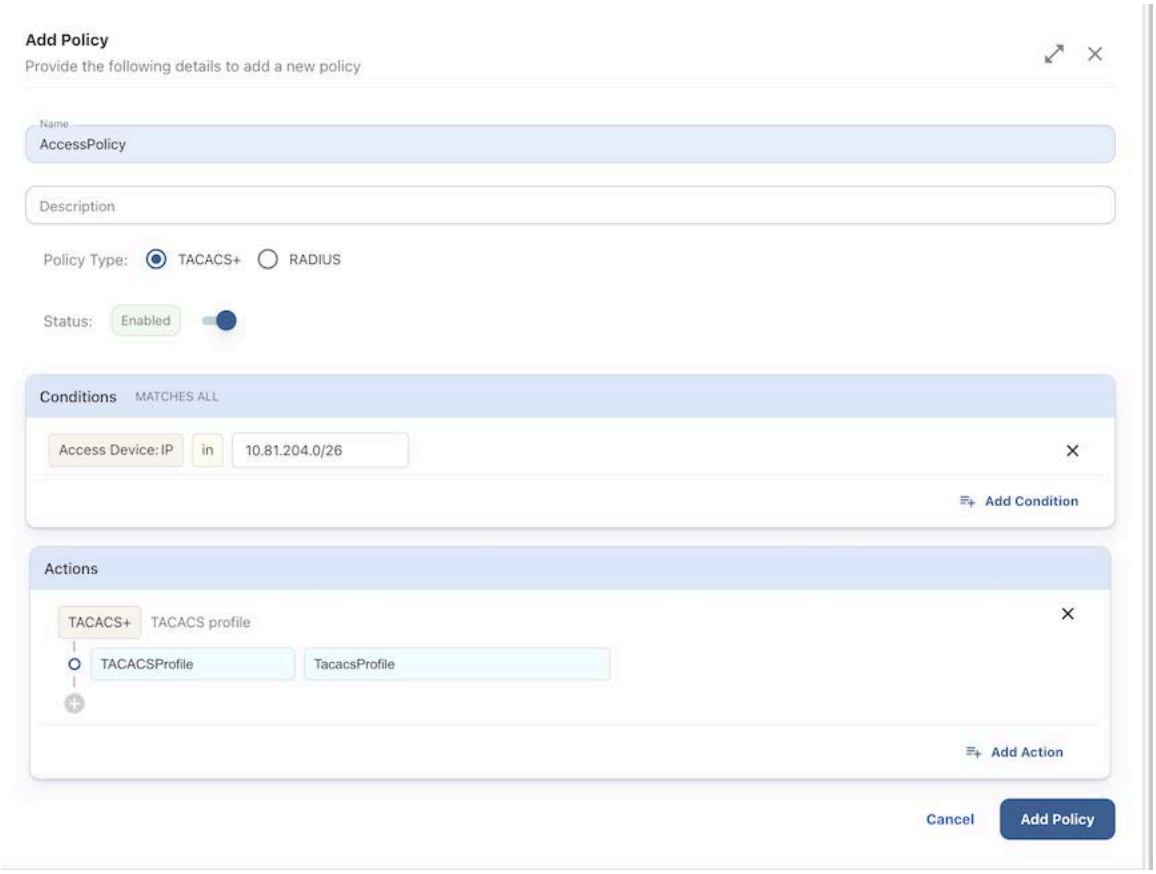
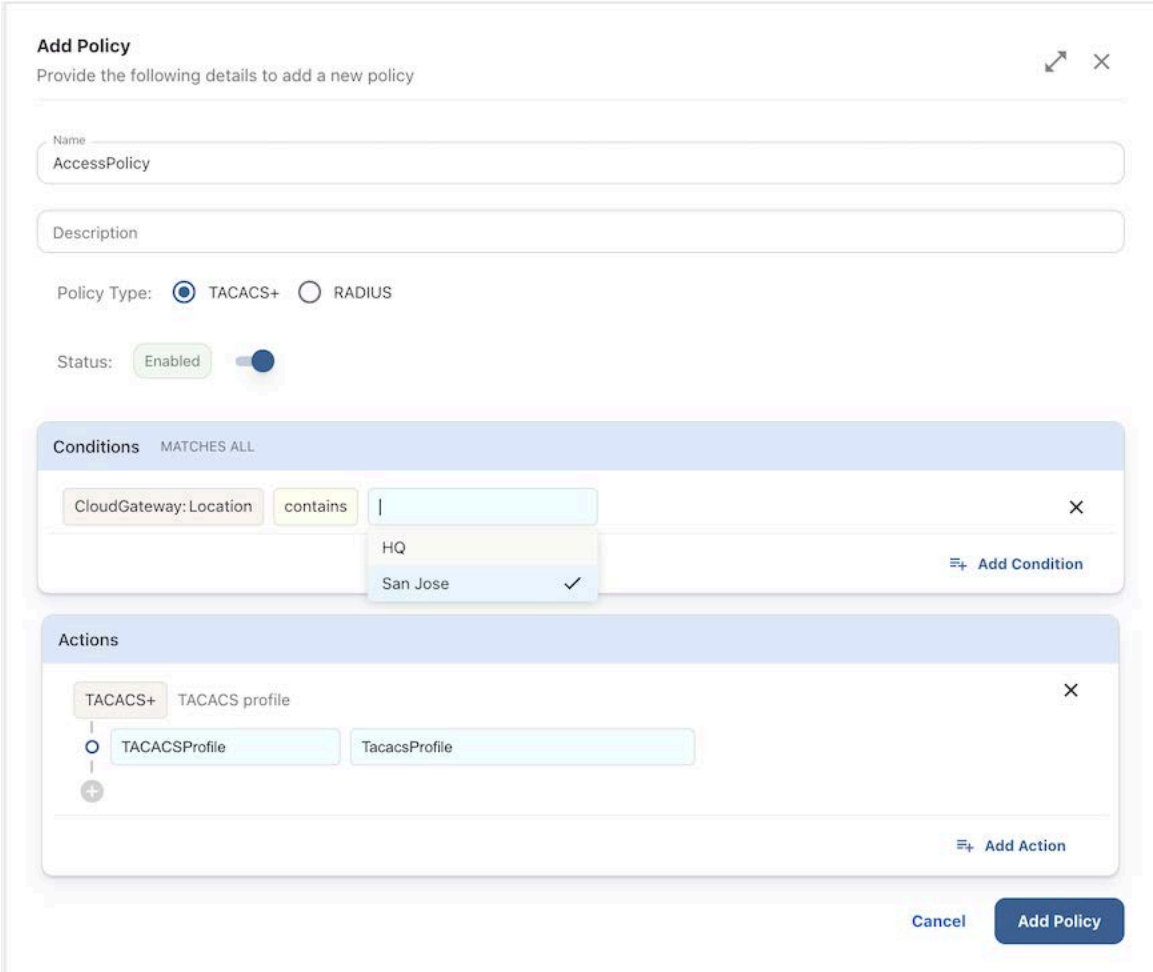


Figure 13-5: Creating TACACS+ Policy Details-Conditions



13.4 Monitoring TACACS Plus on AGNI

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

Figure 13-6: Monitoring Session Details

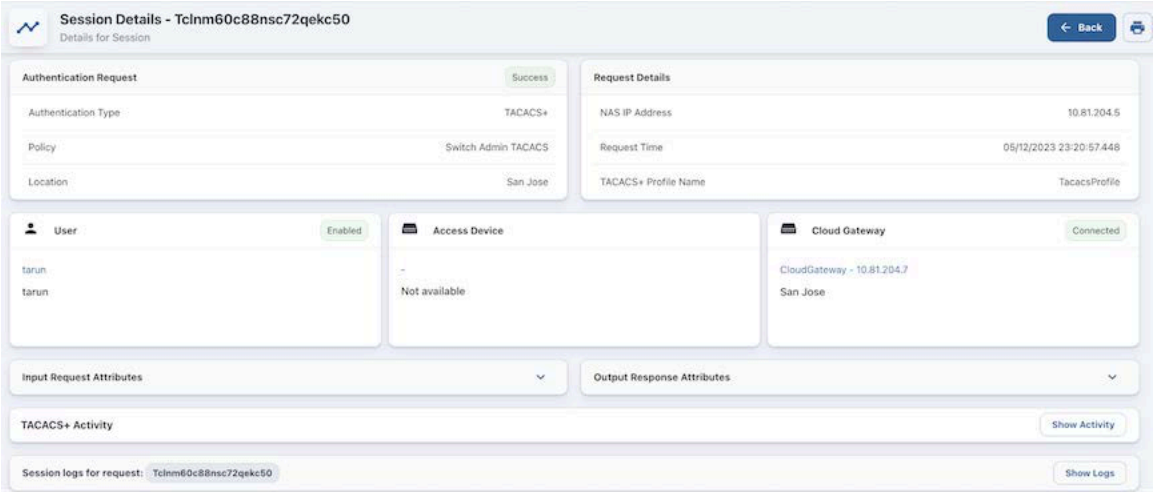
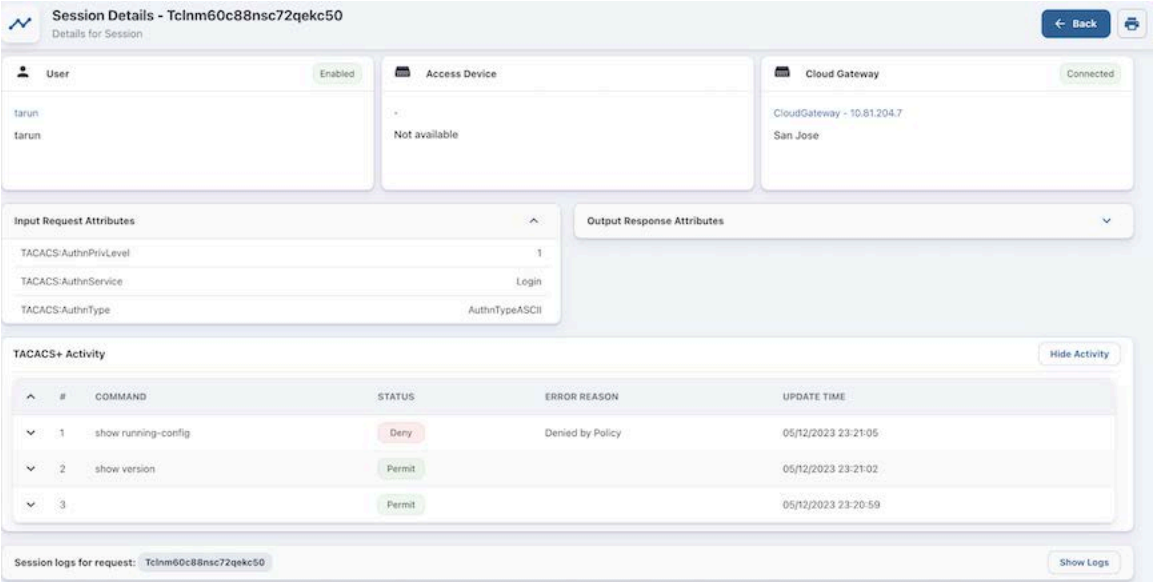


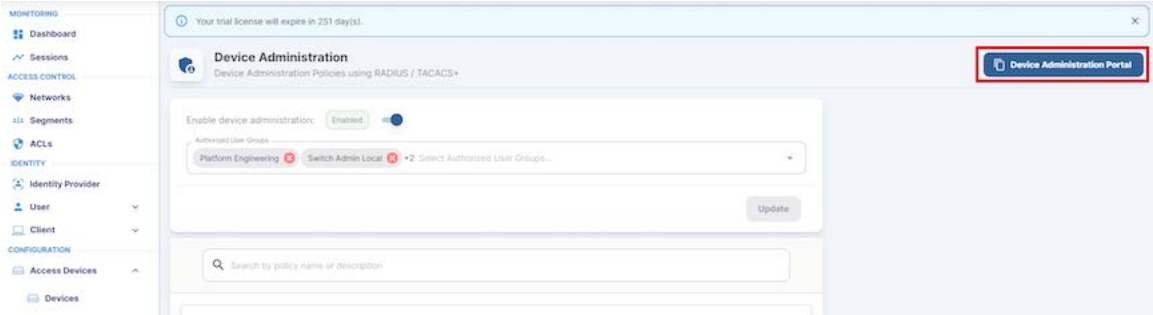
Figure 13-7: Monitoring TACACS+ Session Details



13.5 Accessing Device Admin Portal on AGNI

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

Figure 13-8: Device Admin Portal



Device administration functionality is accessible to users belonging to authorized user groups from the AGNI self-service portal. The self-service portal provides a browser-based shell 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 the 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 13-9: Device Admin Application for Mac OS

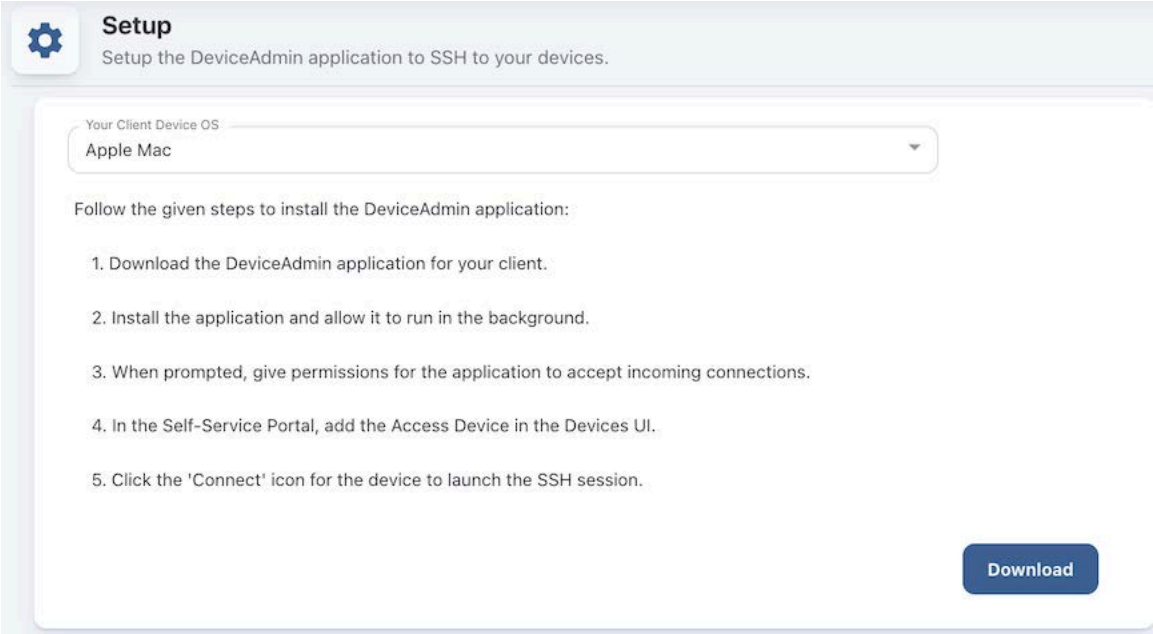
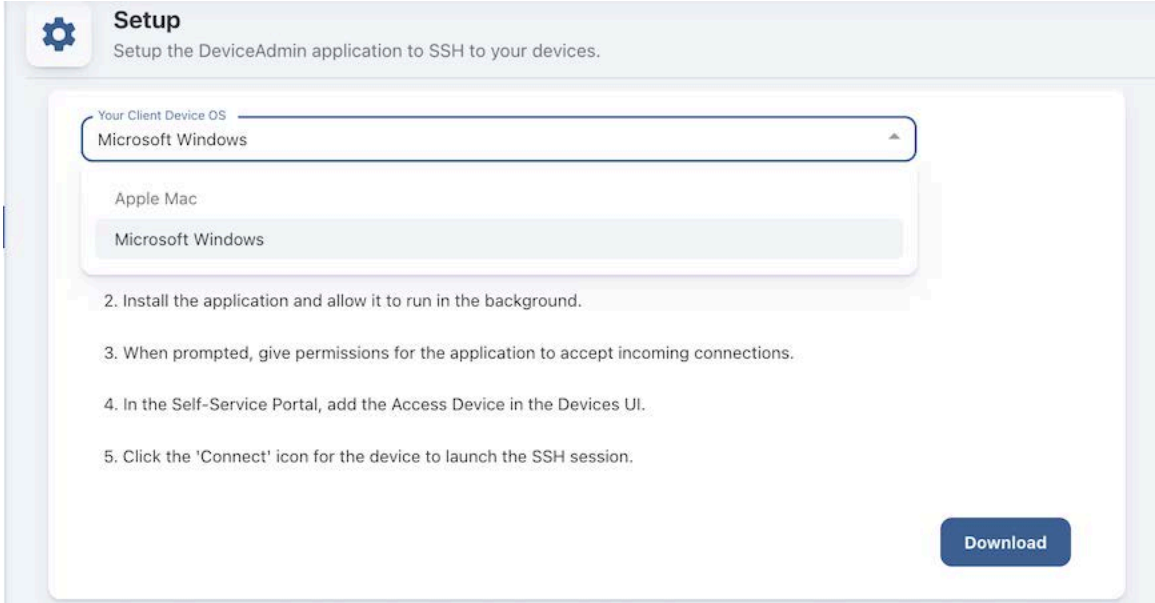


Figure 13-10: Device Admin Application for Windows



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).

> **Note:** The Device Login Credentials 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. (see images below).

Figure 13-11: Device Admin Portal

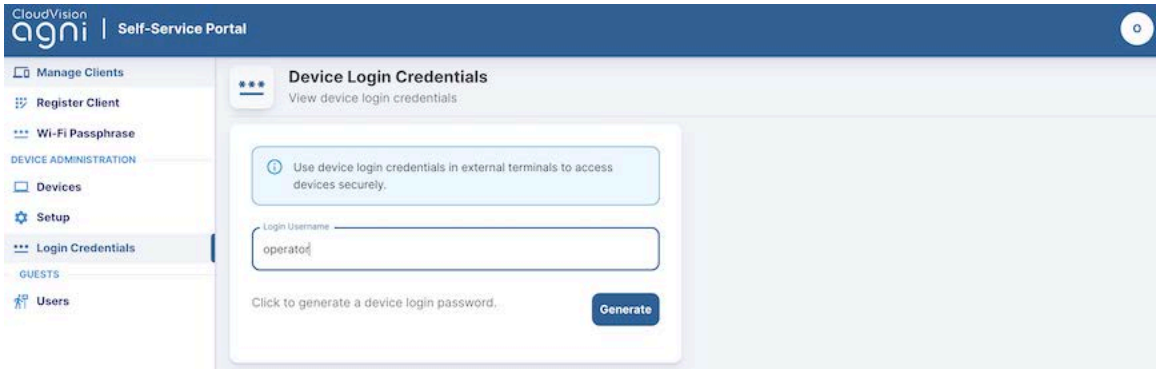
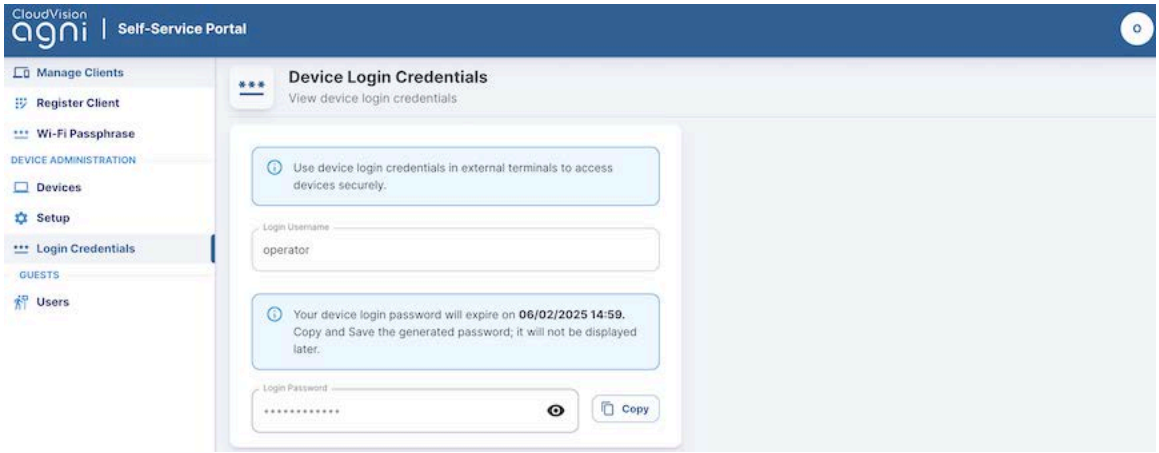


Figure 13-12: Device Login Credentials



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

Figure 13-13: TACACS+ Authorization Allowed and Denied 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#
```

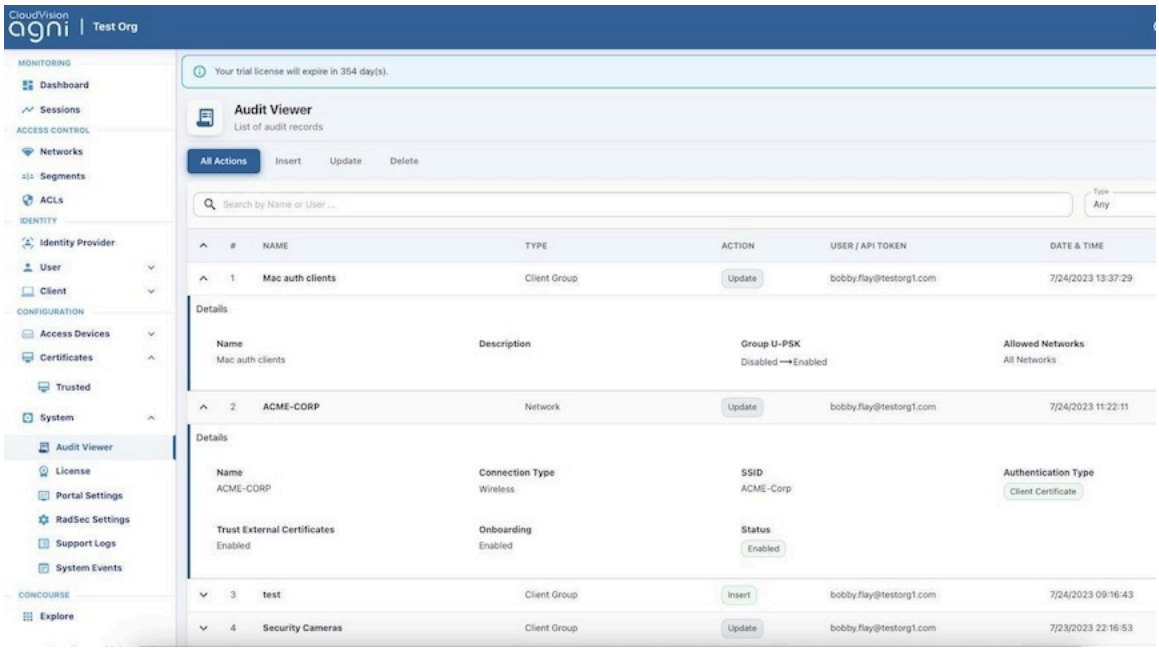
Chapter 14

System

This section captures the administrative tasks at the system level.

14.1 Audit Viewer

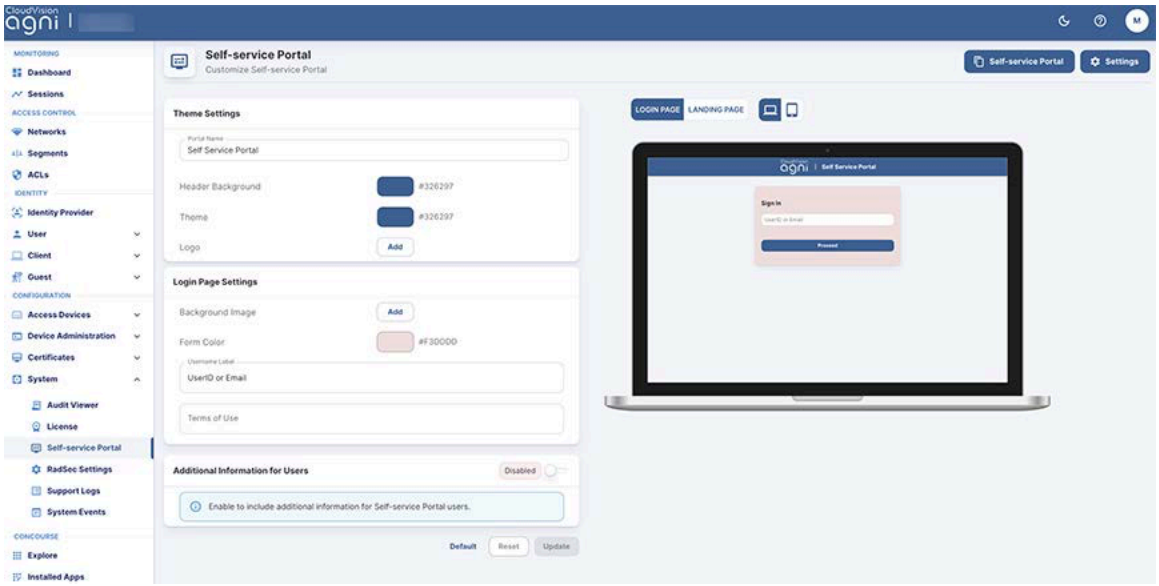
Audit Viewer captures details about system configuration modifications. This page helps to track the changes performed on the system, such as the owner details, modified details, and the timestamp information.



14.2 Self-Service Portal Settings

The Self-Service Portal Settings can be used to customize the portal user experience. AGNI allows the customization of logos, text, images, and themes on the captive portal page as per the requirements of your organization. The customization can also be applied to the landing and login pages.

Figure 14-1: Self-Service Portal

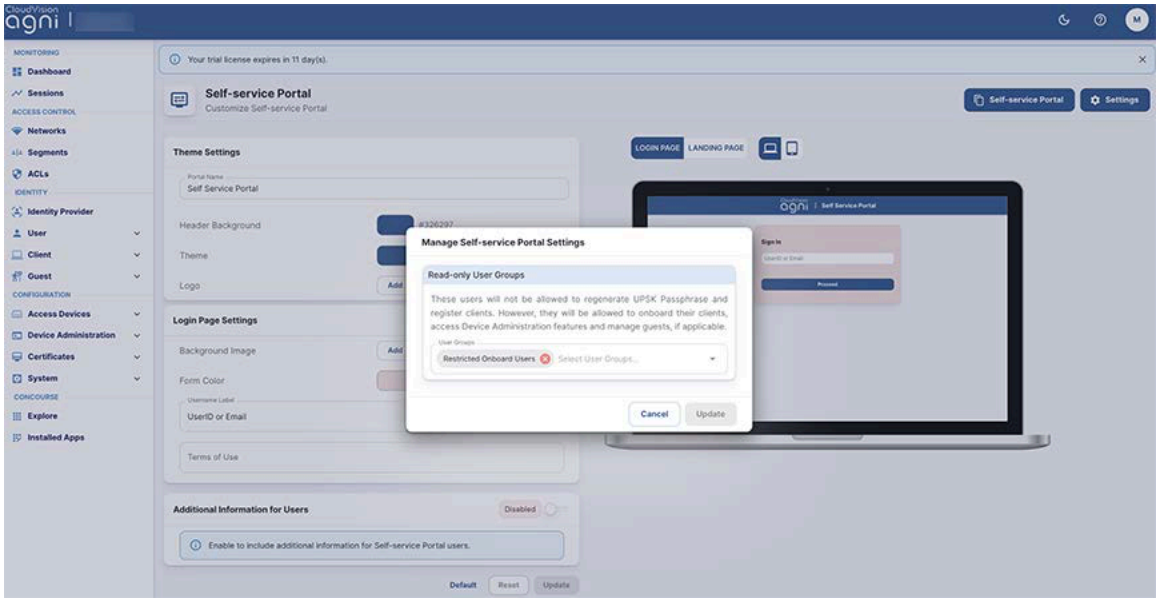


You can also manage the access privileges of user groups by modifying the Self-Service Portal settings. To modify:

- 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 14-2: Manage Self-Service Portal Settings

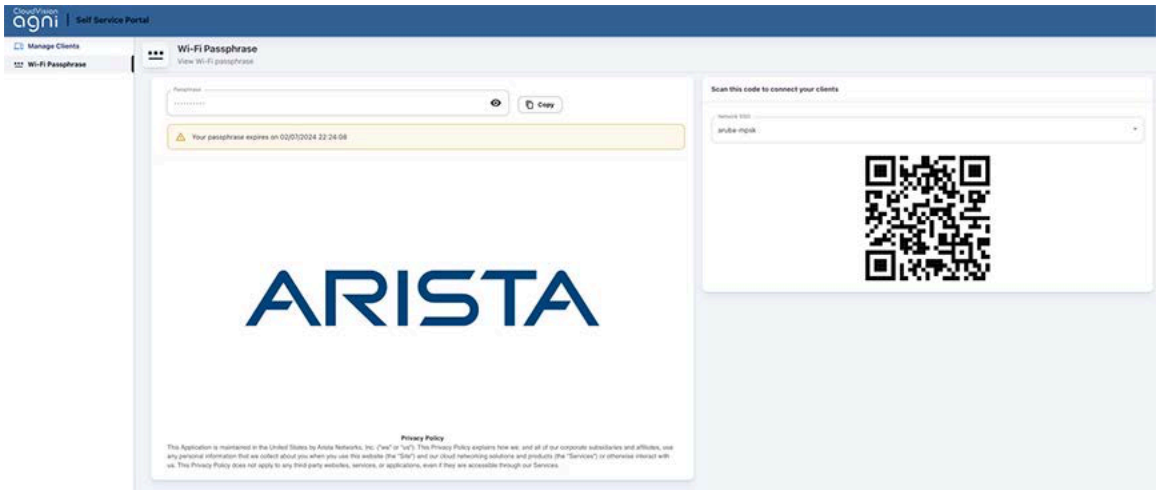


Note: User Groups with read-only permission cannot add, update, or delete clients using the AGNI portal or APIs (see image).

Figure 14-3: Self-Service Portal Clients with Read-only Access

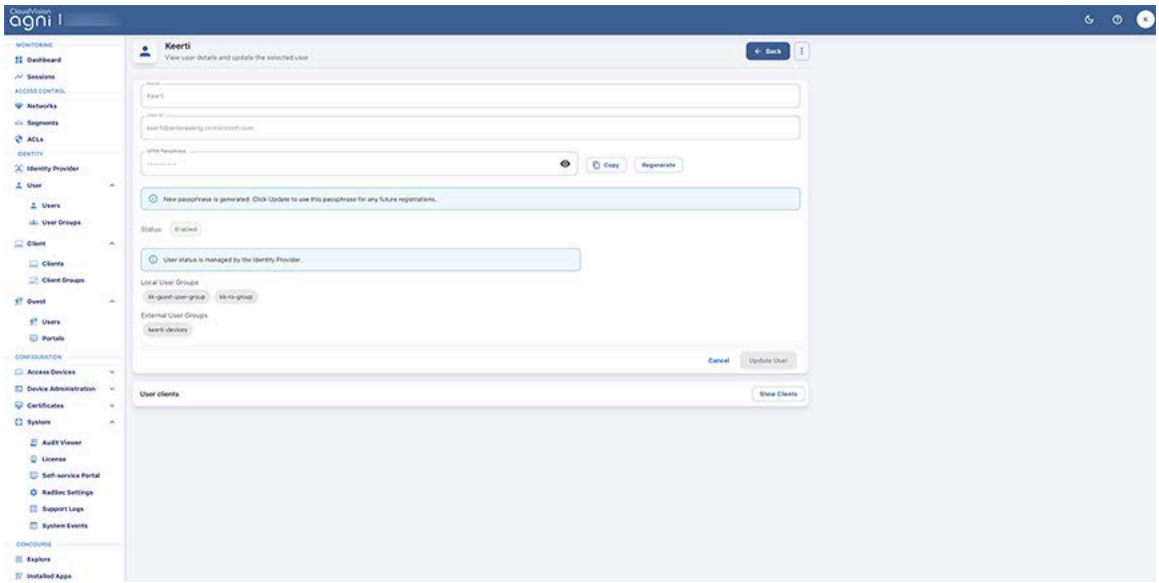
Additionally, the users with read-only access cannot regenerate and update the passphrase (see image).

Figure 14-4: Self-Service Portal WiFi Passphrase (client with Read-only access)



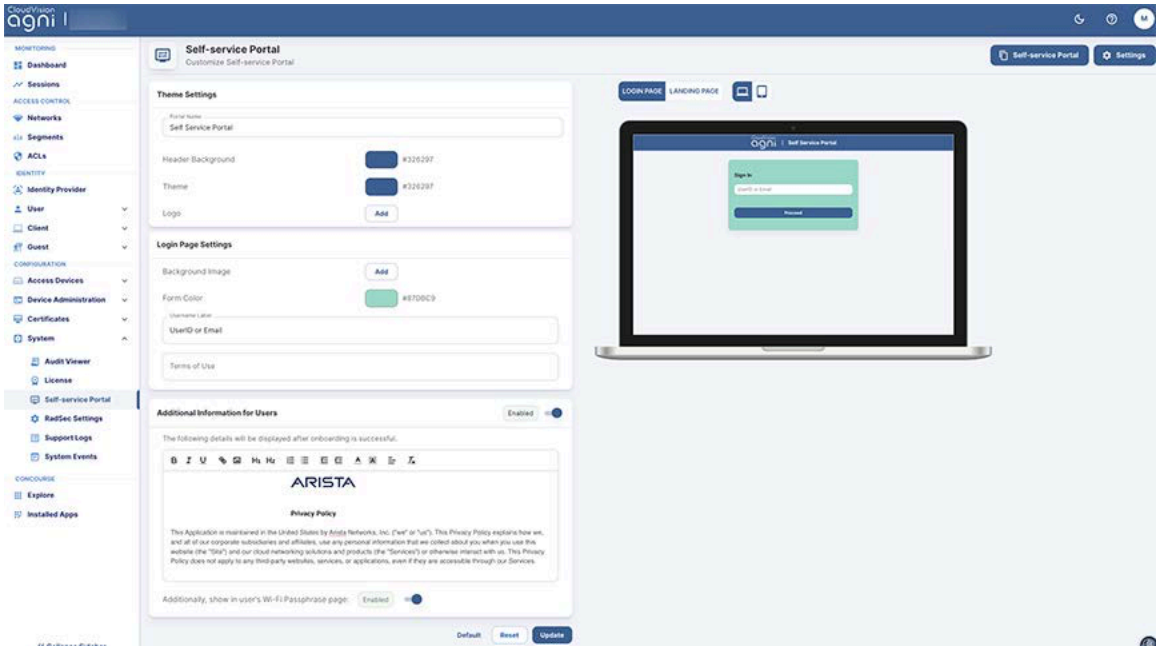
Note: The users with read-only access privileges can contact the AGNI administrator if they want to regenerate their passphrase. The AGNI administrator can regenerate the passphrase from the User accounts page (see image).

Figure 14-5: 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 14-6: 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). The custom text is displayed in the Wi-Fi Passphrase window of the Self-Service portal:

Figure 14-7: Self-Service Portal Wi-Fi-Passphrase

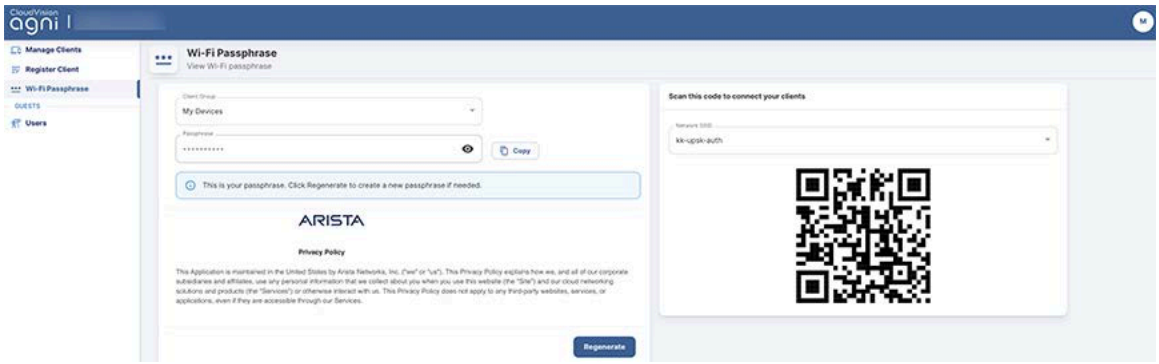


Figure 14-8: Self-Service Portal Wi-Fi/UPSK-Passphrase

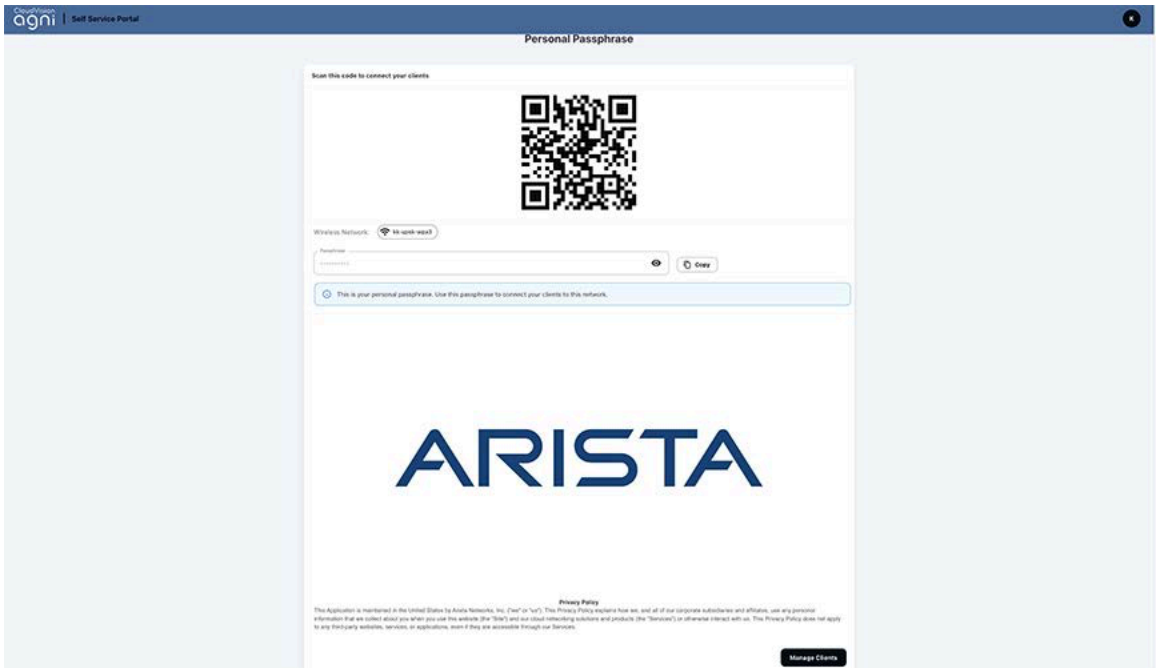
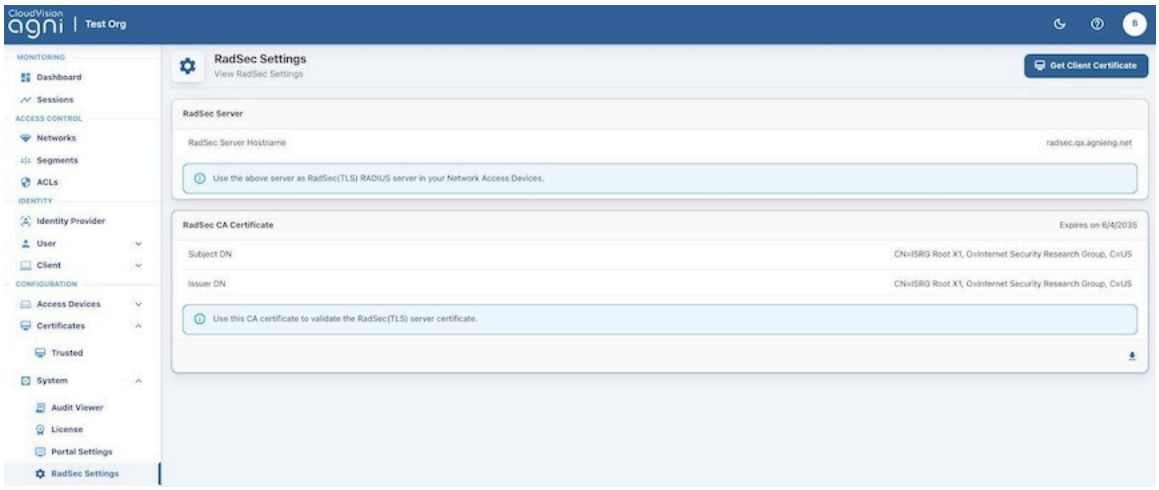


Figure 14-9: Self-Service Portal Registering a Client in the Native Onboarding page

14.3 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 a RadSec tunnel.

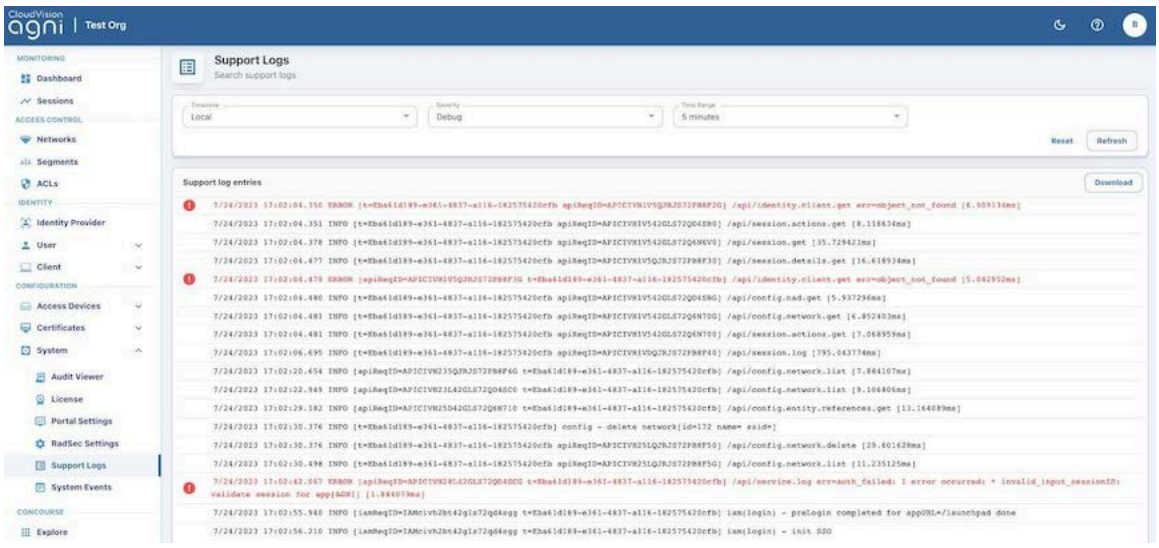
Figure 14-10: RadSec Settings



14.4 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 during troubleshooting.

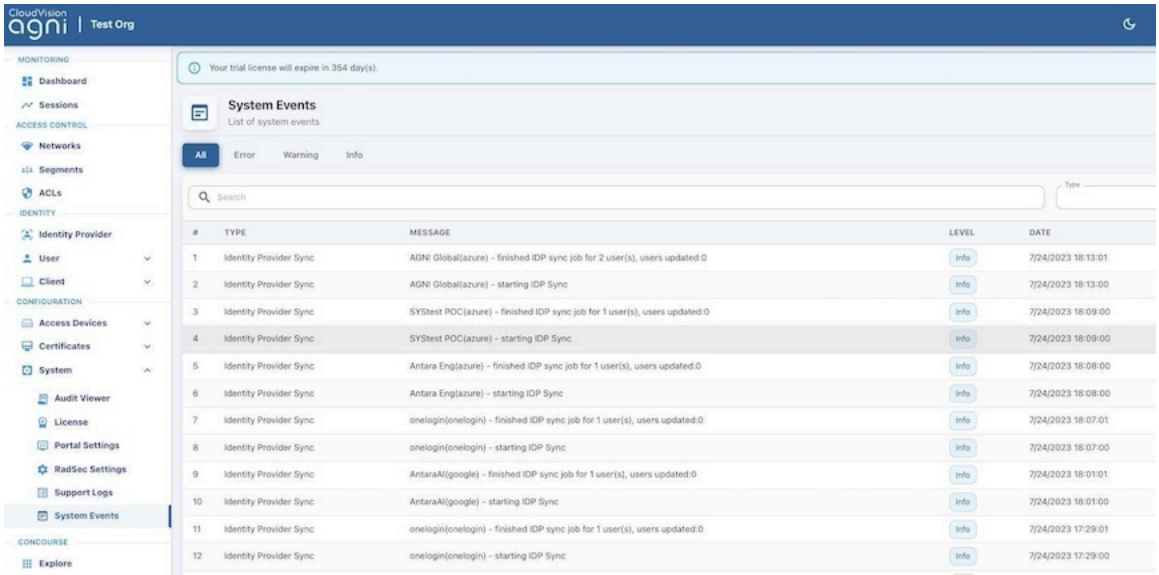
Figure 14-11: Support Logs



14.5 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.

Figure 14-12: System Events



14.6 Notification Settings

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

14.6.1 Configure 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 work-flow 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:

1. From the AGNI dashboard, click the **here** link in the "Email Settings are not configured. Click here to configure. OR
2. Navigate to **Configuration** > **System** > **Notification Settings** > **Email Settings**.
3. Configure the following SMTP server details: Customize the **Sender Name** and the **Reply Email** and click the **Email Templates** button (see image).
   a. **Sender Name**
   b. **SMTP Server** name
   c. **Username**

d. **Password**

e. **From email**

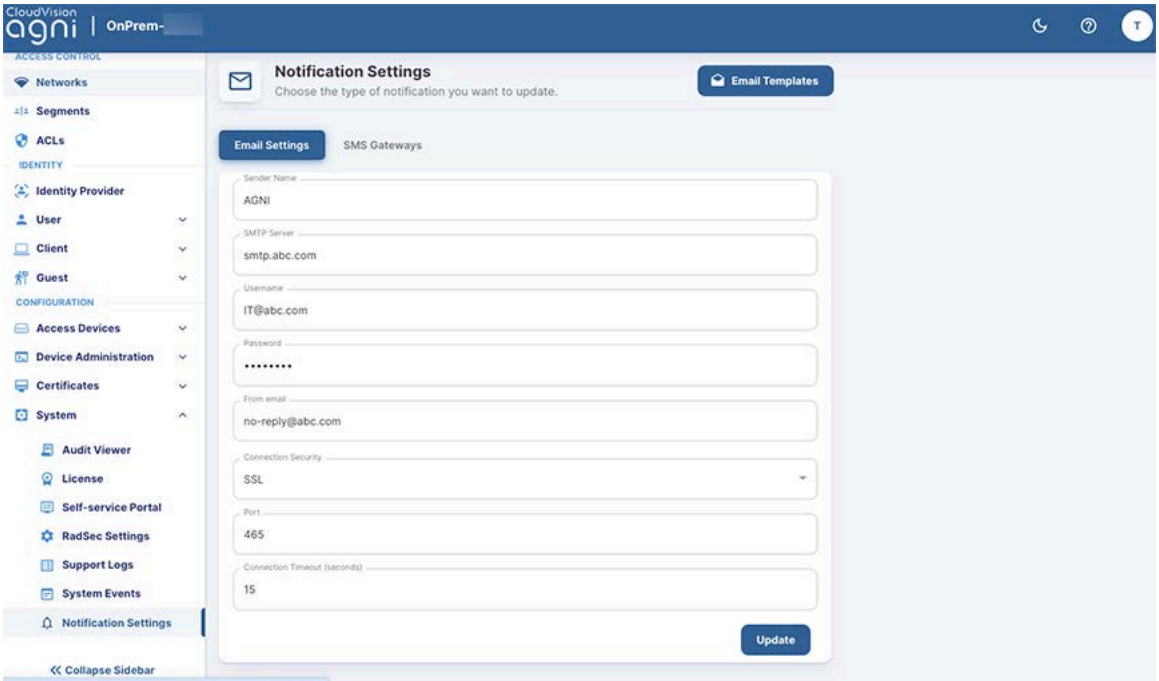
f. Choose the **Connection Security** as **None**, **SSL**, or **Start TLS**.

g. Enter the **Port** number

h. Enter the **Connection Timeout** in seconds.

4. Click the **Add** button to add the SMTP server.

Figure 14-13: Notification Settings- Email Settings



Once the email settings are added successfully, you can send a test email to verify the settings.

5. Click the **Send Test Email** down-arrow and enter the following details:

a. Email address of the recipient.

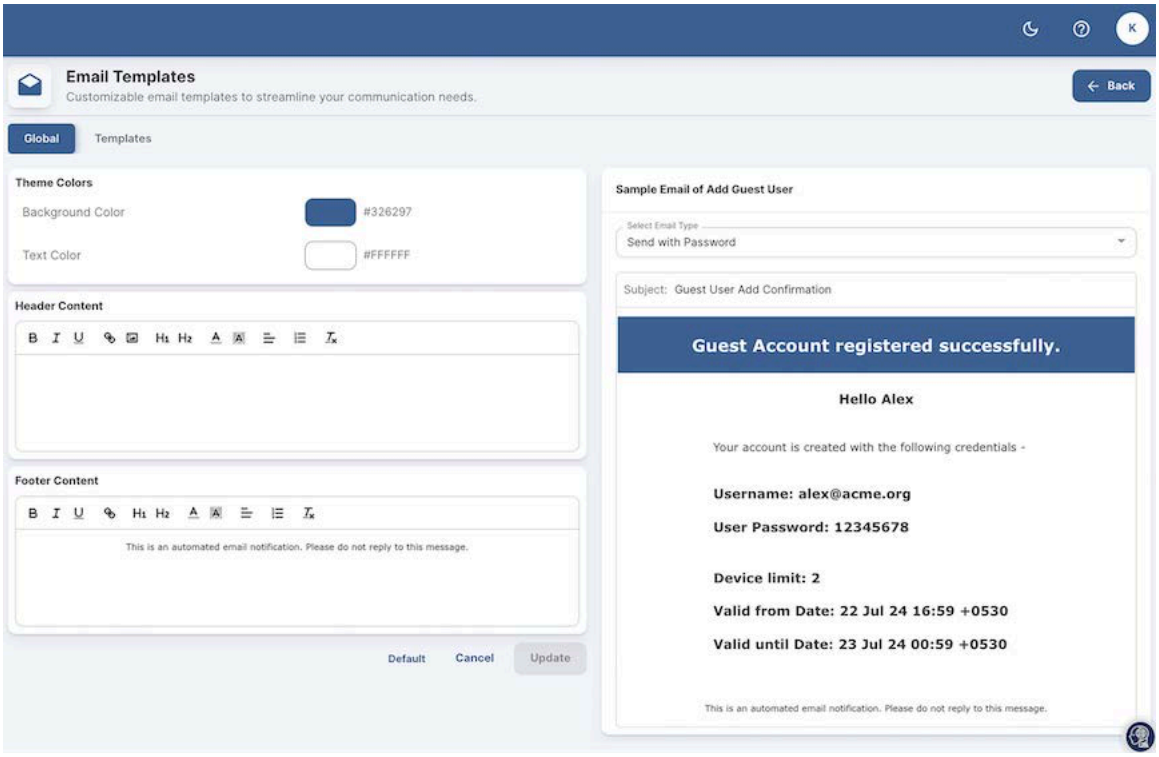
b. Subject of the email.

c. Email message.

d. Click **Send Email** button to send the email. An email sent successfully message is displayed at the top right corner of the page.

6. Click the **Email Templates** button at the top right to update the email templates. 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).

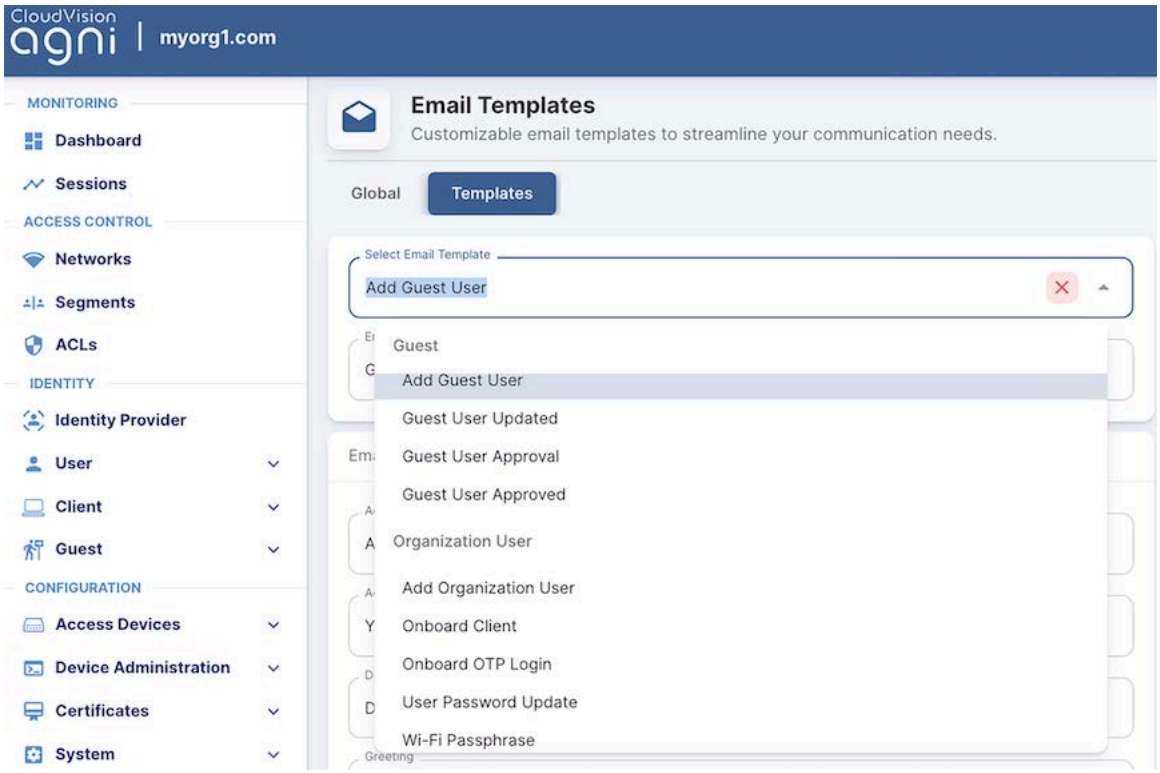
Figure 14-14: Email Settings - Global Settings



7. Select the **Templates** tab in the Email Templates page (see image).
8. Select the desired **Email Template** and customize the placeholder details (image):

a. In the **Select Email Template** field, choose one of the options from the Organizational User or Guest from the drop-down list (see image).

Figure 14-15: Email Template Settings



b. Enter the Email Subject.

c. Customize the text in the Email Placeholders section.

d. On the right side, choose one of the options (**Send with Password** or **Send with Passphrase**) from the **Select Email Type** field.

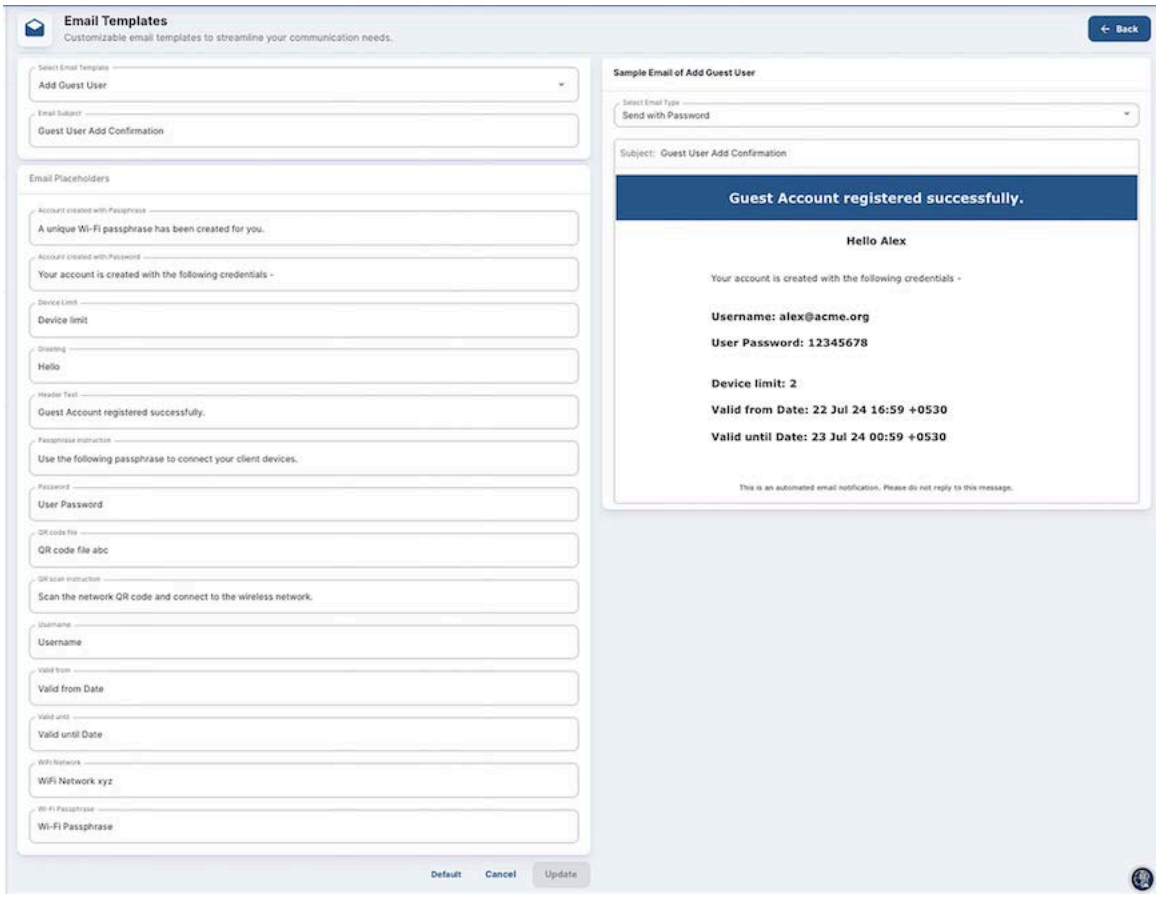
e. Preview the Email template and email customizations displayed on the right side and modify, if required (image).

f. 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.

Figure 14-16: Email Templates Example



14.6.2 Configuring SMS Gateway

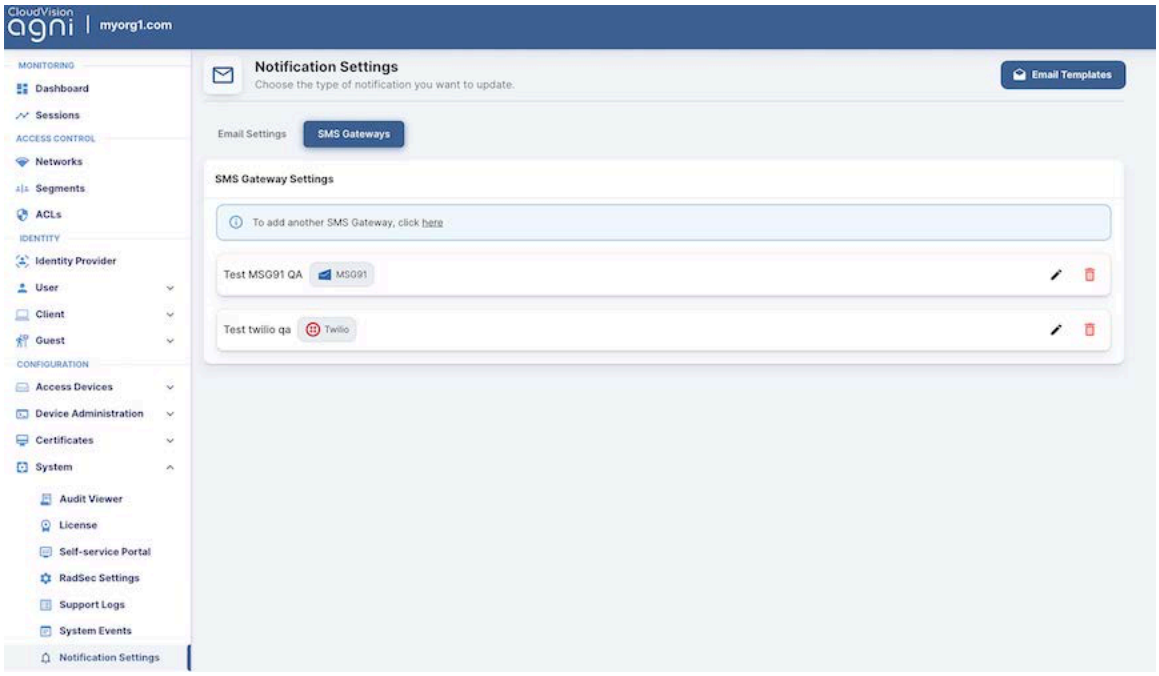
Configure SMS gateway to enable registered guest users to receive SMS notifications whenever a guest account is added, modified, or disabled. AGNI supports two SMS Gateway configuration:

- 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, log in as an admin and perform the following steps:

Navigate to **Configuration** > **System** > **Notification Settings** > **SMS Gateways**

Figure 14-17: Notification Settings - SMS Gateways

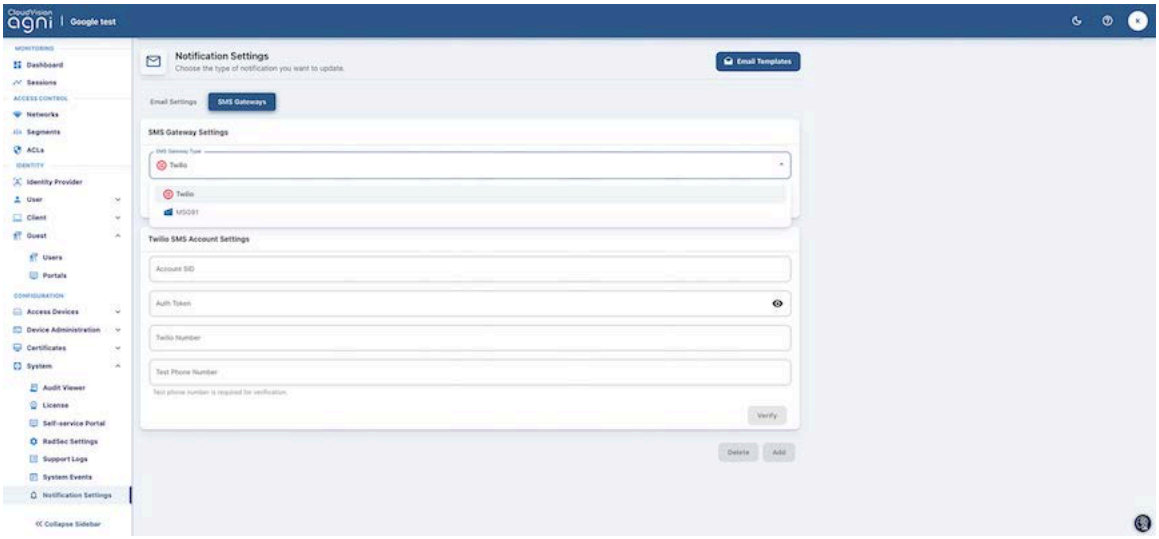


14.6.2.1 Configuring the Twilio SMS Gateway

To configure the Twilio SMS gateway:

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

   Figure 14-18: SMS Gateway - Twilio Settings



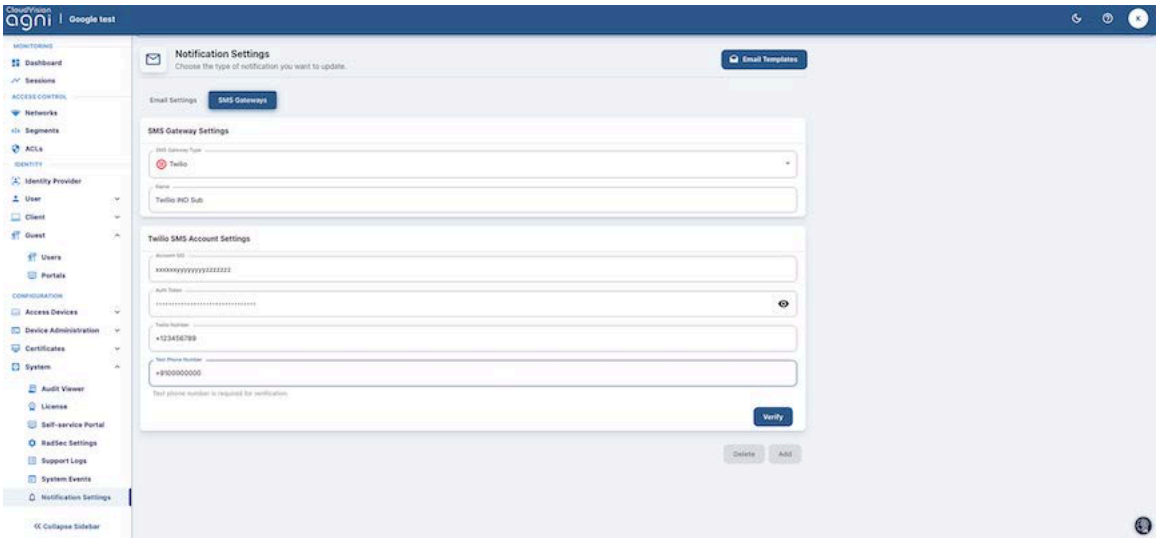
3. In the Twilio SMS Account Settings section, enter the details:
   a. Account SID

b. Auth Token

c. Twilio Number

d. Test Phone Number

Figure 14-19: SMS Gateway - Twilio Settings Details



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

Related information

https://arista.my.site.com/AristaCommunity/s/article/Configuring-SMS-Gateway-in-AGNI

14.6.2.2 Configuring the MSG91 SMS Gateway

To configure MSG91 SMS gateway:

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

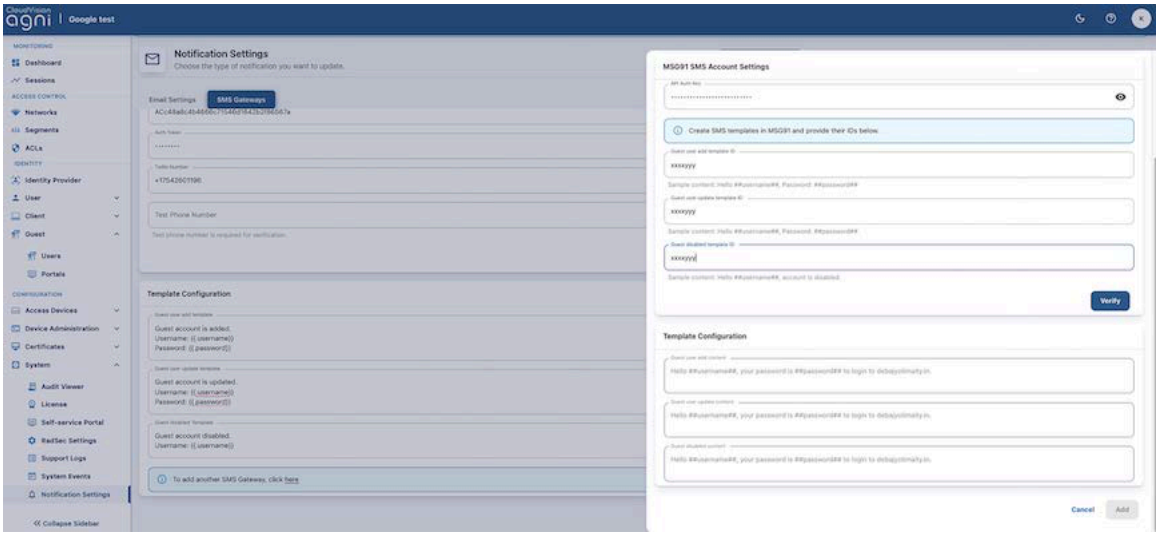
a. Guest user add content

b. Guest user update content

c. Guest disabled content

6. Click the **Add** button to add the details.

Figure 14-20: SMS Gateway - MSG91 Settings



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

Related information

https://arista.my.site.com/AristaCommunity/s/article/Configuring-SMS-Gateway-in-AGNI

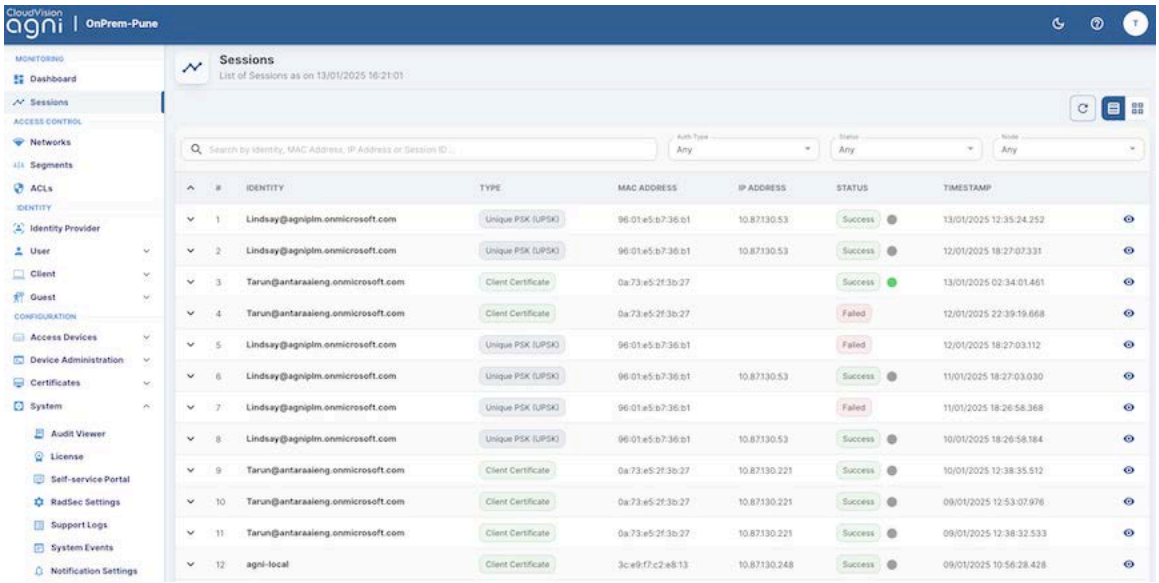
Chapter 15

Sessions

This section provides 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 the list of devices and the corresponding session details.

> **Note:** The session details of each node in the cluster can be viewed from every node. For example, you can view the session details of Standby and Auxiliary nodes from the Principal node by selecting the specific node in the Nodes drop-down field. Similarly you can view the session details of other nodes from the Standby and Auxiliary nodes.

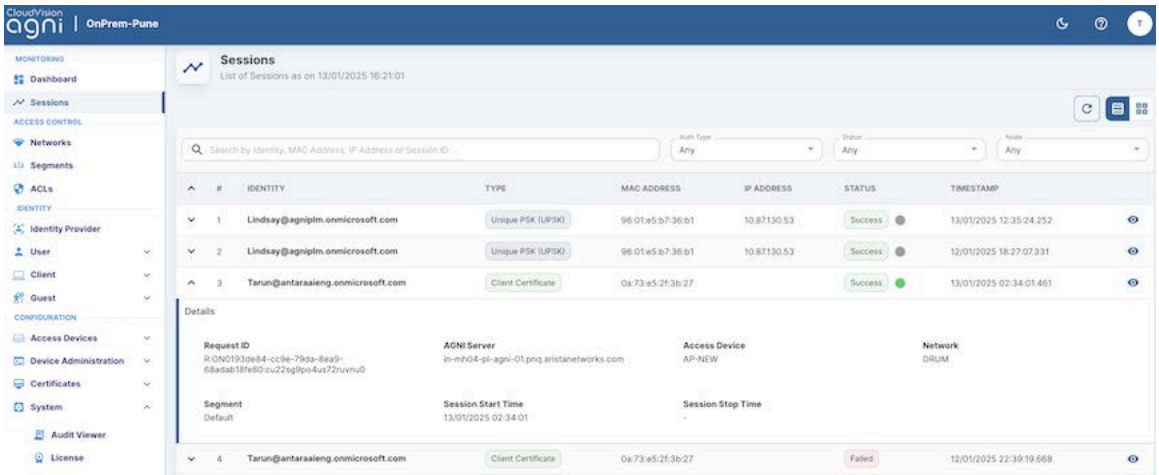
Figure 15-1: Monitoring Sessions



Click the down arrow for a session to view the details.

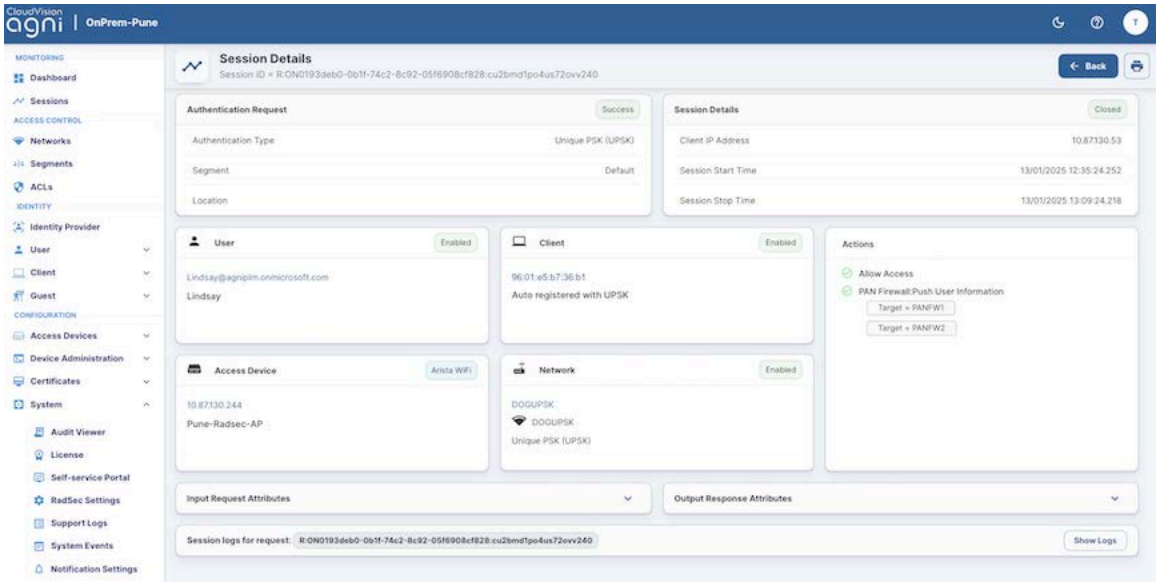
In this section you can view which node in the cluster is serving the authentication request.

Figure 15-2: Session Details



Click the **eye** icon at the far right column to view the details of that session. (see image).

Figure 15-3: Monitor Session Details



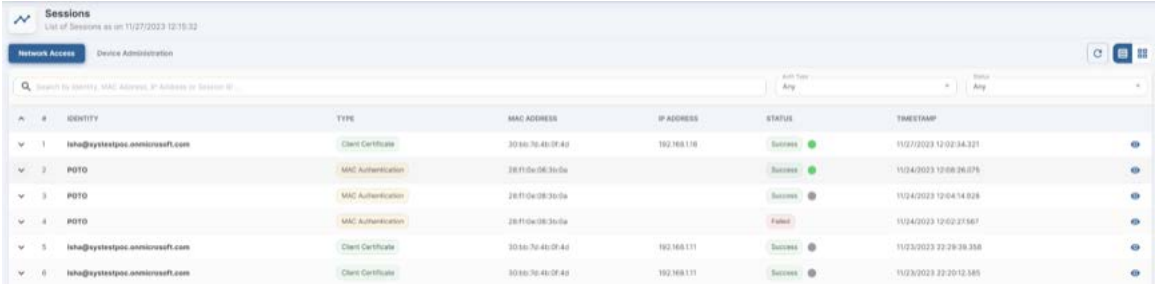
15.1 On-Demand Disconnecting a Client from the Network

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 at on-demand, navigate to the Sessions menu on the left pane of the dashboard and perform the following steps:

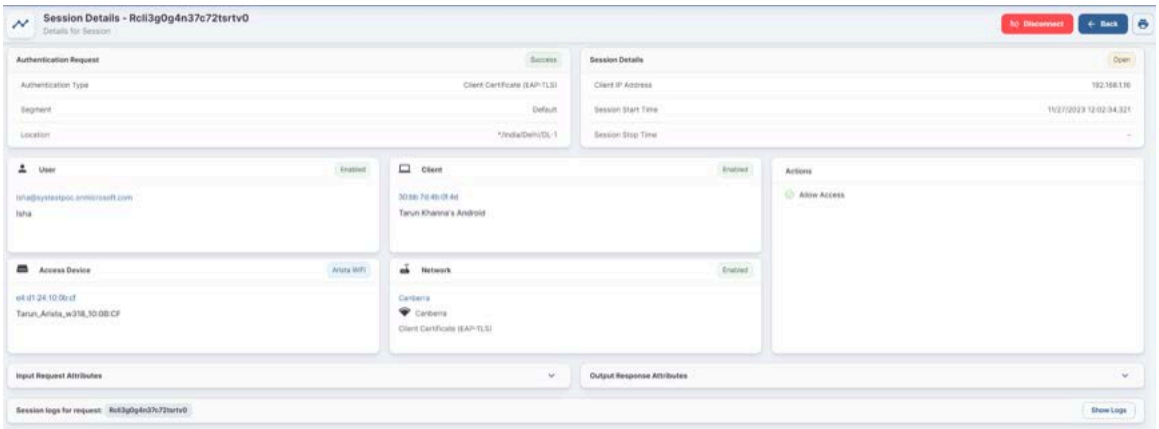
1. Open the client's active session (see image below).

   Figure 15-4: Client Session Details



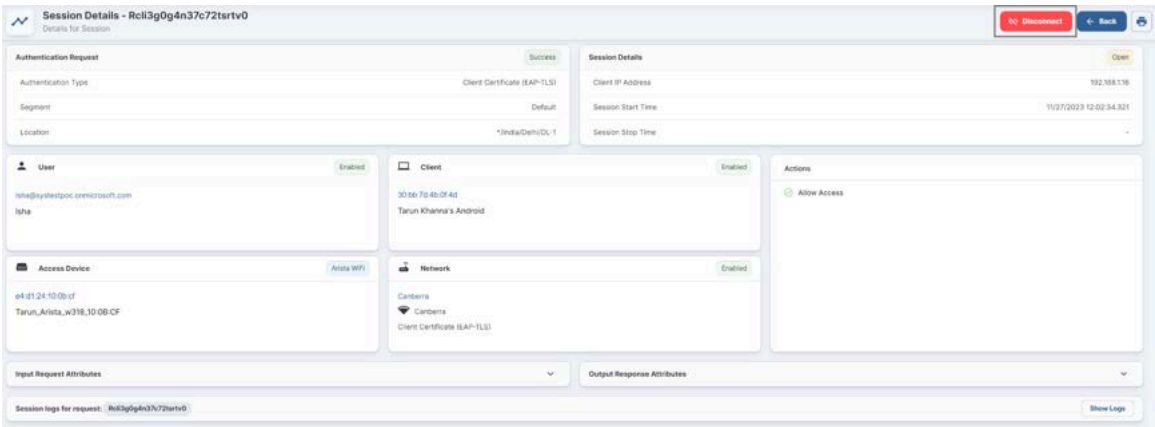
2. Click the **eye** icon to open the active session details (see image below).

   Figure 15-5: Client Session Details Page 2



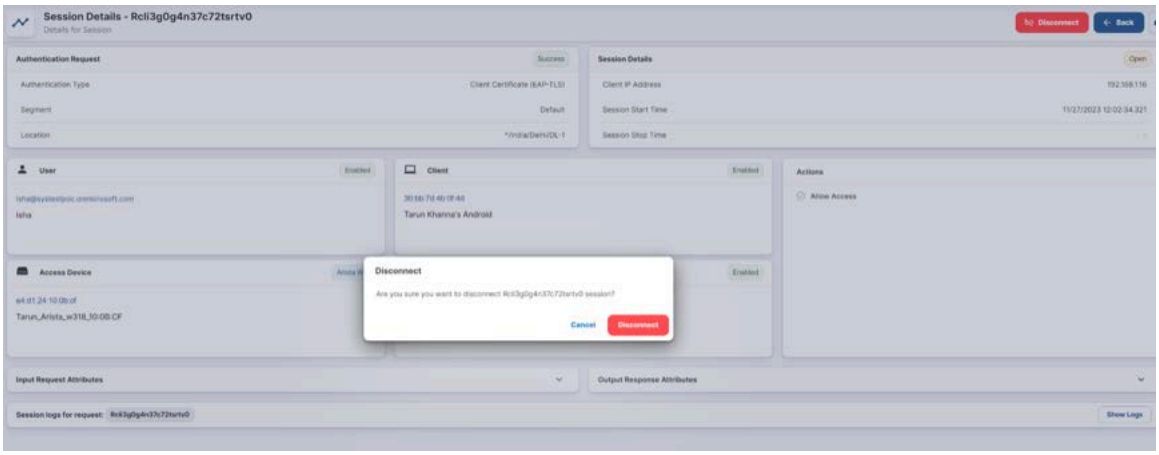
3. Click the **Disconnect** button.

   Figure 15-6: Client Session Details Page 3



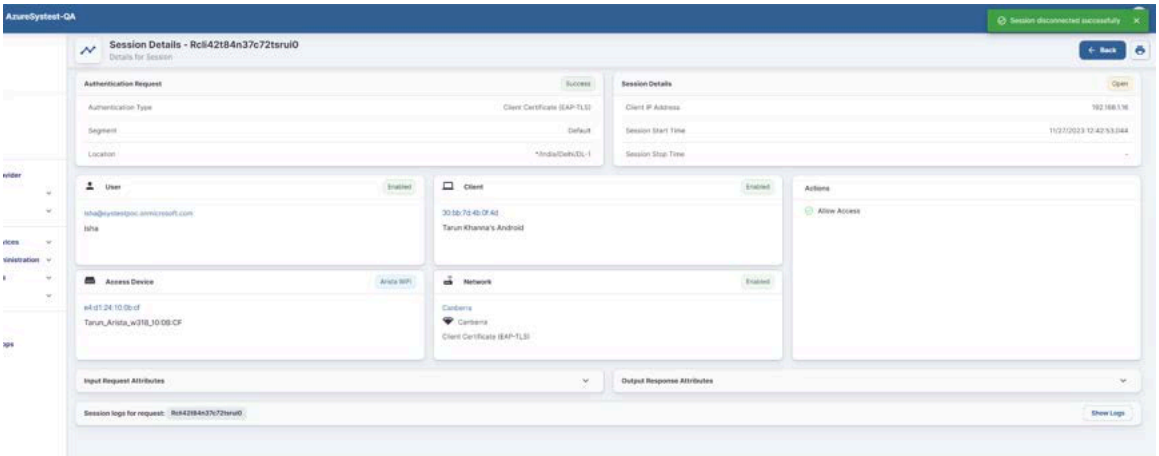
AGNI dashboard displays a confirmation message for admin approval (see image below).

Figure 15-7: Client Sessions Details Page 4



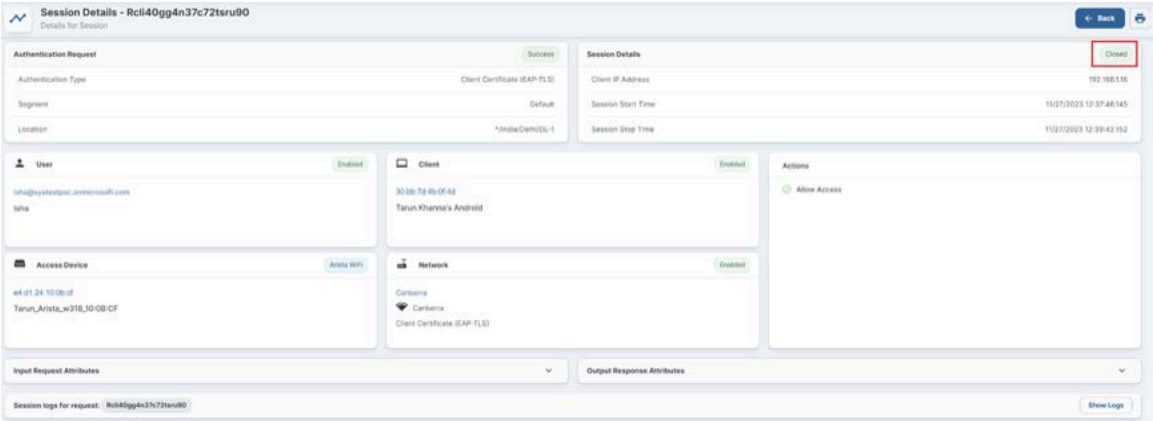
4. Click **Approve**. A Change of Authorization (COA) disconnect request is sent to the client device and the device gets disconnected from the network.

Figure 15-8: Client Session Details Page 5



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

Figure 15-9: Client Session Details Page 6



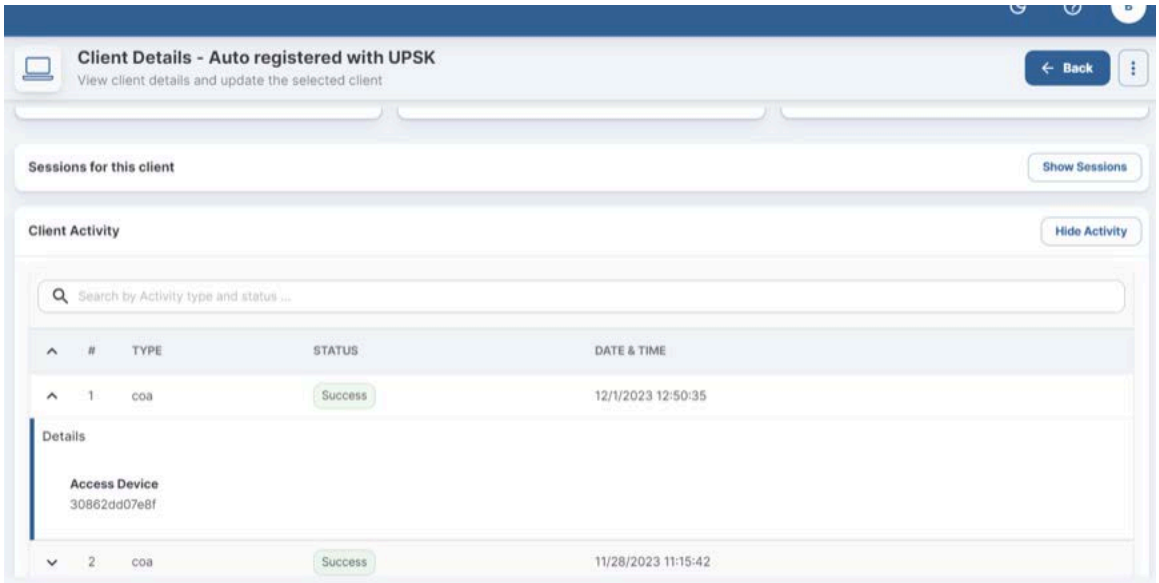
> **Note:** AGNI supports distributed CoA. That is, if an authentication request was served by an Auxiliary node, then the session can be disconnected from the Principal, Standby or any other Auxiliary nodes. This is true for all nodes in the cluster.

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

Figure 15-10: Disconnect Debug Logs

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

Figure 15-11: CoA Action Status



Chapter 16

Troubleshooting

16.1 Monitoring

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

16.2 Dashboards

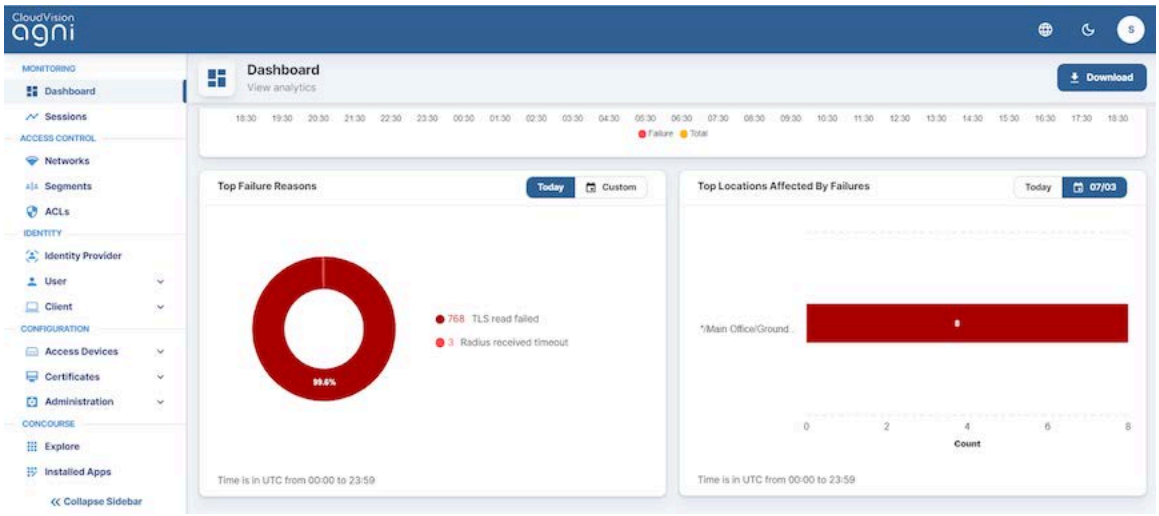
View the user and client authentication details and access device status from the AGNI dashboards. The Sessions page captures the authentication trend with the details on the total and failed authentications over a specified period.

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

Figure 16-1: AGNI Dashboard and Session Trend

Charts 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 16-2: AGNI Dashboard and charts



16.3 Sessions

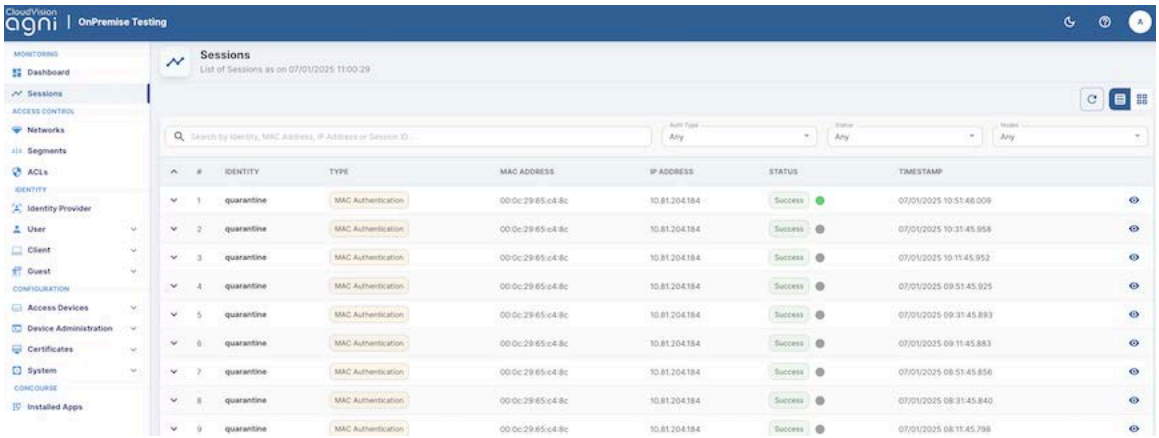
Sessions provide a runtime view of authentication trends. All the authentication details from 802.1X, UPSK, Captive Portal, and MBA are captured in this view.

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

- MAC address
- Identity
- IP address
- Session Identifier

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

Figure 16-3: Monitoring Current Sessions



To view the session details, click on the **eye** icon. This action displays detailed session information, which helps in troubleshooting the issues.

Figure 16-4: Session Details

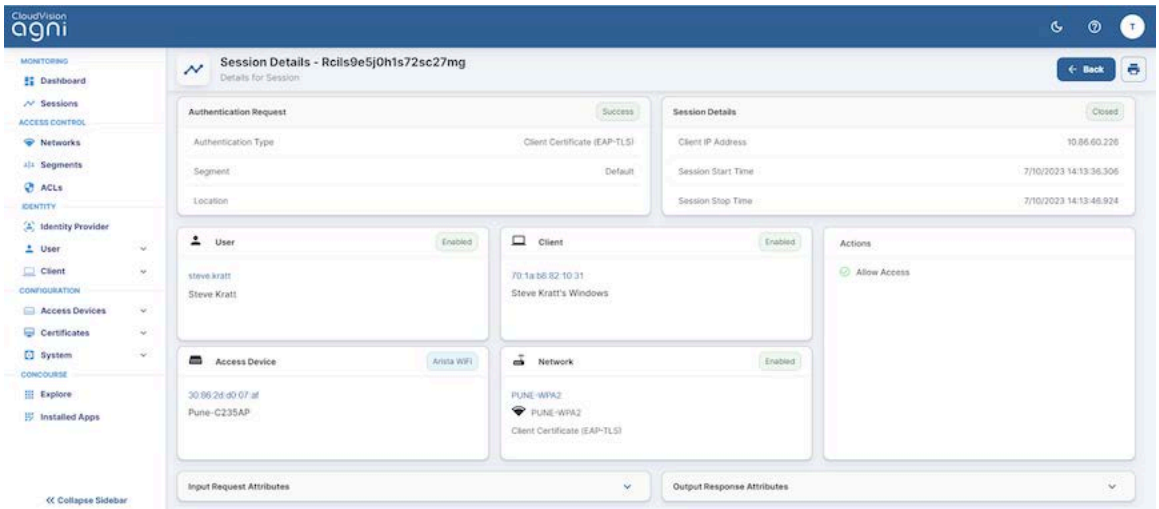
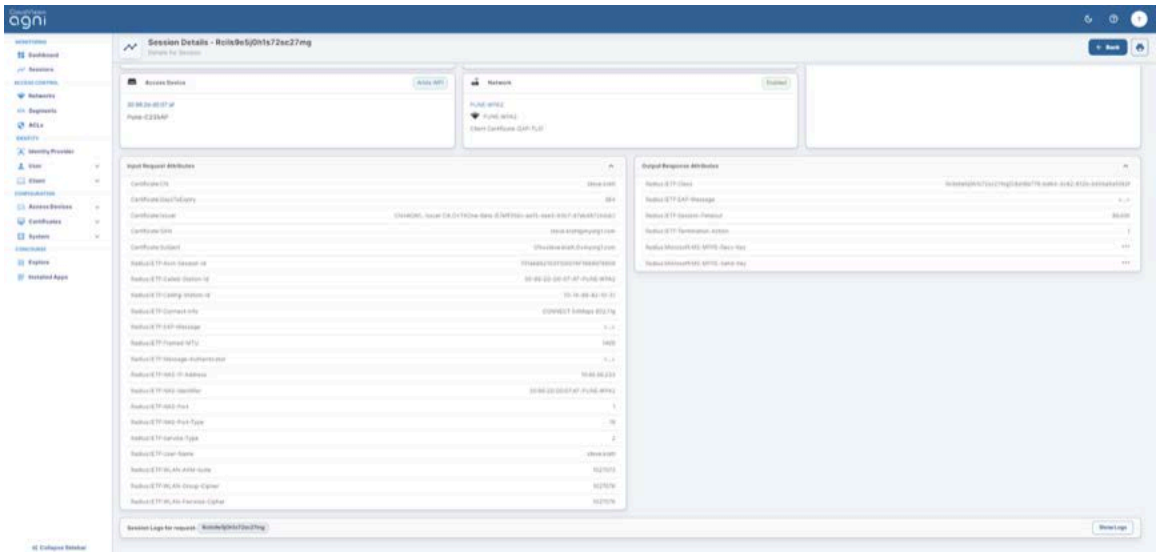
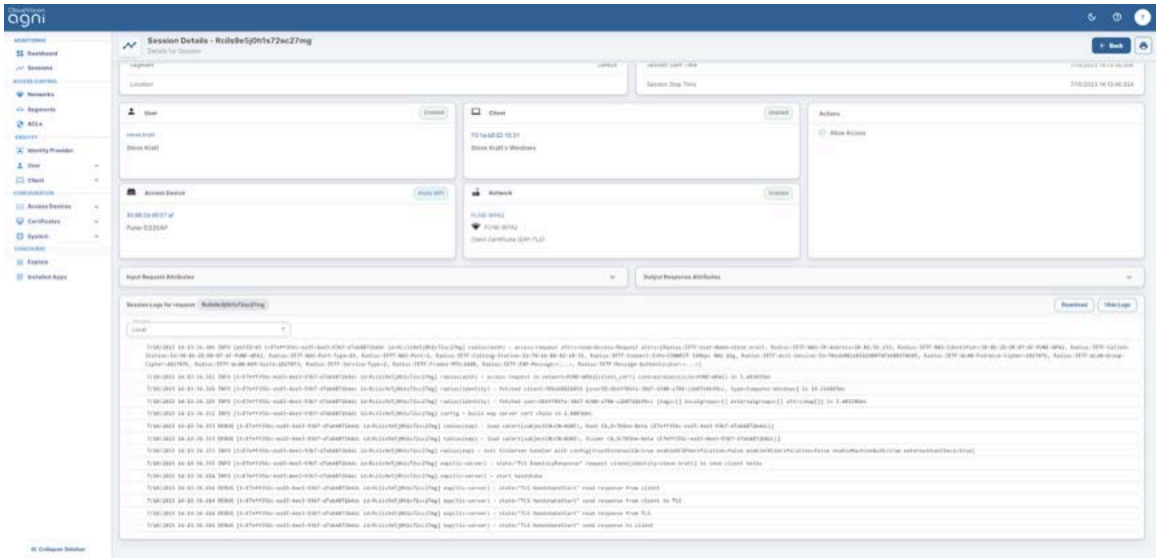


Figure 16-5: Session Details page 2



Show logs option in session details provide information about the session as well as the complete debug logs of the request. Use this information to troubleshoot the failure and take appropriate action.

Figure 16-6: Sessions and Show Logs



Appendix

This section briefly describes:

- Authentication methods supported by AGNI and the factors that help in choosing a suitable authentication method.
- Identity Providers supported by AGNI.
- Supported URLs and open ports.

A.1 OIDC Vs SAML

The authentication protocol, OpenID Connect (OIDC), verifies the user's identity when accessing a protected resource by using the OAuth 2.0 protocol to provide identity services; whereas in the case of Security Assertion Markup Language (SAML), the identity providers use SAML to exchange authentication and authorization data with service providers.

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

- SAML is an old standard and difficult to use for modern application use cases due to 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 addressed 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.

A.2 Identity Providers

The following Identity Providers are supported in AGNI.

A.2.1 Microsoft Azure Active Directory

1. Log in to Azure Active Directory instance.

2. Create a New Registration by navigating to **Home** > **Manage** > **App Registrations**.
3. Click on the newly created registration. Take note of the values for:
   a. Application (client) ID: Use this value for the Client ID field in AGNI.
   b. Directory (tenant) ID: Use this value for the Tenant ID field in AGNI.
4. Navigate to **Manage** > **Certificates & Secrets**. Add a **New Client Secret**. Take note of the value of the newly created secret. Use this value for the Client Secret value in AGNI.
5. Navigate to **Manage** > **API Permissions**. Set the following permissions (see image).

Figure A-1: API Permissions

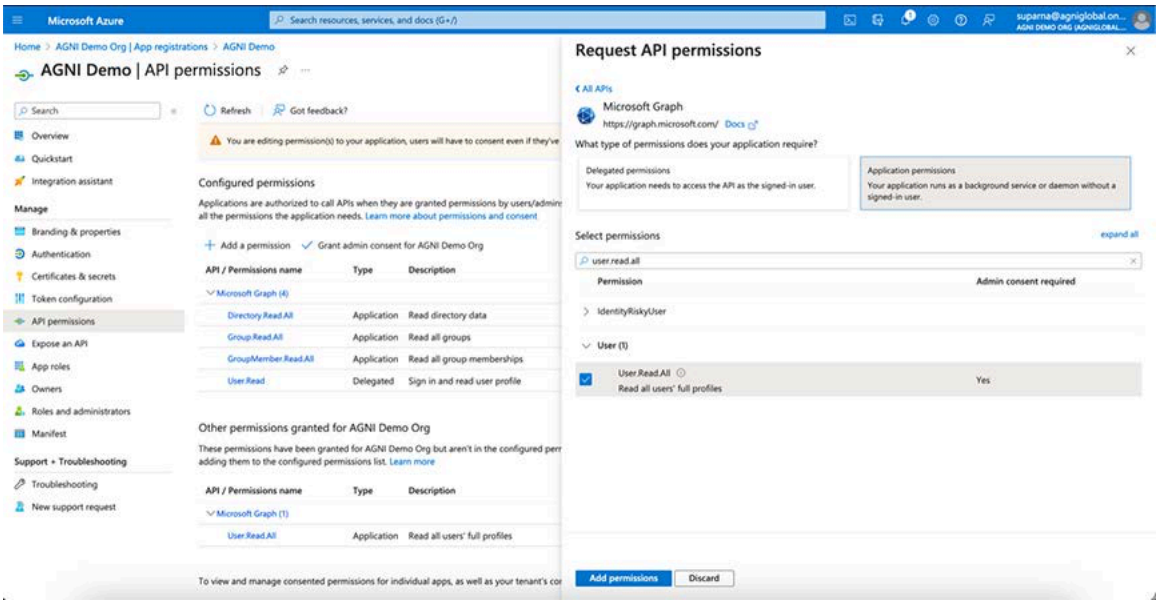


Table 1: API Permissions table

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

A.2.2 Google Workspace

1. Log in to Google Workspace.
2. Take note of the following entities from Google Console:
   a. Customer ID
   b. Domain
   c. **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.
   d. **Service Account**
3. To read Customer ID and Domain:

   a. Log in to **https://admin.google.com**
   b. Navigate to **Account** > **Account Settings**
   c. Take note of the **Customer ID** that is displayed in the Profile section.
   d. Navigate to **Domains** > **Manage Domains**
   e. Take note of the primary domain name as Domain.
4. Configuring the Service Account:
   a. Log in to **https://console.cloud.google.com**.
   b. Create a new project for AGNI.
   c. Navigate to **APIs & Services** > **Credentials**
   d. Create a new Service Account and download the JSON file.
5. Scopes for Service Account:
   a. Log in to **https://admin.google.com**
   b. Select **Enable Google Workspace domain-wide delegation** for the Service Account.
   c. Enter the following common OAuth scopes separated by comma:
      - 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

A.2.3 OneLogin

1. Log in to OneLogin administration interface and perform the following steps:
2. Navigate to **Applications** > **Applications** and add new **OpenId Connect** (OIDC) application.
3. Take note of the **Client ID** and **Issuer URL** under the SSO section of the application.
4. Navigate to **Developers** > **API Credentials**.
5. Add New Credentials and set the privileges to **Read users**.
6. Take note of the **Client ID** and **Client Secret**.

A.2.4 Okta

1. Log in to Okta administration interface and perform the following steps:
2. Navigate to **Applications** > **Applications** and add a new **Create App Registration**.
3. Choose **Client Authentication** as None.

4. Choose **Proof Key for Code Exchange** (PKCE).
5. Set the **Application Type** as **Single Page App** (SPA).
6. Set the **Grant Type** to **Client Acting on behalf of a user**.
7. Enter the:
   a. **Authorization Code**
   b. **Refresh Token**
8. Specify the Sign in redirect URLs (AGNI's cluster details as documented).
9. Set **Login initiated** by App Only.
10. Once created, take note of the **Client ID**.
11. Navigate to **Security** > **API**.
12. Create a new token and note down the:
    a. **Issuer URL**
    b. **API Key**

A.2.5 URLs and Open Ports in Firewall

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

For details on onboarding an Android device, see the EAP-TLS based Enterprise SSID using CV-CUE and AGNI: Configuration and Onboarding article.

See table for the URLs and open ports:

Table 2: URLs and Open Ports in Firewall

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